D-Link®
Building Networks for People

Network Security Firewall Log Reference Guide

NetDefendOS

Ver. 12.00.20

Network Security Solution http://www.dlink.com

NetDefend

Log Reference Guide

DFL-260E/860E/870/1660/2560/2560G

NetDefendOS Version 12.00.20

D-Link Corporation
No. 289, Sinhu 3rd Rd, Neihu District, Taipei City 114, Taiwan R.O.C.
http://www.DLink.com

Published 2019-09-16

Log Reference Guide
DFL-260E/860E/870/1660/2560/2560G

NetDefendOS Version 12.00.20

Published 2019-09-16

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. D-Link makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. D-Link reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

List of Tables

List of Examples

Preface

Audience

The target audience for this reference guide consists of:

- Administrators that are responsible for configuring and managing a NetDefendOS installation.
- Administrators that are responsible for troubleshooting a NetDefendOS installation.

This guide assumes that the reader is familiar with NetDefendOS and understands the fundamentals of IP network security.

Notation

The following notation is used throughout this reference guide when specifying the parameters of a log message:

Angle Brackets <name> Used for specifying the *name* of a log message parameter.

Square Brackets [name] Used for specifying the *name of a conditional* log message parameter.

Example 1. Log Message Parameters

Log Message New configuration activated by user <username>, and committed via <authsystem>

Parameters authsystem
username

Both the *authsystem* and the *username* parameters will be included.

Example 2. Conditional Log Message Parameters

Log Message Administrative user <username> logged in via <authsystem>. Access level: <access_level>

Parameters authsystem
username
access_level
[userdb]
[server_ip]
[server_port]
[client_ip]
[client_port]

The *authsystem*, *username* and the *access_level* parameters will be included. The other parameters of *userdb*, *server_ip*, *server_port*, *client_ip* and *client_port* may or may not be included,

depending on the context of the log message.

Abbreviations

The following abbreviations are used throughout this reference guide:

Abbreviation	Full name
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HA	High Availability
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
NAT	Network Address Translation
OSPF	Open Shortest Path First
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
RADIUS	Remote Authentication Dial In User Service
SAT	Static Address Translation
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Table 1. Abbreviations

Chapter 1: Introduction

This guide is a reference for all log messages generated by NetDefendOS. It is designed to be a valuable information source for both management and troubleshooting.

1.1. Log Message Structure

All log messages have a common design with attributes that include category, severity and recommended actions. These attributes enable the easy filtering of log messages, either within NetDefendOS prior to sending them to a log receiver, or as part of analysis that takes place after the logging and storage of messages on an external log server.

The following information is provided for each specific log message:

Name The name of the log message, which is a short string, 1-6 words separated by _. Please note that the name *cannot* be used as a unique identification of the log message, as several log messages might share the same name.

ID The ID is a number made up of a string of 8 digits which uniquely identifies the log message. The first 3 digits identify the category to which the log message belongs.

Note

In this guide, the Name and the ID of the log message form the title of the section describing the log message.

Category Log messages are grouped into categories, where each category maps to a specific subsystem in NetDefendOS. For instance, the IPSEC category includes some hundreds of log messages, all related to IPSec VPN activities. Other examples of categories include ARP, DHCP, IGMP and USERAUTH.

In this guide, categories are listed as sections in Chapter 2, *Log*

Message Reference.

As previously mentioned, the category is identified by the first 3 digits in the message ID. All messages in a particular category have the same first 3 digits in their ID.

Default Severity The default severity level for this log message. For a list of severity levels, please see section Section 1.3, “Severity levels”.

Log Message A brief explanation of the event that took place. This explanation often features references to parameters, enclosed in angle brackets. Example:

Administrative user <username> logged in via <authsystem>. Access level: <access_level>

Note that this information is only featured in this reference guide, and is never actually included in the log message.

Explanation A detailed explanation of the event.

Note that this information is only featured in this reference guide, and is never actually included in the log message.

Firewall Action A short string, 1-3 words separated by _, of what action NetDefendOS will take. If the log message is purely informative, this is set to "None".

Recommended Action A detailed recommendation of what the administrator should do if this log message is received. If the log message is purely informative, this is set to "None".

Note that this information is only featured in this reference guide, and is never actually included in the log message.

Revision The current revision of the log message. This is increased each time a log message is changed between two releases.

Additional Information

Depending on the log message, the following information may also be included:

Parameters The name of the parameters that are included in this log message. If a parameter is specified within square brackets (for example [username]), then the parameter is optional and may or may not be included in the log message.

Context Parameters The name of the context parameters that are included in this log message. Please see Section 1.2, “Context Parameters” for a description of all available context parameters.

1.2. Context Parameters

In many cases, information regarding a certain object is featured in the log message. This can be information about, for example, a connection. In this case, the log message should, besides all the normal log message attributes, also include information about which protocol is used, source and destination IP addresses and ports (if applicable), and so on.

As the same information will be included in many log messages, these are referenced as a *Context Parameter*. So whenever a log message includes information about a connection, it will feature the CONN parameter in the Context Parameter list. This means that additional information about the connection will also be included in the log message.

A description of all available context parameters follows with an explanation of all the additional parameters. The names of the additional parameters are specified using the Syslog format.

ALG Module Name

An ALG is always of a certain type, for example FTP, H323 or HTTP. This parameter specifies the name of the ALG sub-module, in order to quickly distinguish which type of ALG this is.

algmod The name of the ALG sub-module.

ALG Session ID

Each ALG session has its own session ID, which uniquely identifies an ALG session. This is useful, for example, when matching the opening of an ALG session with the closure of the same ALG session.

algsesid The session ID of an ALG session.

Packet Buffer

Information about the packet buffer, which in turn contains a large number of additional objects. Certain parameters may or may not be included, depending on the type of packet buffer. For example, the TCP flags are only included if the buffer contains a TCP protocol, and the ICMP-specific parameters are only included if the buffer contains a ICMP protocol.

recvif The name of the receiving interface.

recvzone The zone assigned to the receiving interface.

[hwsender] The sender hardware address. Valid if the protocol is ARP.

[hwdest] The destination hardware address. Valid if the protocol is ARP.

[arp] The ARP state. Valid if the protocol is ARP. Possible values: *request*|*reply*.

[srcip] The source IP Address. Valid if the protocol is not ARP.

[destip] The destination IP Address. Valid if the protocol is not ARP.

iphdrlen The IP header length.

[fragoffs] Fragmentation offset. Valid if the IP packet is fragmented.

[fragid] Fragmentation ID. Valid if the IP packet is fragmented.

ipproto The IP Protocol.

ipdatalen The IP data length.

[srcport] The source port. Valid if the protocol is TCP or UDP.

[destport] The destination port. Valid if the protocol is TCP or UDP.

[tcphdrlen] The TCP header length. Valid if the protocol is TCP.

[udptotlen] The total UDP data length. Valid if the protocol is UDP.

[[tcpflag]=1] The specific TCP flag is set. Valid if the protocol is TCP. Possible values for tcpflag: *syn, rst, ack, psh, fin, urg, ece, cwr* and *ns*.

[icmptype] The ICMP sub-protocol name. Valid if the protocol is ICMP.

[echoid] The ICMP echo ID. Valid if the protocol is ICMP and sub-protocol is echo.

[echoseq] The ICMP echo sequence number. Valid if the protocol is ICMP and sub-protocol is echo.

[unreach] The ICMP destination unreachable code. Valid if the protocol is ICMP and sub-protocol is destination unreachable.

[redirect] The ICMP redirect code. Valid if the protocol is ICMP and sub-protocol is redirect.

[icmpcode] The ICMP sub-protocol code. Valid if the protocol is ICMP and sub-protocol is not echo, destination unreachable or redirect.

Connection

Additional information about a connection. Certain parameters may or may not be included depending on the type and status of the connection. For example, the number of bytes sent by the originator and terminator is only included if the connection is closed.

conn The status of the connection. Possible values: *open, close, closing* and *unknown*.

connipproto The IP protocol used in this connection.

connrecvif The name of the receive interface.

connrecvzone The zone assigned to the receiving interface.

connsrcip The source IP address.

[connsrcport] The source port. Valid if the protocol is TCP or UDP.

[connsrcidt] The source ID. Valid if the protocol is not TCP or UDP.

conndestif The name of the destination interface.

conndestzone The zone assigned to the destination interface.

conndestip The destination IP address.

[conndestport] The destination port. Valid if the protocol is TCP or UDP.

[conndestidt] The destination ID. Valid if the protocol is not TCP or UDP.

[origsent] The number of bytes sent by the originator in this connection. Valid if the connection is closing or closed.

[termsent] The number of bytes sent by the terminator in this connection. Valid if the connection is closing or closed.

IDP

Specifies the name and a description of the signature that triggered this event.

Note

For IDP log messages an additional log receiver, an SMTP log receiver, can be configured. This information is only sent to log receives of that kind, and not included in the Syslog format.

Dropped Fragments

Specifies detailed information about dropped fragments in a packet.

Rule Name

Specifies the name of the rule that was used when this event was triggered.

rule The name of the rule.

Rule Information

Additional information about the rule that was used when this event was triggered. Certain parameters may or may not be included, depending on the type of rule. For example, the name of an authenticated user is only included if this rule contains network objects that has user authentication information in them.

rule The name of the rule.

[satsrcrule] The name of the SAT source rule. Valid if the rule action is SAT.

[satdestrule] The name of the SAT destination rule. Valid if the rule action is SAT.

[srcusername] The name of the authenticated user in the source network object. Valid if the source network object has user authentication information.

[destusername] The name of the authenticated user in the destination network object. Valid if the destination network object has user authentication information.

User Authentication

Additional information about a user authentication event.

authrule The name of the user authentication rule.

authagent The name of the user authentication agent.

authevent The user authentication event that occurred. Possible values: *login, logout, timedout, disallowed_login, accounting* and *unknown*.

username The name of the user that triggered this event.

srcip The source IP address of the user that triggered this event.

OSPF

Additional information about OSPF.

logsection The OSPF section Possible values: *packet, hello, ddesc, exchange, lsa, spf, route* and *unknown*.

loglevel The log level value.

OSPF LSA

Additional information about OSPF LSA.

lsatype The LSA type Possible values: *Router, network, IP summary, ASBR summary* and *AS external*.

lsaid The LSA identifier.

lsaadvrtr The originating router for the LSA.

Dynamic Route

Additional information about events regarding a dynamic route.

event The dynamic routing event that occurred. Possible values: *add, remove, modify, export, unexport* and *unknown*.

from Originating router process.

to Destination router process.

Route

Additional information about a route.

route	Route network.
routeiface	Route destination interface.
routezone	The zone assigned to the destination interface.
routegw	Route gateway.
routemetric	Route metric (cost).

1.3. Severity levels

An event has a default severity level, based on how serious the event is. The following eight severity levels are possible, as defined by the Syslog protocol:

0 - Emergency	Emergency conditions, which most likely led to the system being unusable.
1 - Alert	Alert conditions, which affected the functionality of the unit. Needs attention immediately.
2 - Critical	Critical conditions, which affected the functionality of the unit. Action should be taken as soon as possible.
3 - Error	Error conditions, which probably affected the functionality of the unit.
4 - Warning	Warning conditions, which could affect the functionality of the unit.
5 - Notice	Normal, but significant, conditions.
6 - Informational	Informational conditions.
7 - Debug	Debug level events.

Priority in Syslog Messages

In Syslog messages the priority is indicated by the parameter **prio=*nn***.

Excluding Logged Messages

NetDefendOS allows the exclusion from logging of entire catageories of log messages or just specific log messages. It is also possible to change the severity level of log messages so that a specific category or a specific message has the severity reset to a particular level when it is sent by NetDefendOS. These features are documented further in the NetDefendOS Administrators Guide.

Chapter 2: Log Message Reference

Sort Order
All log messages are sorted by their category and then by their ID number.

2.1. ALG

These log messages refer to the **ALG (Events from Application Layer Gateways)** category.

2.1.1. alg_session_open (ID: 00200001)

Default Severity	INFORMATIONAL
Log Message	ALG session opened
Explanation	A new ALG session has been opened.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.2. alg_session_closed (ID: 00200002)

Default Severity	INFORMATIONAL
Log Message	ALG session closed
Explanation	An ALG session has been closed.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.3. max_line_length_exceeded (ID: 00200003)

Default Severity	ERROR
Log Message	Maximum line length <max> exceeded, got <len> characters. Closing connection
Explanation	The maximum length of an entered line was exceeded, and the connection will be closed.
Firewall Action	close
Recommended Action	If the maximum line length is configued too low, increase it.
Revision	1
Parameters	len max
Context Parameters	ALG Module Name ALG Session ID

2.1.4. alg_session_allocation_failure (ID: 00200009)

Default Severity	CRITICAL
Log Message	Failed to allocate ALG session
Explanation	The system failed to allocate an ALG session. The reason for this is either that the total number of concurrent ALG sessions has been reached or that the system has run out of memory.
Firewall Action	None
Recommended Action	Increase the number of ALG sessions on services configured with ALGs or try to free up some RAM depending on the situation.
Revision	1

2.1.5. invalid_client_http_header_received (ID: 00200100)

Default Severity	WARNING
Log Message	HTTPALG: Invalid HTTP header was received from the client. Closing Connection. ALG name: <algname>.
Explanation	An invalid HTTP header was received from the client.
Firewall Action	close
Recommended Action	Research the source of this and try to find out why the client is sending an invalid header.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.6. invalid_url_format (ID: 00200101)

Default Severity	ERROR
Log Message	HTTPALG: Failed to parse the URL requested by the client: <reason>. ALG name: <algname>.
Explanation	The unit failed parsing the requested URL. The reason for this is problaby because the requested URL has an invalid format, or it contains invalid UTF8 formatted characters.
Firewall Action	close
Recommended Action	Make sure that the requested URL is formatted correctly.
Revision	1
Parameters	reason algname
Context Parameters	ALG Module Name ALG Session ID

2.1.7. allow_unknown_protocol (ID: 00200102)

Default Severity	NOTICE
Log Message	Allowing unknown protocol. ALG name: <algname>.
Explanation	Invalid protocol data received from the client. The connection will be allowed to pass through without inspection according to the configuration.

Firewall Action	allow
Recommended Action	If unknown protocols should be blocked, change the configuration.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.8. allow_unknown_protocol (ID: 00200103)

Default Severity	NOTICE
Log Message	Allowing unknown protocol. ALG name: <algname>.
Explanation	Invalid protocol data received from the server. The connection will be allowed to pass through without inspection according to the configuration.
Firewall Action	allow
Recommended Action	If unknown protocols should be blocked, change the configuration.
Revision	2
Parameters	algname
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.9. wcf_srv_connection_error (ID: 00200104)

Default Severity	ERROR
Log Message	HTTPALG: HTTP request not validated by Web Content Filter and denied.
Explanation	The Web Content Filtering servers could not be contacted. The request has been denied since fail-mode parameter is in deny mode.
Firewall Action	deny
Recommended Action	Investigate why the Web Content Filtering servers cannot be reached.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.10. unknown_client_data_received (ID: 00200105)

Default Severity	WARNING
Log Message	HTTPALG: Invalid client request - unexpected data received after the the client request header. Closing connection. ALG name: <algname>.
Explanation	Data was received after the client request header, although the header specified that no such data should be sent.
Firewall Action	closing_connecion
Recommended Action	Research the source of this, and try to find out why the client is sending an invalid request.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.11. suspicious_data_received (ID: 00200106)

Default Severity	WARNING
Log Message	HTTPALG: Too much suspicious data has been received from the server. Closing the connection. ALG name: <algname>.
Explanation	The unit is configured to do content blocking, but the data from the server contains too much suspicious data. The unit can not properly determin if this data is a valid or if it should be blocked.
Firewall Action	closing_connecion
Recommended Action	Research the source of this, and try to find out why the server is sending such large amounts of suspicious data.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.12. invalid_chunked_encoding (ID: 00200107)

Default Severity	WARNING
Log Message	HTTPALG: The server sent invalid chunked encoding. Closing connection. ALG name: <algname>.
Explanation	The data received from the server was sent in chunked mode, but it

	was not properly formatted.
Firewall Action	closing_connecion
Recommended Action	Research the source of this, and try to find out why the server is sending invalid formatted chunked data.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.13. invalid_server_http_header_received (ID: 00200108)

Default Severity	WARNING
Log Message	HTTPALG: An invalid HTTP header was received from the server. Closing connection. ALG name: <algname>.
Explanation	An invalid HTTP header was received from the server.
Firewall Action	closing_connecion
Recommended Action	Research the source of this and try to find out why the server is sending an invalid header.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.14. compressed_data_received (ID: 00200109)

Default Severity	ERROR
Log Message	HTTPALG: Compressed data was received from the server, although uncompressed was requested. Closing connection. ALG name: <algname>.
Explanation	The unit requested that no compressed data should be used, but the server ignored this and sent compressed data anyway. As content processing will not work if the data is compressed, the connection will be closed.
Firewall Action	close
Recommended Action	Research the source of this, and try to find out why the server is sending compressed data.
Revision	1
Parameters	algname

Context Parameters	ALG Module Name ALG Session ID

2.1.15. max_http_sessions_reached (ID: 00200110)

Default Severity	WARNING
Log Message	HTTPALG: Maximum number of HTTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent HTTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of HTTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.16. failed_create_new_session (ID: 00200111)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to create new HTTPALG session (out of memory)
Explanation	An attempt to create a new HTTPALG session failed, because the unit is out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed HTTPALG sessions, or try to free some of the RAM used.
Revision	2
Context Parameters	ALG Module Name

2.1.17. failure_connect_http_server (ID: 00200112)

Default Severity	ERROR
Log Message	HTTPALG: Failed to connect to the HTTP Server. Closing connection. ALG name: <algname>.
Explanation	The unit failed to connect to the HTTP Server, resulting in that the ALG session could not be successfully opened.
Firewall Action	close

Recommended Action	Verify that there is a listening HTTP Server on the specified address.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.18. content_type_mismatch (ID: 00200113)

Default Severity	NOTICE
Log Message	HTTPALG: Content type mismatch in file <filename>. Identified filetype <filetype>
Explanation	The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.
Firewall Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename filetype contenttype
Context Parameters	ALG Module Name ALG Session ID

2.1.19. wcf_override_full (ID: 00200114)

Default Severity	ERROR
Log Message	HTTPALG: WCF override cache full
Explanation	The WCF override hash is full. The oldest least used value will be replaced.
Firewall Action	replace
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.20. no_valid_license (ID: 00200115)

Default Severity	ERROR
Log Message	HTTPALG: Web Content Filtering disabled

Explanation	Web Content Filtering has been disabled due to license restriction.
Firewall Action	content_filtering_disabled
Recommended Action	Extend valid time for Content Filtering.
Revision	3
Context Parameters	ALG Module Name

2.1.21. max_download_size_reached (ID: 00200116)

Default Severity	WARNING
Log Message	HTTPALG: The file <filename> with file size <filesize>kB exceeds the maximum allowed download size <max_download_size>kB. Closing connection
Explanation	The data received from the server exceeds the maximun allowed download file size, the request is rejected and the connection is closed.
Firewall Action	close
Recommended Action	If the configurable maximum download size is too low, increase it.
Revision	2
Parameters	filename filesize max_download_size
Context Parameters	ALG Module Name ALG Session ID

2.1.22. blocked_filetype (ID: 00200117)

Default Severity	NOTICE
Log Message	HTTPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Firewall Action	block
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.23. out_of_memory (ID: 00200118)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to allocate memory
Explanation	The unit does not have enough available RAM. WCF could not allocate memory for override functionality.
Firewall Action	none
Recommended Action	Try to free up some RAM by changing configuration parameters.
Revision	1
Context Parameters	ALG Module Name

2.1.24. wcf_servers_unreachable (ID: 00200119)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to connect to web content servers
Explanation	Web Content Filtering was unable to connect to the Web Content Filtering servers.
Firewall Action	none
Recommended Action	Verify that the unit has been configured with Internet access.
Revision	2
Context Parameters	ALG Module Name

2.1.25. wcf_srv_connection_error (ID: 00200120)

Default Severity	ERROR
Log Message	HTTPALG: HTTP request not validated by Web Content Filter and allowed.
Explanation	The Web Content Filtering servers could not be contacted. The request has been allowed since fail-mode parameter is in allow mode.
Firewall Action	allow
Recommended Action	Investigate why the Web Content Filtering servers cannot be reached.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name

ALG Session ID

2.1.26. wcf_server_unreachable (ID: 00200121)

Default Severity	ERROR
Log Message	HTTPALG: Failed to connect to web content server <failedserver>
Explanation	Web Content Filtering was unable to connect to the Web Content Filtering server. The system will try to contact one of the backup servers.
Firewall Action	switching_server
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.27. wcf_connecting (ID: 00200122)

Default Severity	INFORMATIONAL
Log Message	HTTPALG:Connecting to web content server <server>
Explanation	Connecting to Web Content Filtering server.
Firewall Action	connecting
Recommended Action	None.
Revision	1
Parameters	server
Context Parameters	ALG Module Name

2.1.28. wcf_server_connected (ID: 00200123)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: Web content server <server> connected
Explanation	The connection with the Web Content server has been established.
Firewall Action	none
Recommended Action	None.
Revision	1

Parameters	server
Context Parameters	ALG Module Name

2.1.29. wcf_primary_fallback (ID: 00200124)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: Falling back from secondary servers to primary server
Explanation	Web Content Filtering falls back to primary server after 60 minutes or when a better server has been detected.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.30. request_url (ID: 00200125)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. Audit: <audit>. Override: <override>. ALG name: <algname>.
Explanation	The URL has been requested.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	categories audit override url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.31. request_url (ID: 00200126)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. Audit: <audit>. Override: <override>. ALG name: <algname>.

Explanation	The URL has been requested.
Firewall Action	block
Recommended Action	None.
Revision	2
Parameters	categories audit override url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.32. wcf_server_auth_failed (ID: 00200127)

Default Severity	ERROR
Log Message	HTTPALG: Failed to authenticate with WCF server
Explanation	The WCF service could not authenticate with the WCF server.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.33. wcf_server_bad_reply (ID: 00200128)

Default Severity	ERROR
Log Message	HTTPALG: Failed to parse WCF server response
Explanation	The WCF service could not parse the server response. The WCF transmission queue is reset and a new server connection will be established.
Firewall Action	restarting
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.34. request_url (ID: 00200129)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. Audit: <audit>. Override: <override>. ALG name: <algname>.
Explanation	The URL has been requested.
Firewall Action	allow_audit_mode
Recommended Action	None.
Revision	2
Parameters	categories audit override url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.35. out_of_memory (ID: 00200130)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to allocate memory
Explanation	The unit does not have enough available RAM.
Firewall Action	none
Recommended Action	Try to free up some RAM by changing configuration parameters.
Revision	1
Context Parameters	ALG Module Name

2.1.36. wcf_bad_sync (ID: 00200131)

Default Severity	ERROR
Log Message	HTTPALG: WCF request out of sync
Explanation	The WCF response received from the server did not match the expected value. The requested URL is treaded as unknown category.
Firewall Action	compensating
Recommended Action	None.

Revision	1
Parameters	url_orig url_req url_reply
Context Parameters	ALG Module Name

2.1.37. restricted_site_notice (ID: 00200132)

Default Severity	WARNING
Log Message	HTTPALG: User requests the forbidden URL <url>, even though Restricted Site Notice was applied. ALG name: <algname>.
Explanation	The URL has been requested and the categories are forbidden. Restricted Site Notice was applied.
Firewall Action	allow
Recommended Action	Disable the RESTRICTED_SITE_NOTICE mode of parameter CATEGORIES for this ALG.
Revision	3
Parameters	url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.38. url_reclassification_request (ID: 00200133)

Default Severity	WARNING
Log Message	HTTPALG: Reclassification request for URL <url>. New Category <newcat>. ALG name: <algname>.
Explanation	The user has requested a category reclassification for the URL.
Firewall Action	allow
Recommended Action	Disable the ALLOW_RECLASSIFICATION mode of parameter CATEGORIES for this ALG.
Revision	2
Parameters	newcat url algname
Context Parameters	Connection Connection ALG Module Name

ALG Session ID

2.1.39. wcf_server_disconnected (ID: 00200134)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: Web content server <server> disconnected
Explanation	The Web Content server has closed the connection.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	server
Context Parameters	ALG Module Name

2.1.40. request_url (ID: 00200135)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. User: <user>. Audit: <audit>. Override: <override>. ALG name: <algname>.
Explanation	The URL has been requested.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	categories audit override url user algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.41. request_url (ID: 00200136)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. User: <user>. Audit: <audit>. Override: <override>. ALG name:

<algname>.

Explanation The URL has been requested.

Firewall Action allow_audit_mode

Recommended Action None.

Revision 3

Parameters
categories
audit
override
url
user
algname

Context Parameters
Connection
Connection
ALG Module Name
ALG Session ID

2.1.42. request_url (ID: 00200137)

Default Severity NOTICE

Log Message HTTPALG: Requesting URL <url>. Categories: <categories>. User: <user>. Audit: <audit>. Override: <override>. ALG name: <algname>.

Explanation The URL has been requested.

Firewall Action block

Recommended Action None.

Revision 3

Parameters
categories
audit
override
url
user
algname

Context Parameters
Connection
Connection
ALG Module Name
ALG Session ID

2.1.43. restricted_site_notice (ID: 00200138)

Default Severity WARNING

Log Message HTTPALG: User requests the forbidden URL <url>, even though Restricted Site Notice was applied. User: <user>. ALG name:

<algname>.

Explanation The URL has been requested and the categories are forbidden. Restricted Site Notice was applied.

Firewall Action allow

Recommended Action Disable the RESTRICTED_SITE_NOTICE mode of parameter CATEGORIES for this ALG.

Revision 4

Parameters
url
user
algname

Context Parameters
Connection
Connection
ALG Module Name
ALG Session ID

2.1.44. url_reclassification_request (ID: 00200139)

Default Severity WARNING

Log Message HTTPALG: Reclassification request for URL <url>. New Category <newcat>. User: <user>. ALG name: <algname>.

Explanation The user has requested a category reclassification for the URL.

Firewall Action allow

Recommended Action Disable the ALLOW_RECLASSIFICATION mode of parameter CATEGORIES for this ALG.

Revision 3

Parameters
newcat
url
user
algname

Context Parameters
Connection
Connection
ALG Module Name
ALG Session ID

2.1.45. wcf_mem_optimized (ID: 00200140)

Default Severity DEBUG

Log Message HTTPALG: Optimizing WCF memory usage

Explanation The Web Content Filtering subsystem has optimized its memory usage and freed up some memory. This is a normal condition and does not affect functionality nor performance.

Firewall Action	optimizing
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.46. out_of_memory (ID: 00200141)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to allocate memory
Explanation	The system failed to allocate memory and the HTTP session will be closed.
Firewall Action	close
Recommended Action	Decrease the maximum allowed HTTPALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.47. wcf_performance_notice (ID: 00200142)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: WCF Performance notice
Explanation	Information about the current WCF performance.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	cache_size cache_repl_per_sec trans_per_sec queue_len in_transit rtt queue_delta_per_sec server srv_prec
Context Parameters	ALG Module Name

2.1.48. wcf_server_timeout (ID: 00200143)

Default Severity	ERROR
Log Message	HTTPALG: WCF request timeout
Explanation	The WCF server took too long time to reply. A new connection attempt is in progress.
Firewall Action	reconnecting
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.49. invalid_http_syntax (ID: 00200144)

Default Severity	ERROR
Log Message	HTTPALG: Invalid HTTP syntax seen in <type>.
Explanation	The HTTPALG received malformed HTTP syntax and closed the connection.
Firewall Action	close
Recommended Action	Investigate why malformed HTTP syntax was received.
Revision	1
Parameters	type reason algname
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.50. intercept_page_failed (ID: 00200145)

Default Severity	DEBUG
Log Message	HTTPALG: Failed to send interception page to client
Explanation	The HTTPALG failed to send an interception page to the client.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	pagetype send algname
Context Parameters	Connection

ALG Module Name
ALG Session ID

2.1.51. disallowed_user_agent (ID: 00200146)

Default Severity WARNING

Log Message HTTPALG: Disallowed user-agent <ua>.

Explanation The HTTPALG blocked access for a browser with a disallowed user-agent string.

Firewall Action close

Recommended Action If this user-agent string should be allowed, add it to the list of allowed user-agent strings in the ALG configuration.

Revision 1

Parameters ua
algname

Context Parameters Connection
ALG Module Name
ALG Session ID

2.1.52. http_pipeline_full (ID: 00200147)

Default Severity ERROR

Log Message HTTPALG: Maximum number of pipelinined requests per session reached.

Explanation The maximum number of unanswered pipelined HTTP requests has been reached. This can be a malicious attempt to drain the firewall of resources. The connection is closed.

Firewall Action close

Recommended Action Investigate which client and software that sends this many pipelinied requests and see if they can be reconfigured.

Revision 2

Parameters count
algname

Context Parameters Connection
Connection
ALG Module Name
ALG Session ID

2.1.53. protocol_upgrade_denied (ID: 00200148)

Default Severity	WARNING
Log Message	HTTPALG: Protocol upgrade denied
Explanation	The HTTPALG blocked a socket upgrade e.g. websocket. The connection is no longer allowed.
Firewall Action	close
Recommended Action	Modify the configuration is socket upgrades should be allowed.
Revision	1
Parameters	type algname
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.54. protocol_upgrade (ID: 00200149)

Default Severity	NOTICE
Log Message	HTTPALG: Protocol Upgrade
Explanation	The HTTPALG allowed a socket upgrade e.g. websocket. No more content inspection will be made on this connection.
Firewall Action	allow
Recommended Action	Modify the configuration if socket upgrades should not be allowed.
Revision	1
Parameters	type algname
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.55. max_smtp_sessions_reached (ID: 00200150)

Default Severity	WARNING
Log Message	SMTPALG: Maximum number of SMTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent SMTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of SMTP sessions is too low, increase it.

Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.56. maximum_email_per_minute_reached (ID: 00200151)

Default Severity	WARNING
Log Message	SMTPALG: Maximum number of emails per client and minute reached.
Explanation	Client is trying to send emails at a rate higher than the configured value.
Firewall Action	session_rejected
Recommended Action	This can be a possible DoS attack.
Revision	3
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.57. failed_create_new_session (ID: 00200152)

Default Severity	CRITICAL
Log Message	SMTPALG: Failed to create new SMTPALG session (out of memory)
Explanation	An attempt to create a new SMTPALG session failed. The unit has run out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed SMTPALG sessions, or try to free some of the RAM used.
Revision	2
Context Parameters	ALG Module Name

2.1.58. failed_connect_smtp_server (ID: 00200153)

Default Severity	ERROR
Log Message	SMTPALG: Failed to connect to the SMTP Server. Closing the connection.
Explanation	The SMTP ALG could not connect to the receiving SMTP server, resulting in that the ALG session could not be successfully opened.

Firewall Action	close
Recommended Action	None.
Revision	3
Context Parameters	ALG Module Name ALG Session ID

2.1.59. invalid_server_response (ID: 00200155)

Default Severity	ERROR
Log Message	SMTPALG: Could not parse server response code
Explanation	The SMTP ALG failed to parse the SMTP response code from server.
Firewall Action	close
Recommended Action	If possible, verify response codes sent from server.
Revision	3
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.60. sender_email_id_mismatched (ID: 00200156)

Default Severity	WARNING
Log Message	SMTPALG: Mismatching sender address
Explanation	The SMTP "MAIL FROM:" command does not match the "From:" header. The e-mail will be tagged as spam.
Firewall Action	spam tag
Recommended Action	Disable the Verify E-Mail Sender ID setting if you experience that valid e-mails are being wrongly tagged.
Revision	3
Parameters	sender_email_address recipient_email_addresses data_sender_address
Context Parameters	ALG Module Name ALG Session ID

2.1.61. sender_email_id_mismatched (ID: 00200157)

Default Severity	WARNING

Log Message	SMTPALG: Mismatching sender address
Explanation	The SMTP "MAIL FROM:" command does not match the "From:" header. The transaction will be denied.
Firewall Action	reject
Recommended Action	Disable the Verify E-Mail Sender ID setting if you experience that valid e-mails are being wrongly blocked.
Revision	3
Parameters	sender_email_address recipient_email_addresses data_sender_address
Context Parameters	ALG Module Name ALG Session ID

2.1.62. sender_email_id_is_in_blacklist (ID: 00200158)

Default Severity	WARNING
Log Message	SMTPALG: Sender e-mail address is in Black List
Explanation	Since "MAIL FROM:" Email Id is in Black List, SMTP ALG rejected the Client request.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.63. recipient_email_id_in_blacklist (ID: 00200159)

Default Severity	WARNING
Log Message	SMTPALG: Recipient e-mail address is in Black List
Explanation	Since "RCPT TO:" e-mail address is in Black List, SMTP ALG rejected the client request.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address recipient_email_addresses

Context Parameters	ALG Module Name ALG Session ID

2.1.64. some_recipient_email_ids_are_in_blocklist (ID: 00200160)

Default Severity	WARNING
Log Message	SMTPALG: Some recipients email id are in Black List
Explanation	Since some "RCPT TO:" Email ids are in Black List, SMTP ALG has blocked mail to those recipients.
Firewall Action	reject
Recommended Action	Emails can be forwarded only to the Non-Black List users.
Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.65. base64_decode_failed (ID: 00200164)

Default Severity	ERROR
Log Message	SMTPALG: Base 64 decode failed. Attachment blocked
Explanation	The base64 encoded attachment could not be decoded. This can occur if the email sender sends incorrectly formatted data. The attachment has been blocked.
Firewall Action	block_allow
Recommended Action	Research how the sender is encoding the data.
Revision	2
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.66. base64_decode_failed (ID: 00200165)

Default Severity	ERROR

Log Message	SMTPALG: Base 64 decode failed. Attachment is allowed
Explanation	The data sent to Base64 decoding failed. This can occur if the email sender sends incorrectly formatted data. Fail-mode is set to allow so date will be forwared.
Firewall Action	allow_block
Recommended Action	Research how the sender is encoding the data.
Revision	2
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.67. blocked_filetype (ID: 00200166)

Default Severity	NOTICE
Log Message	SMTPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Firewall Action	block
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	2
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.68. content_type_mismatch (ID: 00200167)

Default Severity	WARNING
Log Message	SMTPALG: Content type mismatch in file <filename>. Identified filetype <filetype>
Explanation	The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.
Firewall Action	block_data

Recommended Action	None.
Revision	4
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.69. max_email_size_reached (ID: 00200170)

Default Severity	WARNING
Log Message	SMTPALG: Maximum email size limit <max_email_size>kb reached
Explanation	Email body and all attachments size of email has crossed the limitation.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	sender_email_address recipient_email_addresses max_email_size
Context Parameters	ALG Module Name ALG Session ID

2.1.70. content_type_mismatch_mimecheck_disabled (ID: 00200171)

Default Severity	NOTICE
Log Message	SMTPALG: Content type mismatch found for the file <filename>. It is identified as type <filetype> file
Explanation	Received type of data in the packet and its actual type do not match. As there is a mismatch and mime type check is disabled, the data will be allowed.
Firewall Action	allow
Recommended Action	Content type should be matched.
Revision	3
Parameters	filename filetype sender_email_address recipient_email_addresses

Context Parameters	ALG Module Name ALG Session ID

2.1.71. all_recipient_email_ids_are_in_blocklist (ID: 00200172)

Default Severity	WARNING
Log Message	SMTPALG: All recipients e-mail addresses are in Black List
Explanation	Since "RCPT TO:" email ids are in Black List, SMTP ALG rejected the client request.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.72. out_of_memory (ID: 00200175)

Default Severity	ALERT
Log Message	SMTPALG: Failed to allocate memory (out of memory)
Explanation	An attempt to allocate memory failed.
Firewall Action	close
Recommended Action	Try to free up unwanted memory.
Revision	3
Context Parameters	ALG Module Name ALG Session ID

2.1.73. invalid_end_of_mail (ID: 00200176)

Default Severity	WARNING
Log Message	SMTPALG: Invalid end of mail "\\n.\\n" received.
Explanation	The client is sending invalid end of mail. Transaction will be terminated.
Firewall Action	block
Recommended Action	Research how the client is sending invalid end of mail.

Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.74. dnsbl_init_error (ID: 00200177)

Default Severity	ERROR
Log Message	DNSbl internal error
Explanation	The email could not be checked for spam. Email will be processed without spam checks.
Firewall Action	none
Recommended Action	None.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.75. cmd_too_long (ID: 00200179)

Default Severity	ERROR
Log Message	SMTPALG: Command line too long
Explanation	The SMTP Command line exceeds the maximum command length of 712 characters. (RFC 2821 Ch. 4.5.3.1 says 512).
Firewall Action	reject
Recommended Action	None.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.76. failed_send_reply_code (ID: 00200181)

Default Severity	ERROR
Log Message	SMTPALG: Could not send error code to client
Explanation	The SMTP ALG failed to send an error response code to the client.
Firewall Action	none

Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.77. smtp_no_header (ID: 00200184)

Default Severity	WARNING
Log Message	SMTPALG: Email without SMTP headers received
Explanation	The SMTP ALG received an email without headers.
Firewall Action	allow
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.78. unsupported_extension (ID: 00200185)

Default Severity	INFORMATIONAL
Log Message	SMTPALG: Removed capability <capa> from EHLO response
Explanation	The SMTP ALG removed the [capa] capability from the EHLO response since the ALG does not support the specified extension.
Firewall Action	capability_removed
Recommended Action	None.
Revision	1
Parameters	capa
Context Parameters	ALG Module Name ALG Session ID

2.1.79. cmd_pipelined (ID: 00200186)

Default Severity	ERROR
Log Message	SMTPALG: Received pipelined request.
Explanation	The SMTP ALG does not support pipelined requests. The appearance of this log message indicates that the client used PIPELINING even though it was removed from capability list.

Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.80. smtp_state_violation (ID: 00200190)

Default Severity	WARNING
Log Message	SMTPALG: State violation: <violation>.
Explanation	The client sent an invalid sequence of commands. The protocol violation is explained by the [violation] parameter.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	violation
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.81. sender_email_dnsbl_spam_mark_removed_by_whitelist (ID: 00200195)

Default Severity	WARNING
Log Message	SMTPALG: Whitelist override DNSBL result for Email.
Explanation	Email was marked as SPAM by DNSBL. As Email Id was matched in whitelist, this mark is removed.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.82. request_url_redirected (ID: 00200200)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url> redirected to <redirect>. ALG name: <algname>.
Explanation	The request has been redirected.
Firewall Action	allow
Recommended Action	None.
Revision	1
Parameters	redirect url user algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.83. illegal_data_direction (ID: 00200202)

Default Severity	ERROR
Log Message	FTPALG: TCP data from <peer> not allowed in this direction. Closing connection
Explanation	TCP Data was sent in an invalid direction, and the connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.1.84. hybrid_data (ID: 00200206)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Hybrid connection made
Explanation	A hybrid connection was successfully created.
Firewall Action	None
Recommended Action	None.

Revision 1

Context Parameters ALG Module Name
ALG Session ID
Rule Information
Connection

2.1.85. hybrid_data (ID: 00200209)

Default Severity INFORMATIONAL

Log Message FTPALG: Hybrid data channel closed

Explanation A hybrid data channel was closed.

Firewall Action None

Recommended Action None.

Revision 1

Context Parameters ALG Module Name
ALG Session ID
Rule Information
Connection

2.1.86. illegal_chars (ID: 00200210)

Default Severity WARNING

Log Message FTPALG: 8 bit characters in control channel from <peer> not allowed. Closing connection

Explanation 8 bit characters were discovered in the control channel. This is not allowed according to the FTPALG configuration, and the connection will be closed.

Firewall Action close

Recommended Action If 8 bit characters should be allowed, modify the FTPALG configuration.

Revision 1

Parameters peer

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.87. control_chars (ID: 00200211)

Default Severity WARNING

Log Message	FTPALG: Unexpected telnet control chars in control channel from <peer>. Closing connection
Explanation	Unexpected telnet control characters were discovered in the control channel. This is not allowed according to the FTPALG configuration, and the connection will be closed.
Firewall Action	close
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.88. illegal_command (ID: 00200212)

Default Severity	WARNING
Log Message	FTPALG: Failed to parse command from <peer> as a FTP command. String=<string>. Closing connection
Explanation	An invalid command was received on the control channel. This is not allowed, and the connection will be closed.
Firewall Action	close
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.89. illegal_command (ID: 00200213)

Default Severity	WARNING
Log Message	FTPALG: Failed to parse command from <peer> as a FTP command. String=<string>. Rejecting command
Explanation	An invalid command was received on the control channel. This is allowed, but the command will be rejected as it is not understood.
Firewall Action	rejecting_command

Recommended Action	If unknown commands should not be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.90. port_command_disabled (ID: 00200214)

Default Severity	WARNING
Log Message	FTPALG: PORT command not allowed from <peer>. Rejecting command
Explanation	The client tried to issue a "PORT" command, which is not valid since the client is not allowed to do active FTP. The command will be rejected.
Firewall Action	rejecting_command
Recommended Action	If the client should be allowed to do active FTP, modify the FTPALG configuration.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.91. illegal_command (ID: 00200215)

Default Severity	WARNING
Log Message	FTPALG: Failed to parse PORT parameters from <peer>. String=<string>. Closing connection
Explanation	Invalid parameters to the "PORT" command were received. The connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name

ALG Session ID
Connection

2.1.92. illegal_ip_address (ID: 00200216)

Default Severity	CRITICAL
Log Message	FTPALG: Illegal PORT command from <peer>, bad IP address <ip4addr>. String=<string>. Rejecting command
Explanation	An illegal "PORT" command was received from the client. It requests that the server should connect to another IP than its own. This is not allowed, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	The FTP client could be compromised, and should not be trusted.
Revision	1
Parameters	peer ip4addr string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.93. illegal_port_number (ID: 00200217)

Default Severity	CRITICAL
Log Message	FTPALG: Illegal PORT command from <peer>, port <port> not allowed. String=<string>. Rejecting command
Explanation	An illegal "PORT" command was received from the client. It requests that the server should connect to a port which is out of range. This is not allowed, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	The FTP client could be compromised, and should not be trusted.
Revision	1
Parameters	peer port string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.94. failed_to_create_connection1 (ID: 00200218)

Default Severity	ERROR
Log Message	FTPALG: Failed to create connection(1). Connection: <connection>. String=<string>
Explanation	An error occured when creating a data connection from the server to client. This could possibly be a result of lack of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	peer connection string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.95. illegal_command (ID: 00200219)

Default Severity	WARNING
Log Message	FTPALG: SITE EXEC from <peer> not allowed, rejecting command
Explanation	The client tried to issue a "SITE EXEC" command, which is not valid since the client is not allowed to do this. The command will be rejected.
Firewall Action	rejecting_command
Recommended Action	If the client should be allowed to do issue "SITE EXEC" commands, modify the FTPALG configuration.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.96. illegal_direction1 (ID: 00200220)

Default Severity	WARNING
Log Message	FTPALG: Illegal direction for command(1), peer=<peer>. Closing connection.
Explanation	A command was sent in an invalid direction, and the connection will be closed.

Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.97. illegal_direction2 (ID: 00200221)

Default Severity	WARNING
Log Message	FTPALG: Illegal direction for command(2), peer=<peer>. Closing connection.
Explanation	A command was sent in an invalid direction, and the connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.98. illegal_option (ID: 00200222)

Default Severity	WARNING
Log Message	FTPALG: Invalid OPTS argument from <peer>. String=<string>. Rejecting command.
Explanation	An invalid OPTS argument was received. The argument does not start with an alphabetic letter, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.99. illegal_option (ID: 00200223)

Default Severity	WARNING
Log Message	FTPALG: Disallowed OPTS argument from <peer>. String:<string>. Rejecting command.
Explanation	A disallowed OPTS argument was received, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.100. unknown_option (ID: 00200224)

Default Severity	WARNING
Log Message	FTPALG: Unknown OPTS argument from <peer>. String=<string>. Rejecting command.
Explanation	An unknown OPTS argument was received, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.101. illegal_command (ID: 00200225)

Default Severity	WARNING
Log Message	FTPALG: Illegal command from <peer>. String=<string>. Rejecting command.

Explanation	An illegal command was received, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.102. unknown_command (ID: 00200226)

Default Severity	WARNING
Log Message	FTPALG: Unknown command from <peer>. String=<string>. Rejecting command.
Explanation	An unknown command was received, and the command will be rejected.
Firewall Action	rejecting_command
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.103. illegal_reply (ID: 00200228)

Default Severity	WARNING
Log Message	FTPALG: Illegal numerical reply (<reply>) from <peer>. String=<string>. Closing connection.
Explanation	An illegal numerical reply was received from server, and the connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer

reply
string

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.104. illegal_reply (ID: 00200230)

Default Severity WARNING

Log Message FTPALG: Illegal multiline response (<reply>) from <peer>. String=<string>. Closing connection.

Explanation An illegal multiline response was received from server, and the connection will be closed.

Firewall Action close

Recommended Action None.

Revision 1

Parameters peer
reply
string

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.105. illegal_reply (ID: 00200231)

Default Severity WARNING

Log Message FTPALG: Unsolicted 227 (passive mode) response from <peer>. String=<string>. Closing connection.

Explanation An illegal response was received from the server, and the connection is closed.

Firewall Action close

Recommended Action None.

Revision 1

Parameters peer
string

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.106. illegal_reply (ID: 00200232)

Default Severity	WARNING
Log Message	FTPALG: Reply 229 (extended passive mode) from <peer> is not allowed. String=<string>. Closing connection.
Explanation	An illegal response was received from the server, and the connection is closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.107. bad_port (ID: 00200233)

Default Severity	CRITICAL
Log Message	FTPALG: Bad port <port> from <peer>, should be within the range (<range>). String=<string>. Closing connection.
Explanation	An illegal "PORT" command was received from the server. It requests that the client should connect to a port which is out of range. This is not allowed, and the connection will be closed.
Firewall Action	close
Recommended Action	The FTP server could be compromised, and should not be trusted.
Revision	1
Parameters	peer port range string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.108. bad_ip (ID: 00200234)

Default Severity	CRITICAL
Log Message	FTPALG: Invalid IP <ip4addr>, Server IP is <ip4addr_server>. String=<string>. Closing connection.
Explanation	The FTP Server requests that the client should connect to another IP

	than its own. This is not allowed, and the connection will be closed.
Firewall Action	close
Recommended Action	The FTP server could be compromised, and should not be trusted.
Revision	1
Parameters	peer ip4addr ip4addr_server string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.109. failed_to_create_connection2 (ID: 00200235)

Default Severity	ERROR
Log Message	FTPALG: Failed to create connection(2) Peer=<peer> Connection=<connection>. String=<string>.
Explanation	An error occured when creating a data connection from the client to server. This could possibly be a result of lack of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	peer connection string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.110. failed_to_create_server_data_connection (ID: 00200236)

Default Severity	ERROR
Log Message	FTPALG: Failed to create server data connection. Peer=<peer> Connection=<connection>
Explanation	An error occured when creating server data connection.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters	peer connection
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.111. failed_to_send_port (ID: 00200237)

Default Severity	WARNING
Log Message	FTPALG: Failed to send port. Peer=<peer>
Explanation	An error occured when trying to send the "PORT" command to the server.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.112. failed_to_register_rawconn (ID: 00200238)

Default Severity	ERROR
Log Message	FTPALG: Internal Error - failed to register eventhandler. Closing connection
Explanation	An internal error occured when registering an eventhandler, and the connection will be closed.
Firewall Action	close
Recommended Action	Contact the support.
Revision	1
Context Parameters	ALG Module Name

2.1.113. failed_to_merge_conns (ID: 00200239)

Default Severity	ERROR
Log Message	FTPALG: Internal Error - failed to merge conns. Closing connection
Explanation	An internal error occured when two connections were being merged into one, and the connection will be closed.

Firewall Action	close
Recommended Action	Contact the support.
Revision	1
Context Parameters	ALG Module Name

2.1.114. max_ftp_sessions_reached (ID: 00200241)

Default Severity	WARNING
Log Message	FTPALG: Maximum number of FTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent FTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of FTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.115. failed_create_new_session (ID: 00200242)

Default Severity	ERROR
Log Message	FTPALG: Failed to create new FTPALG session (out of memory)
Explanation	An attempt to create a new FTPALG session failed, because the unit is out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed FTPALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.116. failure_connect_ftp_server (ID: 00200243)

Default Severity	ERROR
Log Message	FTPALG: Failed to connect to the FTP Server. Closing connection
Explanation	The unit failed to connect to the FTP Server, resulting in that the ALG

session could not be successfully opened.

Firewall Action close

Recommended Action Verify that there is a listening FTP Server on the specified address.

Revision 1

Context Parameters ALG Module Name
ALG Session ID

2.1.117. content_type_mismatch (ID: 00200250)

Default Severity NOTICE

Log Message FTPALG: Content type mismatch in file <filename>. Identified filetype <filetype>

Explanation The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.

Firewall Action data_blocked_control_and_data_channel_closed

Recommended Action None.

Revision 1

Parameters filename
filetype

Context Parameters ALG Module Name
ALG Session ID

2.1.118. failed_to_send_command (ID: 00200251)

Default Severity NOTICE

Log Message FTPALG:Failed to send the command.

Explanation The command sent by the ALG to the server could not be sent.

Firewall Action none

Recommended Action None.

Revision 1

Context Parameters ALG Module Name

2.1.119. resumed_compressed_file_transfer (ID: 00200252)

Default Severity WARNING

Log Message FTPALG: The file <filename> (File type: <filetype>) cannot be sent to

	antivirus scan engine.
Explanation	The data cannot be sent to AVSE for scanning since file transfer begins from within the middle of the file. The scanning process will fail for compressed files.
Firewall Action	data_blocked_control_and_data_channel_closed
Recommended Action	Change fail mode setting to allow, if resumed file transfers of compressed files should be allowed.
Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.120. blocked_filetype (ID: 00200253)

Default Severity	NOTICE
Log Message	FTPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Firewall Action	data_blocked_control_and_data_channel_closed
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.121. resumed_compressed_file_transfer (ID: 00200254)

Default Severity	WARNING
Log Message	FTPALG: The file <filename> (File type: <filetype>) cannot be sent to antivirus scan engine.
Explanation	Decompression module cannot decompress a file that has been resumed. The file is allowed without any further scanning since Fail Mode is Allow.
Firewall Action	allow_data_without_scan
Recommended Action	Update Fail-Mode parameter if the file should be blocked.
Revision	2

Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.122. failed_to_send_response_code (ID: 00200255)

Default Severity	NOTICE
Log Message	FTPALG:Failed to send the response code.
Explanation	The FTP ALG could not send the correct response code to the client.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.123. request_url_redirected (ID: 00200260)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url> redirected to <redirect>. ALG name: <algname>.
Explanation	The request has been redirected.
Firewall Action	allow
Recommended Action	None.
Revision	1
Parameters	redirect url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.124. redirect_page_failed (ID: 00200261)

Default Severity	DEBUG
Log Message	HTTPALG: Failed to send redirect page to client
Explanation	The HTTPALG failed to send a redirect page to the client.

Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	pagetype location send algname
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.125. illegal_command (ID: 00200267)

Default Severity	WARNING
Log Message	FTPALG: REST from <peer> not allowed, rejecting command
Explanation	The client tried to issue a "REST" command, which is not valid since the client is not allowed to do this. The command will be rejected.
Firewall Action	rejecting_command
Recommended Action	If the client should be allowed to do issue "REST" commands, modify the FTPALG configuration.
Revision	1
Parameters	filename peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.126. https_not_allowed (ID: 00200270)

Default Severity	ERROR
Log Message	HTTPS protocol is not allowed.
Explanation	Policy does not allow the HTTPS protocol.
Firewall Action	block
Recommended Action	Reconfigure the service to allow HTTPS if it should be allowed.
Revision	2
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.127. http_not_allowed (ID: 00200271)

Default Severity	ERROR
Log Message	HTTP protocol is not allowed.
Explanation	Policy does not allow the HTTP protocol.
Firewall Action	block
Recommended Action	Reconfigure the service to allow HTTP if it should be allowed.
Revision	2
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.128. clienthello_server_name (ID: 00200272)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: HTTPS (c) Found server DNS name <hostname> in ClientHello datagram
Explanation	Found DNS server DNS name in ClientHello datagram.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	hostname algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.129. invalid_clienthello (ID: 00200273)

Default Severity	ERROR
Log Message	HTTPALG: HTTPS (c) Failed to parse ClientHello datagram (<cause>).
Explanation	Failed to parse ClientHello datagram.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters	cause algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.130. invalid_clienthello (ID: 00200274)

Default Severity	ERROR
Log Message	HTTPALG: HTTPS (c) Failed to parse ClientHello datagram.
Explanation	Failed to parse ClientHello datagram.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.131. invalid_clienthello_server_name (ID: 00200275)

Default Severity	ERROR
Log Message	HTTPALG: HTTPS (s) Failed to parse SNI server name from ClientHello SNI extension (<cause>).
Explanation	Failed to parse SNI server name from ClientHello SNI extension.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	cause algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.132. invalid_clienthello_server_name (ID: 00200276)

Default Severity	ERROR
Log Message	HTTPALG: HTTPS (s) Failed to parse SNI server name from ClientHello

	SNI extension.
Explanation	Failed to parse SNI server name from ClientHello SNI extension.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.133. certificate_server_name (ID: 00200277)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: HTTPS (s) Found server DNS name <hostname> in Certificate datagram
Explanation	Found server DNS name in Certificate datagram.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	hostname algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.134. invalid_certificate (ID: 00200278)

Default Severity	ERROR
Log Message	HTTPALG: HTTPS (s) Failed to parse Certificate datagram (<cause>).
Explanation	Failed to parse Certificate datagram.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	cause algname
Context Parameters	ALG Module Name ALG Session ID

Connection

2.1.135. invalid_certificate (ID: 00200279)

Default Severity	ERROR
Log Message	HTTPALG: HTTPS (s) Failed to parse Certificate datagram.
Explanation	Failed to parse Certificate datagram.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.136. blacklisted_url_blocked (ID: 00200280)

Default Severity	NOTICE
Log Message	HTTPALG: HTTPS (c) Blacklisted URL <hostname> blocked
Explanation	Connection to blaclisted URL closed.
Firewall Action	close
Recommended Action	If the connection is to be allowed, update the URL filter to include the hostname as whilelisted.
Revision	1
Parameters	hostname algname
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.137. unknown_state (ID: 00200300)

Default Severity	WARNING
Log Message	H323ALG: H.225 parser is in unknown state
Explanation	The H.225 parser failed to parse the H.225 message. The ALG session will be closed.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	peer state
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.138. invalid_message (ID: 00200301)

Default Severity	WARNING
Log Message	H323ALG: An invalid message was received from peer
Explanation	An invalid message was received from the peer. The ALG session will be closed.
Firewall Action	closing_session
Recommended Action	None.
Revision	2
Parameters	peer message state
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.139. decode_failed (ID: 00200302)

Default Severity	WARNING
Log Message	H323ALG: Decoding of message from peer failed. Closing session
Explanation	The H.225 parser failed to decode the H.225 message. The ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.140. encode_failed (ID: 00200303)

Default Severity	WARNING
Log Message	H323ALG: Encoding of message from peer failed. Closing session
Explanation	The ASN.1 encoder failed to encode the message. The ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.141. encode_failed (ID: 00200304)

Default Severity	WARNING
Log Message	H323ALG: Failed before encoding message from peer. Closing session
Explanation	The ASN.1 encoder failed to allocate memory used for encoding of the message. The ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.142. encode_failed (ID: 00200305)

Default Severity	WARNING
Log Message	H323ALG: Failed after encoding message from peer. Closing session
Explanation	The ASN.1 encoder failed to encode the message properly. The ALG session will be closed.

Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.143. decode_failed (ID: 00200306)

Default Severity	WARNING
Log Message	H323ALG: Failed before encoding H.245 message. Closing connection
Explanation	The H.245 encoder failed to allocate memory used for encoding of the message. The ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.144. encode_failed (ID: 00200307)

Default Severity	WARNING
Log Message	H323ALG: Failed after encoding H.245 message. Closing connection
Explanation	The H.245 encoder failed to encode the message. The ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.145. max_tcp_data_connections_exceeded (ID: 00200308)

Default Severity	WARNING
Log Message	H323ALG: Maximum number of TCP data channels exceeded
Explanation	The maximum number of concurrent TCP data channels has been reached for this session.
Firewall Action	None
Recommended Action	If the maximum number of TCP data channels per session is too low, increase it.
Revision	1
Parameters	max_channels
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.146. max_connections_per_call_exceeded (ID: 00200309)

Default Severity	WARNING
Log Message	H323ALG: No more connections allowed for this call
Explanation	The maximum number of concurrent logical channels (calls) has been reached for this session.
Firewall Action	None
Recommended Action	If the maximum number of concurrent logical channels (calls) per session is too low, increase it.
Revision	1
Parameters	max_connections
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.147. ignoring_channel (ID: 00200310)

Default Severity	WARNING
Log Message	H323ALG: Ignoring mediaChannel info in openLogicalChannel
Explanation	Media channel information in the openLogicalChannel message is not handled.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.148. com_mode_response_message_not_translated (ID: 00200311)

Default Severity	WARNING
Log Message	H323ALG: CommunicationModeResponse not translated.
Explanation	The H.245 Communication Mode Response message is not translated.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.149. max_h323_session_reached (ID: 00200312)

Default Severity	WARNING
Log Message	H323ALG: Maximum number of H.323 sessions (<max_sessions>) for service reached. Closing connection.
Explanation	The maximum number of concurrent H.323 sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of H.323 session is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.150. failed_create_new_session (ID: 00200313)

Default Severity	WARNING
Log Message	H323ALG: Failed to create new H.323 session (out of memory)
Explanation	Could not create a new H.323 session due to lack of memory. No more sessions can be created unless the system increases the amount of free memory.
Firewall Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.151. max_h323_gk_sessions_reached (ID: 00200314)

Default Severity	WARNING
Log Message	H323ALG: Maximum number of H.323 gatekeeper sessions for service reached
Explanation	The maximum number of concurrent H.323 gatekeeper sessions has been reached for this service. Connection will be closed.
Firewall Action	close
Recommended Action	If the maximum number of concurrent H.323 gatekeeper sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.152. failed_create_new_session (ID: 00200315)

Default Severity	WARNING
Log Message	H323ALG: Failed to create new gatekeeper session (out of memory)
Explanation	Could not create a new H.323 gatekeeper session due to lack of memory. No more sessions can be created unless the system increases the amount of free memory.
Firewall Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.153. failure_connect_h323_server (ID: 00200316)

Default Severity	ERROR
Log Message	H323ALG: Failed to connect to the H.323 Server. Closing connection
Explanation	The unit failed to connect to the H.323 Server, resulting in that the ALG session could not open successfully.
Firewall Action	close
Recommended Action	Verify that there is a listening H.323 Server on the specified address.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.154. com_mode_command_message_not_translated (ID: 00200317)

Default Severity	WARNING
Log Message	H323ALG: CommunicationModeCommand not translated.
Explanation	The H.245 Communication Mode Command message is not translated.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.155. packet_failed_initial_test (ID: 00200350)

Default Severity	WARNING
Log Message	TFTPALG: Packet failed initial test (Invalid TFTP packet). Packet length <packet_length>
Explanation	An invalid TFTP packet was received. Refusing connection.
Firewall Action	reject
Recommended Action	None.
Revision	1

Parameters	packet_length
Context Parameters	ALG Module Name Connection

2.1.156. packet_failed_traversal_test (ID: 00200351)

Default Severity	WARNING
Log Message	TFTPALG: Filename <filename> failed test for directory traversal
Explanation	Filename failed test for directory traversal (contains invalid characters).Closing connection.
Firewall Action	reject
Recommended Action	If all characters in filenames should be allowed modify the TFTP Alg configuration.
Revision	1
Parameters	filename
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.157. command_not_allowed (ID: 00200353)

Default Severity	WARNING
Log Message	TFTPALG: <command> command not allowed
Explanation	Command (GET or PUT) not allowed. Closing connection.
Firewall Action	reject
Recommended Action	If command should be allowed modify the TFTP Alg configuration.
Revision	1
Parameters	command
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.158. option_value_invalid (ID: 00200354)

Default Severity	WARNING
Log Message	TFTPALG: Option <option> contained invalid value <value>
Explanation	Option contained invalid value.Closing connection.

Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	option value
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.159. option_value_invalid (ID: 00200355)

Default Severity	WARNING
Log Message	TFTPALG: Option <option> contained no readable value
Explanation	Option contained no readable value.Closing connection.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.160. option_tsize_invalid (ID: 00200356)

Default Severity	WARNING
Log Message	TFTPALG: Option tsize value <value> exceeding allowed max value <maxvalue>
Explanation	Option tsize value exceeding allowed value.Closing connection.
Firewall Action	reject
Recommended Action	If connection should be allowed modify the filetransfersize of the TFTP Alg configuration .
Revision	1
Parameters	value maxvalue
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.161. unknown_option_blocked (ID: 00200357)

Default Severity	WARNING
Log Message	TFTPALG: Request contained unknown option <option>
Explanation	Request contained unknown option.Closing connection.
Firewall Action	reject
Recommended Action	If connection should be allowed modify the TFTP Alg configuration .
Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.162. option_tsize_invalid (ID: 00200358)

Default Severity	WARNING
Log Message	TFTPALG: Option tsize value <value> exceeding allowed value <maxvalue>
Explanation	Option tsize value exceeding allowed value.Closing connection.
Firewall Action	close
Recommended Action	If connection should be allowed modify the filetransfersize of the TFTP Alg configuration .
Revision	1
Parameters	value maxvalue
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.163. unknown_option_blocked (ID: 00200359)

Default Severity	WARNING
Log Message	TFTPALG: Request contained unknown option <option>
Explanation	Request contained unknown option.Closing connection.
Firewall Action	close
Recommended Action	If connection should be allowed modify the TFTP Alg configuration .

Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.164. option_not_sent (ID: 00200360)

Default Severity	WARNING
Log Message	TFTPALG: The received option <option> was not sent
Explanation	The received option was not sent.Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.165. option_value_invalid (ID: 00200361)

Default Severity	WARNING
Log Message	TFTPALG: Option <option> contained invalid value <value> or option not sent
Explanation	Option contained invalid value or option not sent.Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	option value
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.166. option_value_invalid (ID: 00200362)

Default Severity	WARNING

Log Message	TFTPALG: Option <option> contained no readable value
Explanation	Option contained no readable value.Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.167. blksize_out_of_range (ID: 00200363)

Default Severity	WARNING
Log Message	TFTPALG: Option blksize value <old_blksize> exceeding allowed value. Rewriting to <new_blksize>
Explanation	Option blksize value exceeding allowed value.Rewriting value.
Firewall Action	rewrite
Recommended Action	If the value should be allowed modify the TFTP Alg configuration.
Revision	1
Parameters	old_blksize new_blksize
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.168. max_tftp_sessions_reached (ID: 00200364)

Default Severity	WARNING
Log Message	FTPALG: Maximum number of TFTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent TFTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of TFTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions

Context Parameters	ALG Module Name

2.1.169. failed_create_new_session (ID: 00200365)

Default Severity	ERROR
Log Message	TFTPALG: Failed to create new TFTPALG session (out of memory)
Explanation	An attempt to create a new TFTPALG session failed, because the unit is out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed TFTPALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.170. invalid_packet_received (ID: 00200366)

Default Severity	WARNING
Log Message	TFTPALG: Received invalid packet Opcode <opcode> Packet length <packet_length>
Explanation	Received invalid packet.Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.171. failed_create_connection (ID: 00200367)

Default Severity	ERROR
Log Message	TFTPALG: Failed to create listening connection,internal error(<error_code>). Closing session
Explanation	The unit failed to create listening connection, resulting in that the ALG session could not be successfully opened.
Firewall Action	close

Recommended Action	None.
Revision	1
Parameters	error_code
Context Parameters	ALG Module Name ALG Session ID

2.1.172. invalid_packet_received_reopen (ID: 00200368)

Default Severity	WARNING
Log Message	TFTPALG: Received invalid packet Opcode <opcode> Packet length <packet_length>
Explanation	Received invalid packet.Closing listening connection and opening new instead.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.173. packet_out_of_sequence (ID: 00200369)

Default Severity	WARNING
Log Message	TFTPALG: Received packet out of sequence opcode <opcode> packet length <packet_length>
Explanation	Received packet out of sequence.Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.174. transfer_size_exceeded (ID: 00200370)

Default Severity	WARNING
Log Message	TFTPALG: Received bytes <received> exceeding allowed max value <maxvalue>
Explanation	Transferred bytes exceeding allowed value.Closing connection.
Firewall Action	close
Recommended Action	If connection should be allowed modify the filetransfersize option of the TFTP Alg configuration .
Revision	1
Parameters	received maxvalue
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.175. options_removed (ID: 00200371)

Default Severity	WARNING
Log Message	TFTPALG: Options not allowed. Stripping options from packet
Explanation	Options not allowed. Stripping options from packet.
Firewall Action	rewrite
Recommended Action	If options should be allowed modify the TFTP Alg configuration.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.176. failed_strip_option (ID: 00200372)

Default Severity	ERROR
Log Message	TFTPALG: Failed to strip options , (internal error)
Explanation	An attempt to send request packet without options failed because of an internal error.
Firewall Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.177. failed_create_connection (ID: 00200373)

Default Severity	ERROR
Log Message	TFTPALG: Failed to create listening connection,internal error(<error_code>). Closing session
Explanation	The unit failed to create listening connection, resulting in that the ALG session could not be successfully opened.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	error_code
Context Parameters	ALG Module Name

2.1.178. invalid_error_message_received (ID: 00200374)

Default Severity	WARNING
Log Message	TFTPALG: Received invalid error message Opcode <opcode> Packet length <packet_length>
Explanation	Received invalid error message.Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.179. max_pop3_sessions_reached (ID: 00200380)

Default Severity	WARNING
Log Message	POP3ALG: Maximum number of POP3 sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent POP3 sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close

Recommended Action	If the maximum number of POP3 sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.180. failed_create_new_session (ID: 00200381)

Default Severity	WARNING
Log Message	POP3ALG: Failed to create new POP3ALG session (out of memory)
Explanation	An attempt to create a new POP3ALG session failed, because the unit is out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed POP3ALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.181. failed_connect_pop3_server (ID: 00200382)

Default Severity	ERROR
Log Message	POP3ALG: Failed to connect to the POP3 Server. Closing the connection.
Explanation	The unit failed to connect to the remote POP3 Server, resulting in that the ALG session could not be successfully opened.
Firewall Action	close
Recommended Action	Verify that there is a listening POP3 Server on the specified address.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.182. out_of_memory (ID: 00200383)

Default Severity	ERROR
Log Message	POP3ALG: Failed to allocate memory (out of memory)
Explanation	An attempt to allocate memory failed.
Firewall Action	close

Recommended Action	Try to free up unwanted memory.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.183. blocked_filetype (ID: 00200384)

Default Severity	NOTICE
Log Message	POP3ALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Firewall Action	block
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	1
Parameters	filename filetype sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.184. response_blocked_unknown (ID: 00200385)

Default Severity	WARNING
Log Message	POP3ALG: Response blocked.Invalid response=<response>
Explanation	The server is sending unknown response. The response will be blocked.
Firewall Action	block
Recommended Action	None.
Revision	1
Parameters	command" response
Context Parameters	ALG Module Name ALG Session ID

2.1.185. base64_decode_failed (ID: 00200386)

Default Severity	ERROR

Log Message	POP3ALG: Base 64 decode failed. Attachment blocked
Explanation	The data sent to Base64 decoding failed. This can occur if the email sender sends incorrectly formatted data. The attachment has been blocked.
Firewall Action	block_data
Recommended Action	Research how the sender is encoding the data.
Revision	1
Parameters	filename filetype sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.186. possible_invalid_mail_end (ID: 00200387)

Default Severity	WARNING
Log Message	POP3ALG: Possible invalid end of mail "\\n.\\n" received.
Explanation	The client is sending possible invalid end of mail.
Firewall Action	allow
Recommended Action	Research how the client is sending possible invalid end of mail.
Revision	1
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.187. command_blocked_invalid_len (ID: 00200388)

Default Severity	WARNING
Log Message	POP3ALG: Command line blocked,line begins with linebegin. Invalid line length <len>
Explanation	The client is sending command with invalid command length. The command will be blocked.
Firewall Action	block
Recommended Action	None.
Revision	1
Parameters	len linebegin"

Context Parameters	ALG Module Name ALG Session ID

2.1.188. response_blocked_invalid_len (ID: 00200389)

Default Severity	WARNING
Log Message	POP3ALG: Response blocked.Invalid response length <len>
Explanation	The server is sending response with invalid response length. The response will be blocked.
Firewall Action	block
Recommended Action	None.
Revision	1
Parameters	command" len
Context Parameters	ALG Module Name ALG Session ID

2.1.189. content_type_mismatch (ID: 00200390)

Default Severity	NOTICE
Log Message	POP3ALG: Content type mismatch in file <filename>. Identified filetype <filetype>
Explanation	The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.
Firewall Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename filetype sender_email_address
Context Parameters	ALG Module Name

2.1.190. content_type_mismatch_mimecheck_disabled (ID: 00200391)

Default Severity	NOTICE
Log Message	POP3ALG: Content type mismatch found for the file <filename>. It is identified as type <filetype> file

Explanation	Received type of data in the packet and its actual type do not match. As there is a mismatch and mime type check is disabled, the data will be allowed.
Firewall Action	allow
Recommended Action	Content type should be matched.
Revision	2
Parameters	filename filetype sender_email_address
Context Parameters	ALG Module Name

2.1.191. command_blocked_invalid_argument (ID: 00200392)

Default Severity	WARNING
Log Message	POP3ALG: Command blocked.Invalid argument <argument> given
Explanation	The client is sending command with invalid argument. The command will be blocked.
Firewall Action	block
Recommended Action	None.
Revision	1
Parameters	command" argument
Context Parameters	ALG Module Name ALG Session ID

2.1.192. command_blocked (ID: 00200393)

Default Severity	WARNING
Log Message	POP3ALG: Command <command> blocked.
Explanation	The client is sending command that are not allowed. The command will be blocked.
Firewall Action	block
Recommended Action	If the command are to be allowed change the Alg configuration.Note: The STLS command is allways blocked!.
Revision	1
Parameters	command
Context Parameters	ALG Module Name ALG Session ID

2.1.193. unknown_command_blocked (ID: 00200394)

Default Severity	WARNING
Log Message	POP3ALG: Unknown command blocked.
Explanation	The client is sending unknown command. The command will be blocked.
Firewall Action	block
Recommended Action	If the command are to be allowed change the Alg configuration.
Revision	1
Parameters	command"
Context Parameters	ALG Module Name ALG Session ID

2.1.194. unexpected_mail_end (ID: 00200396)

Default Severity	WARNING
Log Message	POP3ALG: Unexpected end of mail received while parsing mail content.
Explanation	Unexpected end of mail received while parsing mail content..
Firewall Action	block
Recommended Action	Research if mail is not complete.
Revision	1
Parameters	sender_email_address len retrigs
Context Parameters	ALG Module Name ALG Session ID

2.1.195. invalid_line_endings (ID: 00200397)

Default Severity	WARNING
Log Message	POP3ALG: Mail contains invalid line endings.
Explanation	Mail contains invalid line endings.
Firewall Action	block
Recommended Action	Research why mail contains invalid line endings.
Revision	1

Context Parameters	ALG Module Name ALG Session ID

2.1.196. top_mail_end_blocked (ID: 00200398)

Default Severity	WARNING
Log Message	POP3ALG: The last part of mail retreived with TOP command blocked.
Explanation	Only part of mail retrieved using TOP command was received. The last part was therefore blocked by the firewall.
Firewall Action	block
Recommended Action	None.
Revision	1
Parameters	len retrigs
Context Parameters	ALG Module Name ALG Session ID

2.1.197. max_syslog_sessions_reached (ID: 00200400)

Default Severity	WARNING
Log Message	SyslogALG: Maximum number of sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent syslog ALG sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of syslog sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.198. out_of_memory (ID: 00200401)

Default Severity	CRITICAL
Log Message	SYSLOGALG: Failed to allocate memory
Explanation	The unit does not have enough available RAM.

Firewall Action	none
Recommended Action	Try to free up some RAM by changing configuration parameters.
Revision	1
Context Parameters	ALG Module Name Connection

2.1.199. unauthenticated_syslog_detected (ID: 00200402)

Default Severity	ERROR
Log Message	SYSLOGALG: Unauthenticated session
Explanation	Syslog packet rejected due to unauthenticated connection.
Firewall Action	drop
Recommended Action	Investigate the reason to the unauthenticated syslog packets or change the configuration to allow unauthenticated packets.
Revision	1
Context Parameters	ALG Module Name

2.1.200. reverse_syslog_data (ID: 00200403)

Default Severity	ERROR
Log Message	SYSLOGALG: Reverse traffic detected on syslog connection
Explanation	The SYSLOG ALG detected data packets send in the reverse direction i.e from the server towards the client. The session is closed. .
Firewall Action	close
Recommended Action	Investigate why the packets are sent in the reverse direction of the syslog connection.
Revision	1
Context Parameters	ALG Module Name Connection

2.1.201. large_syslog_received (ID: 00200404)

Default Severity	ERROR
Log Message	SYSLOGALG: Too large syslog packet received <size>
Explanation	Syslog packet rejected due to being larger than the configuration allows.

Firewall Action	drop
Recommended Action	If required, change the configuration to allow syslog packets with this size.
Revision	1
Parameters	size limit
Context Parameters	ALG Module Name Connection

2.1.202. prohibited_text_detected (ID: 00200405)

Default Severity	ERROR
Log Message	SYSLOGALG: Prohibited text <text> detected
Explanation	Syslog packet rejected due to presence of prohibited text.
Firewall Action	drop
Recommended Action	Change the configuration to allow syslog packets with this text.
Revision	1
Parameters	text
Context Parameters	ALG Module Name Connection

2.1.203. internal_buffer_error (ID: 00200406)

Default Severity	ERROR
Log Message	SYSLOGALG: Internal buffer error
Explanation	Crafted syslog packet grew too large for internal buffer.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name Connection

2.1.204. max_tls_sessions_reached (ID: 00200450)

Default Severity	WARNING
Log Message	TLSALG: Maximum number of TLS sessions (<max_sessions>) for

	service reached. Closing connection
Explanation	The maximum number of concurrent TLS sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of TLS sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.205. failed_create_new_session (ID: 00200451)

Default Severity	WARNING
Log Message	TLSALG: Failed to create new TLSALG session (out of memory)
Explanation	An attempt to create a new TLSALG session failed, because the unit is out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed TLSALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.206. failure_connect_http_server (ID: 00200452)

Default Severity	ERROR
Log Message	TLSALG: Failed to connect to the HTTP Server. Closing connection. ALG name: <algname>.
Explanation	The unit failed to connect to the HTTP Server, resulting in that the ALG session could not be successfully opened.
Firewall Action	close
Recommended Action	Verify that there is a listening HTTP Server on the specified address.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.207. tls_alert_received (ID: 00200453)

Default Severity	ERROR
Log Message	TLSALG: Received TLS <alert> alert from peer.
Explanation	A TLS alert was received. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	alert level algname
Context Parameters	ALG Module Name ALG Session ID

2.1.208. tls_renegotiation_attempted (ID: 00200454)

Default Severity	WARNING
Log Message	TLSALG: TLS renegotiation attempted but not supported.
Explanation	The TLS peer initiated a renegotiation. Renegotiation is however not supported so an alert was sent to let the peer know that there will be no renegotiation.
Firewall Action	tls_alert_sent
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.209. tls_alert_sent (ID: 00200455)

Default Severity	ERROR
Log Message	TLSALG: Sent TLS <alert> alert to peer.
Explanation	A TLS error has occured that caused an alert to be sent to the peer. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.

Revision	1
Parameters	alert level algname
Context Parameters	ALG Module Name ALG Session ID

2.1.210. tls_cipher_suite_certificate_mismatch (ID: 00200456)

Default Severity	ERROR
Log Message	TLSALG: The negotiated cipher suite can not be used with the configured certificate.
Explanation	The negotiated cipher suite, which is an exportable cipher suite, does not permit using the certificate's key to perform the key exchange. The certificate can not be sent and the TLS ALG session will be closed.
Firewall Action	close
Recommended Action	Change cipher suites and/or certificate.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.211. ssl_renegotiation_attempted (ID: 00200457)

Default Severity	ERROR
Log Message	TLSALG: SSL renegotiation attempted but not supported.
Explanation	The SSL peer initiated a renegotiation. Renegotiation is however not supported so the TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.212. tls_disallowed_key_exchange (ID: 00200458)

Default Severity	WARNING
Log Message	TLSALG: Disallowed key exchange.
Explanation	The TLS ALG session will be closed because there are not enough resources to process any TLS key exchanges at the moment. This could be a result of TLS handshake message flooding. This action is triggered by a system that monitors the amount of resources that is spent on key exchanges. This system is controlled by the advanced setting SSL_ProcessingPriority.
Firewall Action	close
Recommended Action	Investigate the source of this, and try to find out if it is a part of a possible attack, or normal traffic.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.213. tls_invalid_message (ID: 00200459)

Default Severity	ERROR
Log Message	TLSALG: Invalid TLS <message_type> message received.
Explanation	A badly formatted TLS message has been received. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	message_type algname
Context Parameters	ALG Module Name ALG Session ID

2.1.214. tls_bad_message_order (ID: 00200460)

Default Severity	ERROR
Log Message	TLSALG: Bad TLS handshake message order.
Explanation	A TLS handshake message of a type that is not expected in the current state of the handshake was received. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.

Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.215. tls_no_shared_cipher_suites (ID: 00200461)

Default Severity	WARNING
Log Message	TLSALG: No shared cipher suites.
Explanation	A connecting TLS peer does not share any cipher suites with the unit. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	Make sure that the client and the unit share atleast one cipher suite.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.216. tls_out_of_memory (ID: 00200462)

Default Severity	ERROR
Log Message	TLSALG: Out of memory.
Explanation	The unit was unable to allocate the memory required to process the TLS connection of a TLS ALG session. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.217. tls_failed_to_verify_finished (ID: 00200463)

Default Severity	ERROR
Log Message	TLSALG: Failed to verify finished message.

Explanation	The unit failed to verify the TLS finished message. The finished message is used to verify that the key exchange and authentication processes were successful. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.218. unknown_tls_error (ID: 00200464)

Default Severity	ERROR
Log Message	TLSALG: Unknown TLS error.
Explanation	An unknown TLS error has occured. The TLS ALG session will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.219. sdp_message_parsing_failed (ID: 00200501)

Default Severity	ERROR
Log Message	SIPALG: SDP message parsing failed
Explanation	SDP part of message failed parsing due to malformed message. Reason: [reason].
Firewall Action	drop
Recommended Action	Examine why client or server is sending a malformed SDP message.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport

Context Parameters ALG Module Name

2.1.220. sdp_message_validation_failed (ID: 00200502)

Default Severity ERROR

Log Message SIPALG: SDP message validation failed

Explanation SDP part of message failed validation due to malformed message. Reason: [reason].

Firewall Action drop

Recommended Action Examine why client or server is sending a malformed SDP message.

Revision 2

Parameters
reason
from_uri
to_uri
srcip
srcport
destip
destport

Context Parameters ALG Module Name

2.1.221. sip_message_parsing_failed (ID: 00200503)

Default Severity ERROR

Log Message SIPALG: SIP message parsing failed

Explanation SIP part of message failed parsing due to malformed message. Reason: [reason].

Firewall Action drop

Recommended Action Examine why client or server is sending a malformed SIP message.

Revision 2

Parameters
reason
from_uri
to_uri
srcip
srcport
destip
destport

Context Parameters ALG Module Name

2.1.222. sip_message_validation_failed (ID: 00200504)

Default Severity	ERROR
Log Message	SIPALG: SIP message validation failed due to malformed message
Explanation	SIP part of message failed validation due to malformed message. Reason: [reason].
Firewall Action	drop
Recommended Action	Examine why client or server is sending a malformed SIP message.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.223. max_sessions_per_uri_reached (ID: 00200505)

Default Severity	WARNING
Log Message	SIPALG: Maximum number of sessions per SIP URI has been reached
Explanation	The configured maximum number of concurrent SIP sessions [max_ses_per_id] per SIP URI has been reached.
Firewall Action	close
Recommended Action	If the maximum number of SIPALG sessions per SIP URI is too low, increase it.
Revision	2
Parameters	max_ses_per_id from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.224. registration_hijack_detected (ID: 00200506)

Default Severity	ALERT
Log Message	Registration hijack attempt detected
Explanation	The number of registration attempts [reg_hijack_count] has been

	exceeded.
Firewall Action	drop
Recommended Action	Check with the user, why he is using false authentication to register.
Revision	2
Parameters	reg_hijack_count from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.225. sip_signal_timeout (ID: 00200507)

Default Severity	WARNING
Log Message	SIPALG: SIP signal timeout
Explanation	SIP signal timeout for session [method]. The session will be deleted.
Firewall Action	close
Recommended Action	If the configured SIP signal timeout value is too low, increase it.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.226. sip_request_response_timeout (ID: 00200508)

Default Severity	WARNING
Log Message	SIPALG: SIP request-response timeout
Explanation	SIP request-response timeout for the session [method]. The session will be deleted.
Firewall Action	close
Recommended Action	If the configured SIP Request-Response timeout value is too low, increase it.

Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.227. registration_time_modified (ID: 00200509)

Default Severity	NOTICE
Log Message	SIPALG: Expire value modified in registration request
Explanation	The SIP-ALG modified the requested registration time since it exceeds the configured maximum registration time value [cfg_registration_time].
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	cfg_registration_time from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.228. unsuccessful_registration (ID: 00200510)

Default Severity	WARNING
Log Message	SIPALG: Unsuccessful registration
Explanation	The user failed to register. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip

	srcport destip destport
Context Parameters	ALG Module Name

2.1.229. unsuccessful_unregistration (ID: 00200511)

Default Severity	NOTICE
Log Message	SIPALG: Failed unregistration
Explanation	The user failed to unregister. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name ALG Session ID

2.1.230. unsuccessful_search_in_registration_table (ID: 00200512)

Default Severity	WARNING
Log Message	SIPALG: Registration entry not found
Explanation	The specified user could not be found in the register table. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.231. sipalg_session_created (ID: 00200513)

Default Severity	NOTICE
Log Message	SIPALG: New SIP-ALG session created
Explanation	New SIP-ALG session for [method] request created.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.232. failed_to_create_session (ID: 00200514)

Default Severity	ERROR
Log Message	SIPALG: Failed to create sipalg session
Explanation	A new SIP-ALG session for [method] request could not be created.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.233. failed_to_find_session (ID: 00200515)

Default Severity	ERROR
Log Message	SIPALG: Failed to find sipalg session

Explanation	Failed to find sipalg session. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.234. sipalg_session_deleted (ID: 00200516)

Default Severity	INFORMATIONAL
Log Message	SIPALG: SIP-ALG session deleted
Explanation	SIP-ALG session deleted for [method] request.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.235. sipalg_session_state_updated (ID: 00200517)

Default Severity	DEBUG
Log Message	SIPALG: SIP-ALG session state updated
Explanation	The SIP-ALG session state updated to [session_state] state.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	session_state

	from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.236. sipalg_transaction_created (ID: 00200520)

Default Severity	NOTICE
Log Message	SIPALG: Transaction created
Explanation	SIP-ALG transaction created for [method] request.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.237. failed_to_create_new_transaction (ID: 00200521)

Default Severity	ERROR
Log Message	SIPALG: Failed to create transaction
Explanation	The SIP-ALG failed to create transaction for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.238. failed_to_find_transaction (ID: 00200522)

Default Severity	WARNING
Log Message	SIPALG: Failed to find transaction
Explanation	Failed to find transaction for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.239. sipalg_transaction_deleted (ID: 00200523)

Default Severity	NOTICE
Log Message	SIPALG: sipalg transaction deleted
Explanation	The transaction for [method] request is deleted.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name ALG Session ID

2.1.240. sipalg_transaction_state_updated (ID: 00200524)

Default Severity	DEBUG
Log Message	SIPALG: Transaction state updated

Explanation	A SIP-ALG transaction state has been updated to [transaction_state] state.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	transaction_state from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.241. no_route_found (ID: 00200526)

Default Severity	ERROR
Log Message	SIPALG: Failed to find route for given host
Explanation	No route information found for the given host. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.242. failed_to_get_free_port (ID: 00200527)

Default Severity	CRITICAL
Log Message	SIPALG: Failed to get free NAT port pair for the given host
Explanation	Failed to get free port for the given host. Reason: [reason].
Firewall Action	drop
Recommended Action	The system is unstable and might require a reboot.
Revision	2

Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.243. failed_to_find_role (ID: 00200528)

Default Severity	ERROR
Log Message	SIPALG: Failed to find role
Explanation	SIPALG: Failed to find role for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.244. failed_to_update_port (ID: 00200529)

Default Severity	ERROR
Log Message	SIPALG: Failed to update port information
Explanation	Failed to update port into session for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport

Context Parameters ALG Module Name

2.1.245. failed_to_update_contact (ID: 00200530)

Default Severity ERROR

Log Message SIPALG: Failed to update contact

Explanation Failed to update contact into session for [method] request.

Firewall Action drop

Recommended Action None.

Revision 2

Parameters
method
from_uri
to_uri
srcip
srcport
destip
destport

Context Parameters ALG Module Name

2.1.246. failed_to_modify_sdp_message (ID: 00200531)

Default Severity ERROR

Log Message SIPALG: Failed to modify SDP message

Explanation Failed to modify SDP part of message. Reason: [reason].

Firewall Action drop

Recommended Action None.

Revision 2

Parameters
reason
from_uri
to_uri
srcip
srcport
destip
destport

Context Parameters ALG Module Name

2.1.247. failed_to_modify_via (ID: 00200532)

Default Severity ERROR

Log Message	SIPALG: Failed to modify via in message
Explanation	Failed to modify the via header in message for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.248. failed_to_modify_from (ID: 00200533)

Default Severity	ERROR
Log Message	SIPALG: Failed to modify FROM tag in message
Explanation	Failed to modify the FROM tag in message for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.249. failed_to_modify_request_uri (ID: 00200534)

Default Severity	ERROR
Log Message	SIPALG: Failed to modify request URI in message
Explanation	Failed to modify the request URI in message for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2

Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.250. failed_to_modify_request (ID: 00200535)

Default Severity	ERROR
Log Message	SIPALG: Failed to modify the request
Explanation	Failed to modify the topology info in the [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.251. method_not_supported (ID: 00200536)

Default Severity	WARNING
Log Message	SIPALG: Method not supported
Explanation	The method [method] is not supported.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport

Context Parameters	ALG Module Name

2.1.252. general_error (ID: 00200537)

Default Severity	WARNING
Log Message	SIPALG: General Error
Explanation	General error while processing message. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.253. third_party_call_control (ID: 00200538)

Default Severity	WARNING
Log Message	SIPALG: Block third party SIP request
Explanation	The SIP-ALG has detected a SIP/SDP message involving third party IP address. Reason: [reason]. The request will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.254. out_of_memory (ID: 00200539)

Default Severity	EMERGENCY
Log Message	SIPALG: Out of memory
Explanation	Memory allocation failed while processing SIP message.
Firewall Action	drop
Recommended Action	Change configuration to free up more RAM.
Revision	1
Parameters	message

2.1.255. null_sip_message_received (ID: 00200540)

Default Severity	ERROR
Log Message	SIPALG: SIP packet reception error. Reason:<reason>
Explanation	Packet without data received.
Firewall Action	drop
Recommended Action	Research how SIPALG received NULL SIP packet.
Revision	1
Parameters	reason
Context Parameters	ALG Module Name

2.1.256. user_registered (ID: 00200541)

Default Severity	NOTICE
Log Message	SIPALG: Successful Registration
Explanation	User [user_name] registered.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	user_name contact
Context Parameters	ALG Module Name

2.1.257. user_unregistered (ID: 00200542)

Default Severity	NOTICE

Log Message	SIPALG: Successful unregistration
Explanation	User [user_name] unregistered successfully.
Firewall Action	allow
Recommended Action	None.
Revision	1
Parameters	user_name contact
Context Parameters	ALG Module Name

2.1.258. dns_resolution_failed (ID: 00200545)

Default Severity	CRITICAL
Log Message	Failed to do dns resolve
Explanation	An attempt to resolve dns failed. Reason: [reason].
Firewall Action	drop
Recommended Action	Check if the dns servers are configured.
Revision	1
Parameters	reason
Context Parameters	ALG Module Name

2.1.259. failed_to_modify_contact (ID: 00200547)

Default Severity	ERROR
Log Message	SIPALG: Failed to modify contact tag in message
Explanation	Failed to modify the contact tag in SIP message. Reason: [reason].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	reason from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.260. invalid_udp_packet (ID: 00200548)

Default Severity	ERROR
Log Message	SIPALG: Invalid SIP UDP packet received
Explanation	The SIP ALG received an invalid UDP packet. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.261. failed_to_parse_media (ID: 00200549)

Default Severity	ERROR
Log Message	SIPALG: Failed to parse media
Explanation	Failed to parse media for the request [method].
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.262. max_session_per_service_reached (ID: 00200550)

Default Severity	WARNING
Log Message	SIPALG: Maximum number of transaction per session has been reached
Explanation	The configured maximum number of concurrent SIP sessions [max_ses_per_service] per SIP SERVICE has been reached.
Firewall Action	close
Recommended Action	If the maximum number of SIPALG sessions per SIP service is too

	low, increase it.
Revision	2
Parameters	max_ses_per_service from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.263. max_tsxn_per_session_reached (ID: 00200551)

Default Severity	WARNING
Log Message	SIPALG: Maximum number of sessions per Service has been reached
Explanation	The configured maximum number of transaction [max_tsxn_per_session] per SIP SESSION has been reached.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	max_tsxn_per_session from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.264. invalid_transaction_state (ID: 00200552)

Default Severity	ERROR
Log Message	SIPALG: Invalid transaction state change
Explanation	Invalid transaction state found [tsxn_invalid_state].
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	tsxn_invalid_state from_uri to_uri

	srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.265. invalid_session_state (ID: 00200553)

Default Severity	ERROR
Log Message	SIPALG: Invalid session state change
Explanation	Invalid session state found [session_invalid_state].
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	session_invalid_state from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.266. sipalg_callleg_created (ID: 00200554)

Default Severity	NOTICE
Log Message	SIPALG: CallLeg created
Explanation	SIP-ALG callleg created for [method] request.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.267. failed_to_create_new_callleg (ID: 00200555)

Default Severity	ERROR
Log Message	SIPALG: Failed to create callleg
Explanation	The SIP-ALG failed to create callleg for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.268. failed_to_find_callleg (ID: 00200556)

Default Severity	WARNING
Log Message	SIPALG: Failed to find callleg
Explanation	Failed to find callleg for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.269. failed_to_update_callleg (ID: 00200557)

Default Severity	WARNING
Log Message	SIPALG: Failed to update callleg

Explanation	Failed to update callleg for [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.270. sipalg_callleg_deleted (ID: 00200558)

Default Severity	NOTICE
Log Message	SIPALG: sipalg callleg deleted
Explanation	The callleg for [method] request is deleted.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name ALG Session ID

2.1.271. failed_to_modify_response (ID: 00200559)

Default Severity	ERROR
Log Message	SIPALG: Failed to modify the response
Explanation	Failed to modify the topology info in the [method] response.
Firewall Action	drop
Recommended Action	None.
Revision	2

Parameters	method from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.272. sipalg_callleg_state_updated (ID: 00200560)

Default Severity	DEBUG
Log Message	SIPALG: SIP-ALG callleg state updated
Explanation	The SIP-ALG callleg state updated to [callleg_state] state.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	callleg_state from_uri to_uri srcip srcport destip destport
Context Parameters	ALG Module Name

2.1.273. failed_to_modify_sat_request (ID: 00200561)

Default Severity	ERROR
Log Message	SIPALG: Failed to modify the SAT request
Explanation	Failed to modify requst ip to SAT destination IP in the [method] request.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	method from_uri to_uri srcip srcport destip destport

Context Parameters	ALG Module Name

2.1.274. max_pptp_sessions_reached (ID: 00200601)

Default Severity	WARNING
Log Message	PPTPALG: Maximum number of PPTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent PPTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of PPTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.275. failed_create_new_session (ID: 00200602)

Default Severity	CRITICAL
Log Message	PPTPALG: Failed to create new PPTPALG session (out of memory)
Explanation	An attempt to create a new PPTPALG session failed. The unit has run out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed PPTPALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.276. failed_connect_pptp_server (ID: 00200603)

Default Severity	ERROR
Log Message	PPTPALG: Failed to connect to the PPTP Server. Closing the connection.
Explanation	The PPTP ALG could not connect to the receiving PPTP server, resulting in that the ALG session could not be successfully opened.
Firewall Action	close
Recommended Action	None.

Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.277. pptp_tunnel_established_client (ID: 00200604)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP tunnel established from client
Explanation	A PPTP tunnel has been established between PPTP client and firewall.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	ALG Session ID ALG Module Name

2.1.278. pptp_tunnel_removed_client (ID: 00200605)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP tunnel between client and firewall removed
Explanation	A PPTP tunnel has been removed between the PPTP client and the PPTP-ALG.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	ALG Session ID ALG Module Name

2.1.279. pptp_tunnel_removed_server (ID: 00200606)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP tunnel between server and firewall removed
Explanation	A PPTP tunnel has been removed betweem the PPTP server and the PPTP-ALG.
Firewall Action	None
Recommended Action	None.

Revision	2
Context Parameters	ALG Session ID ALG Module Name

2.1.280. pptp_session_established (ID: 00200607)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP session established
Explanation	A PPTP session has been established.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Session ID ALG Module Name

2.1.281. pptp_session_removed (ID: 00200608)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP session removed
Explanation	A PPTP session has been removed.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Session ID ALG Module Name

2.1.282. pptp_malformed_packet (ID: 00200609)

Default Severity	WARNING
Log Message	Malformed packet received from <remotegw> on <iface>
Explanation	A malformed packet was received by the PPTP-ALG.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	iface

remotegw

2.1.283. pptp_tunnel_established_server (ID: 00200610)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP tunnel established from server
Explanation	A PPTP tunnel has been established between PPTP server and firewall.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	ALG Session ID ALG Module Name

2.1.284. max_imap_sessions_reached (ID: 00200650)

Default Severity	WARNING
Log Message	IMAPALG: Maximum number of IMAP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent IMAP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of IMAP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.285. failed_create_new_session (ID: 00200651)

Default Severity	WARNING
Log Message	IMAPALG: Failed to create new IMAP ALG session (out of memory)
Explanation	An attempt to create a new IMAP ALG session failed, because the unit is out of memory.
Firewall Action	close
Recommended Action	Decrease the maximum allowed IMAP ALG sessions, or try to free some of the RAM used.

Revision	1
Context Parameters	ALG Module Name

2.1.286. failed_connect_imap_server (ID: 00200652)

Default Severity	ERROR
Log Message	IMAPALG: Failed to connect to the IMAP Server. Closing the connection.
Explanation	The unit failed to connect to the remote IMAP Server, resulting in that the ALG session could not be successfully opened.
Firewall Action	close
Recommended Action	Verify that there is a listening IMAP Server on the specified address.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.287. out_of_memory (ID: 00200656)

Default Severity	ERROR
Log Message	IMAPALG: Failed to allocate memory (out of memory)
Explanation	An attempt to allocate memory failed.
Firewall Action	close
Recommended Action	Try to free up unwanted memory.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.288. blocked_filetype (ID: 00200657)

Default Severity	NOTICE
Log Message	IMAPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Firewall Action	block
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.

Revision	2
Parameters	imap_userid imap_mailbox imap_msg_uid imap_msg_sequence_number imap_mail_size filename filetype sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.289. base64_decode_failed (ID: 00200658)

Default Severity	ERROR
Log Message	IMAPALG: Base 64 decode failed. Attachment blocked
Explanation	The data sent to Base64 decoding failed. This can occur if the email sender sends incorrectly formatted data. The attachment has been blocked.
Firewall Action	block_data
Recommended Action	Research how the sender is encoding the data.
Revision	2
Parameters	imap_userid imap_mailbox imap_msg_uid imap_msg_sequence_number imap_mail_size filename filetype sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.290. command_blocked (ID: 00200659)

Default Severity	WARNING
Log Message	IMAPALG: Command <imap_command> blocked.
Explanation	The client is sending command that are not allowed. The command will be blocked.
Firewall Action	block
Recommended Action	If the command are to be allowed change the Alg configuration.Note: The STLS command is allways blocked!.

Revision	2
Parameters	imap_userid imap_command
Context Parameters	ALG Module Name ALG Session ID

2.1.291. unknown_command_blocked (ID: 00200660)

Default Severity	WARNING
Log Message	IMAPALG: Unknown command blocked.
Explanation	The client is sending unknown command. The command will be blocked.
Firewall Action	block
Recommended Action	If the command are to be allowed change the Alg configuration.
Revision	2
Parameters	imap_userid imap_command
Context Parameters	ALG Module Name ALG Session ID

2.1.292. command_invalid (ID: 00200661)

Default Severity	WARNING
Log Message	IMAP_ALG: Command <imap_command> invalid.
Explanation	The client is sending command that is not a valid command. The command will be blocked.
Firewall Action	block
Recommended Action	If the command are to be allowed change the Alg configuration.
Revision	2
Parameters	imap_userid imap_command
Context Parameters	ALG Module Name ALG Session ID

2.1.293. response_blocked_unknown (ID: 00200662)

Default Severity	WARNING

Log Message	IMAP_ALG: Response blocked. Invalid response.
Explanation	The server is sending unknown response for command [imap_command]. The response will be blocked.
Firewall Action	block
Recommended Action	None.
Revision	2
Parameters	imap_userid imap_command
Context Parameters	ALG Module Name ALG Session ID

2.1.294. content_type_mismatch (ID: 00200663)

Default Severity	NOTICE
Log Message	IMAPALG: Content type mismatch in file <filename>. Identified filetype <filetype>
Explanation	The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.
Firewall Action	block_data
Recommended Action	None.
Revision	2
Parameters	imap_userid imap_mailbox imap_msg_uid imap_msg_sequence_number imap_mail_size filename filetype sender_email_address
Context Parameters	ALG Module Name

2.1.295. plain_auth_blocked (ID: 00200664)

Default Severity	WARNING
Log Message	IMAPALG: Plain text authentication attempt blocked.
Explanation	The client is sending plain text authentication request. It will be blocked.
Firewall Action	block
Recommended Action	If this is not desired, allow plain text authentication in relative email

profile.

Revision 2

Parameters imap_userid
imap_command

Context Parameters ALG Module Name
ALG Session ID

2.1.296. unknown_imap_syntax (ID: 00200665)

Default Severity NOTICE

Log Message IMAPALG: Unknown IMAP syntax in response

Explanation Unknown IMAP syntax in response, content will be passed through without scanning.

Firewall Action allow_response

Recommended Action None.

Revision 1

Parameters imap_userid
imap_mailbox
imap_msg_uid
imap_msg_sequence_number

Context Parameters ALG Module Name
ALG Session ID

2.1.297. unknown_mail_syntax (ID: 00200666)

Default Severity NOTICE

Log Message IMAPALG: Unknown syntax in mail header

Explanation Unknown syntax in mail header, content will be passed through without scanning.

Firewall Action allow_mail

Recommended Action None.

Revision 1

Parameters imap_userid
imap_mailbox
imap_msg_uid
imap_msg_sequence_number
imap_mail_size

Context Parameters ALG Module Name
ALG Session ID

2.1.298. unknown_mail_body_syntax (ID: 00200667)

Default Severity	NOTICE
Log Message	IMAPALG: Unknown syntax in mail content
Explanation	Unknown syntax in mail content, content will be passed through without scanning.
Firewall Action	allow_mail_content
Recommended Action	None.
Revision	1
Parameters	sourceip from to profile imap_userid imap_mailbox imap_msg_uid imap_msg_sequence_number imap_mail_size
Context Parameters	ALG Module Name ALG Session ID

2.1.299. imap_session_statistics (ID: 00200670)

Default Severity	DEBUG
Log Message	IMAPALG: Statistics for closing IMAP session
Explanation	Statistics for IMAP session.
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	imap_userid mail_scanned mail_spam_detected mail_virus_detected blocked_attachments unknown_syntax_imap unknown_syntax_mail_header unknown_syntax_mail_body incomplete_mail_header incomplete_mail_body section_size_mail_header section_size_mail_body
Context Parameters	ALG Module Name ALG Session ID

2.1.300. max_dnscontrol_session_reached (ID: 00200680)

Default Severity	WARNING
Log Message	DNS Control: Maximum number of DNS Control sessions (<max_sessions>) for service reached. Closing connection.
Explanation	The maximum number of concurrent DNS Control sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Firewall Action	close
Recommended Action	If the maximum number of DNS Control session is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.301. failed_create_new_session (ID: 00200681)

Default Severity	WARNING
Log Message	DNS Control: Failed to create new DNS Control session (out of memory)
Explanation	Could not create a new DNS Control session due to lack of memory. No more sessions can be created unless the system increases the amount of free memory.
Firewall Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.302. failure_connect_dns_server (ID: 00200682)

Default Severity	INFORMATIONAL
Log Message	DNS Control: Failed to connect to DNS Server. Closing connection
Explanation	The unit failed to connect to DNS Server, resulting in that the ALG session could not open successfully.
Firewall Action	close
Recommended Action	Verify that there is a listening DNS Server on the specified address.

Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.303. dns_packet_rejected (ID: 00200683)

Default Severity	WARNING
Log Message	DNS Control: DNS packet rejected. Packet: <packet> TransactionID: <transactionid> payload_length: <payload_length>
Explanation	DNS packet rejected, dropping.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	transactionid reason packet payload_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.304. dns_transaction_opened (ID: 00200684)

Default Severity	INFORMATIONAL
Log Message	DNS Profile: Transaction opened.
Explanation	DNS Transaction opened.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	transactionid
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.305. dns_transaction_closed (ID: 00200685)

Default Severity	INFORMATIONAL
Log Message	DNS Profile: Transaction closed.

Explanation	DNS Transaction closed.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	transactionid
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.306. dns_resolving_address (ID: 00200690)

Default Severity	NOTICE
Log Message	DNS Profile: Resolving.
Explanation	DNS resolving address.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	transactionid query-type address
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.307. dns_resolved_address (ID: 00200692)

Default Severity	NOTICE
Log Message	DNS Profile: Resolved.
Explanation	DNS resolved address.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	transactionid domain query-type pref addresses
Context Parameters	ALG Module Name

ALG Session ID
Connection

2.1.308. dns_resolved_address (ID: 00200693)

Default Severity	NOTICE
Log Message	DNS Profile: Resolved.
Explanation	DNS resolved address.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	transactionid domain query-type addresses
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.309. dns_policy_violation (ID: 00200694)

Default Severity	WARNING
Log Message	DNS Profile: DNS packet rejected due to policy violation. Packet: <packet> TransactionID: <transactionid> Violation value <value>
Explanation	DNS packet rejected due to policy violation, dropping.
Firewall Action	drop
Recommended Action	Modify the DNS Profile if the packet should be allowed.
Revision	1
Parameters	transactionid reason packet value
Context Parameters	ALG Module Name ALG Session ID Connection

2.2. ANTISPAM

These log messages refer to the **ANTISPAM (Anti-spam related events)** category.

2.2.1. spam_found (ID: 05900001)

Default Severity	NOTICE
Log Message	Email was classified as spam.
Explanation	An email was classified as spam, but no action was taken.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	sourceip from to profile tests link_categories
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.2. spam_found (ID: 05900002)

Default Severity	INFORMATIONAL
Log Message	Email was classified as spam and has been tagged.
Explanation	An email was classified as spam and was tagged according to the configuration.
Firewall Action	tag
Recommended Action	None.
Revision	1
Parameters	sourceip from to profile methods link_categories
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.3. spam_found (ID: 05900003)

Default Severity	INFORMATIONAL
Log Message	Email was classified as spam and was rejected.
Explanation	An email was classified as spam and was rejected.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	sourceip from to profile methods link_categories
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.4. memory_allocation_failure (ID: 05900010)

Default Severity	ERROR
Log Message	Failed to allocate memory required for anti-spam.
Explanation	A memory allocation failure occurred. The system will be unable to perform anti-spam scanning on this email.
Firewall Action	None
Recommended Action	Review configuration to reduce memory consumption.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.5. domain_verification_timeout (ID: 05900020)

Default Severity	ERROR
Log Message	Domain Verification failed because the DNS query timed out.

Explanation	Domain Verification failed because the DNS query timed out.
Firewall Action	None
Recommended Action	Verify that DNS is configured correctly.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.6. domain_verification_error (ID: 05900021)

Default Severity	ERROR
Log Message	Domain Verification failed because a DNS query could not be sent.
Explanation	Domain Verification failed because a DNS query could not be sent.
Firewall Action	None
Recommended Action	Verify that DNS is configured correctly.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.7. link_protection_allocation_failure (ID: 05900030)

Default Severity	ERROR
Log Message	Failed to allocate memory for Link Protection.
Explanation	A memory allocation failure occurred while performing Link Protection. Malicious links may slip through unnoticed as a result.
Firewall Action	None
Recommended Action	Review configuration to reduce memory consumption.
Revision	1
Parameters	sourceip from

	to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.8. link_protection_timeout (ID: 05900031)

Default Severity	ERROR
Log Message	Link Protection query timed out.
Explanation	A link could not be classified because the WCF servers did not respond.
Firewall Action	None
Recommended Action	Verify that the system is configured to allow WCF lookups.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.9. link_protection_wcf_error (ID: 05900032)

Default Severity	ERROR
Log Message	Link Protection WCF error.
Explanation	A link could not be classified because a query could not be sent to the WCF servers.
Firewall Action	None
Recommended Action	Verify that the system is configured to allow WCF lookups.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.10. link_protection_no_license (ID: 05900033)

Default Severity	ERROR
Log Message	Link Protection has been disabled due to license restrictions.
Explanation	A valid Web Content Filtering license is required to use Link Protection.
Firewall Action	None
Recommended Action	Extend valid time for Web Content Filtering.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.11. dnsbl_allocation_failure (ID: 05900040)

Default Severity	ERROR
Log Message	Failed to allocate memory for DNSBL lookup. DNSBL: <dnsbl>
Explanation	A memory allocation failure occurred while performing DNSBL lookup.
Firewall Action	None
Recommended Action	Review configuration to reduce memory consumption.
Revision	1
Parameters	sourceip from to profile dnsbl
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.12. dnsbl_timeout (ID: 05900041)

Default Severity	ERROR
Log Message	DNSBL check failed because the DNS query timed out. DNSBL:

	<dnsbl>
Explanation	DNSBL check failed because the DNS query timed out.
Firewall Action	None
Recommended Action	Verify that DNS is configured correctly.
Revision	1
Parameters	sourceip from to profile dnsbl
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.13. dnsbl_error (ID: 05900042)

Default Severity	ERROR
Log Message	DNSBL check failed because a DNS query could not be sent. DNSBL: <dnsbl>
Explanation	DNSBL check failed because a DNS query could not be sent.
Firewall Action	None
Recommended Action	Verify that DNS is configured correctly.
Revision	1
Parameters	sourceip from to profile dnsbl
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.14. dcc_allocation_failure (ID: 05900050)

Default Severity	ERROR
Log Message	Failed to allocate memory for DCC.
Explanation	A memory allocation failure occurred while performing DCC.
Firewall Action	None
Recommended Action	Review configuration to reduce memory consumption.

Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.15. dcc_timeout (ID: 05900051)

Default Severity	ERROR
Log Message	DCC query timed out.
Explanation	DCC check failed because no response was received from the DCC servers.
Firewall Action	None
Recommended Action	Verify that the DCC servers are reachable.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.16. dcc_query_error (ID: 05900052)

Default Severity	ERROR
Log Message	Failed to send DCC query.
Explanation	A DCC query could not be sent.
Firewall Action	None
Recommended Action	Verify that the DCC servers are reachable.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name

ALG Session ID

2.2.17. dcc_no_license (ID: 05900053)

Default Severity	ERROR
Log Message	DCC has been disabled due to license restrictions.
Explanation	DCC has been disabled due to license restrictions.
Firewall Action	None
Recommended Action	Extend valid time for DCC.
Revision	1
Parameters	sourceip from to profile
Context Parameters	Connection ALG Module Name ALG Session ID

2.2.18. recipient_email_changed_to_drop_address (ID: 05900196)

Default Severity	NOTICE
Log Message	SMTPALG: Recipient e-mail address is changed to DNSBL Drop address
Explanation	"RCPT TO:" e-mail address is changed to the Drop address configured in DNS Blacklist.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	sender_email_address drop_address
Context Parameters	ALG Module Name ALG Session ID

2.2.19. dnsbl_allocate_error (ID: 05900800)

Default Severity	EMERGENCY
Log Message	Could not allocate memory

Explanation	Could not allocate memory.
Firewall Action	none
Recommended Action	Check memory.
Revision	1
Parameters	type

2.2.20. dnsbl_ipcache_add (ID: 05900810)

Default Severity	NOTICE
Log Message	IP <ipaddr> added to IP Cache for <algname>
Explanation	An IP address was added to the IP Cache.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr

2.2.21. dnsbl_ipcache_remove (ID: 05900811)

Default Severity	NOTICE
Log Message	IP <ipaddr> removed from IP Cache for <algname> due to timeout
Explanation	An IP address was removed from the IP Cache due to timeout.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr

2.2.22. dnsbl_session_add (ID: 05900812)

Default Severity	NOTICE
Log Message	Session created for IP <ipaddr> for <algname>
Explanation	Session created and awaiting processing.

Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr

2.2.23. dnsbl_session_error (ID: 05900813)

Default Severity	ERROR
Log Message	Error creating Session for IP <ipaddr> for <algname>
Explanation	Error creating new Session.
Firewall Action	dnsbl will not process mail
Recommended Action	Check configuration and dns settings.
Revision	1
Parameters	type algname ipaddr

2.2.24. dnsbl_ipcache_add (ID: 05900814)

Default Severity	NOTICE
Log Message	Session for IP <ipaddr> for <algname> is done with result <result>
Explanation	An IP address was added to the IP Cache.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr result

2.2.25. dnsbl_disabled (ID: 05900815)

Default Severity	EMERGENCY
Log Message	DNSBL for <algname> has been disabled
Explanation	The DNSBL has been disabled due to few active BlackLists.

Firewall Action	none
Recommended Action	Check configuration of DNSBL.
Revision	1
Parameters	type algname

2.2.26. dnsbl_active (ID: 05900816)

Default Severity	NOTICE
Log Message	DNSBL for <algname> has been activated
Explanation	The DNSBL has changed status from disabled to active as contact with BlackLists have been restored.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname

2.2.27. dnsbl_query_add (ID: 05900817)

Default Severity	NOTICE
Log Message	Query created for IP <ipaddr> to BlackList <blacklist> for <algname>
Explanation	A DNS Query was created.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr blacklist query

2.2.28. dnsbl_blacklist_disable (ID: 05900818)

Default Severity	WARNING
Log Message	BlackList <blacklist> for <algname> has been disabled

Explanation	BlackList was disable as it failed to respond to the query.
Firewall Action	none
Recommended Action	Check configuration if keeps begin disabled.
Revision	1
Parameters	type algname blacklist

2.2.29. dnsbl_txtrecord_truncated (ID: 05900819)

Default Severity	WARNING
Log Message	TXT records does not fit buffer for Session with IP <ipaddr> for <algname>
Explanation	TXT records will not fit the string buffer and will be truncated.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr

2.2.30. dnsbl_record_truncated (ID: 05900820)

Default Severity	WARNING
Log Message	DNSBL name not fit buffer for Session with IP <ipaddr> for <algname>
Explanation	DNSBL name will not fit the string buffer and will be truncated.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	type algname ipaddr

2.3. ANTIVIRUS

These log messages refer to the **ANTIVIRUS (Anti-Virus related events)** category.

2.3.1. virus_found (ID: 05800001)

Default Severity	WARNING
Log Message	A virus has been detected in a data stream. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Explanation	None.
Firewall Action	block_data
Recommended Action	If the infected file is local, run anti-virus program to clean the file.
Revision	2
Parameters	filename virusname virussig advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.2. virus_found (ID: 05800002)

Default Severity	WARNING
Log Message	A virus has been detected in a data stream. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Explanation	None.
Firewall Action	allow_data
Recommended Action	If the infected file is local, run anti-virus program to clean the file.
Revision	2
Parameters	filename virusname virussig advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.3. excluded_file (ID: 05800003)

Default Severity	NOTICE
Log Message	File <filename> is excluded from scanning. Identified filetype: <filetype>.
Explanation	The named file will be excluded from anti-virus scanning. The filetype is present in the anti-virus scan exclusion list.
Firewall Action	allow_data_without_scan
Recommended Action	None.
Revision	1
Parameters	filename filetype [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.4. decompression_failed (ID: 05800004)

Default Severity	ERROR
Log Message	Decompression error for file <filename>
Explanation	The file could not be scanned by the anti-virus module since the decompression of the compressed file failed. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Firewall Action	block_data
Recommended Action	Change Fail Mode parameter to allow if files that fail decompression should be allowed without scanning.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.5. decompression_failed (ID: 05800005)

Default Severity	ERROR

Log Message	Decompression error for file <filename>
Explanation	The file could not be scanned by the anti-virus module since the decompression of the compressed file failed. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Firewall Action	allow_data
Recommended Action	Change Fail Mode parameter to deny if files that fail decompression should be blocked.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.6. compression_ratio_violation (ID: 05800007)

Default Severity	WARNING
Log Message	Compression ratio violation for file <filename>. Compression ratio threshold: <comp_ratio>
Explanation	Anti-virus has scanned a compressed file with a compression ratio higher than the specified value. Action is set to continue scan.
Firewall Action	abort_scan
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DoS attack.
Revision	2
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.7. compression_ratio_violation (ID: 05800008)

Default Severity	WARNING
Log Message	Compression ratio violation for file <filename>. Compression ratio threshold: <comp_ratio>
Explanation	Anti-virus has scanned a compressed file with a compression ratio higher than the specified value. Action is set to continue scan.

Firewall Action	block_data
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DoS attack.
Revision	2
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.8. out_of_memory (ID: 05800009)

Default Severity	ERROR
Log Message	Out of memory
Explanation	Memory allocation failed. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Firewall Action	allow_data
Recommended Action	Try to free some memory by changing configuration parameters.
Revision	1
Parameters	filename filetype [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.9. out_of_memory (ID: 05800010)

Default Severity	ERROR
Log Message	Out of memory
Explanation	Memory allocation failed. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Firewall Action	block_data
Recommended Action	Try to free some memory by changing configuration parameters.
Revision	1

Parameters	filename filetype [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.10. virus_scan_failure (ID: 05800011)

Default Severity	ERROR
Log Message	Anti-virus scan engine failed for the file: <filename>
Explanation	An error occured in the anti-virus scan engine. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Firewall Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.11. virus_scan_failure (ID: 05800012)

Default Severity	ERROR
Log Message	Anti-virus scan engine failed for the file: <filename>
Explanation	An error occured in the anti-virus scan engine. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Firewall Action	allow_data
Recommended Action	None.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.12. no_valid_license (ID: 05800015)

Default Severity	CRITICAL
Log Message	AVSE: Virus scanning aborted. No valid license present.
Explanation	Anti-virus scanning is aborted since there is no valid license present.
Firewall Action	av_scanning_aborted
Recommended Action	If anti-virus scanning is wanted, you must get a valid license with anti-virus capabilities. Anti-virus scanning can be turned off in order to avoid future postings of this log message.
Revision	2
Context Parameters	ALG Session ID

2.3.13. av_signatures_missing (ID: 05800016)

Default Severity	CRITICAL
Log Message	AVSE: Virus scanning aborted. Not all virus signatures present.
Explanation	Anti-virus scanning is aborted since there is local anti-virus signature databases missing.
Firewall Action	av_scanning_denied
Recommended Action	Connect your firewall to the Internet and download the anti-virus databases or configure automatic updates of anti-virus.
Revision	4
Context Parameters	ALG Session ID

2.3.14. general_engine_error (ID: 05800017)

Default Severity	CRITICAL
Log Message	AVSE: Virus scanning aborted. General error occured during initialization.
Explanation	Anti-virus scanning is aborted since the scan engine returned a general error during initialization.
Firewall Action	av_scanning_aborted
Recommended Action	Try to restart the unit in order to solve this issue.
Revision	2
Context Parameters	ALG Session ID

2.3.15. out_of_memory (ID: 05800018)

Default Severity	CRITICAL
Log Message	AVSE: Virus scanning aborted. Out of memory during initialization.
Explanation	Anti-virus scanning is aborted since the scan engine run out of memory during initialization.
Firewall Action	av_scanning_denied
Recommended Action	Review your configuration in order to free up more RAM.
Revision	2
Context Parameters	ALG Session ID

2.3.16. virus_url_detected (ID: 05800020)

Default Severity	WARNING
Log Message	Virus infected URL found in URL <url>. Advisory ID: <advisoryid>.
Explanation	A virus infected URL request has been detected. Since anti-virus is running in protect mode, the request will be aborted in order to protect the receiver.
Firewall Action	block_data
Recommended Action	None.
Revision	1
Parameters	url advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.17. virus_url_detected (ID: 05800021)

Default Severity	WARNING
Log Message	Virus infected URL found in URL <url>. Advisory ID: <advisoryid>.
Explanation	A virus infected URL request has been detected. Since anti-virus is running in audit mode, the request will be allowed to continue.
Firewall Action	allow_data
Recommended Action	None.

Revision	1
Parameters	url advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.18. decompression_failed_encrypted_file (ID: 05800024)

Default Severity	WARNING
Log Message	Decompression failed for file <filename>. The file is encrypted.
Explanation	The file could not be scanned by the anti-virus module since the compressed file is encrypted with password protection. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Firewall Action	block_data
Recommended Action	Change Fail Mode parameter to allow if files that fail decompression should be allowed without scanning.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.19. decompression_failed_encrypted_file (ID: 05800025)

Default Severity	WARNING
Log Message	Decompression failed for file <filename>. The file is encrypted.
Explanation	The file could not be scanned by the anti-virus module since the compressed file is encrypted with password protection. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Firewall Action	allow_data
Recommended Action	Change Fail Mode parameter to deny if files that fail decompression should be blocked.
Revision	1
Parameters	filename

[layer7_srcinfo]
[layer7_dstinfo]

Context Parameters ALG Module Name
ALG Session ID
Connection

2.3.20. out_of_memory (ID: 05800027)

Default Severity CRITICAL

Log Message Out of memory while allocating anti-virus cache entry.

Explanation An attempt to add a detected virus to the anti-virus cache failed since the system has run out of memory. .

Firewall Action ignore

Recommended Action Try to free some memory by changing configuration parameters.

Revision 1

2.3.21. max_archive_depth_exceeded (ID: 05800028)

Default Severity WARNING

Log Message The file <filename> has too many archive levels. Maximum allowed is <max_depth>.

Explanation The file archive exceeds the maximum allowed depth. Since Fail Mode is set to Deny the data transfer will be aborted in order to protect the receiver.

Firewall Action block_data

Recommended Action Change Fail Mode parameter to Allow if files that fail decompression should be allowed without scanning. Increase the Max. Archive Depth parameter to allow deeper files to be scanned.

Revision 1

Parameters filename
max_depth
[layer7_srcinfo]
[layer7_dstinfo]

Context Parameters ALG Module Name
ALG Session ID
Connection

2.3.22. max_archive_depth_exceeded (ID: 05800029)

Default Severity WARNING

Log Message	The file <filename> has too many archive levels. Maximum allowed is <max_depth>.
Explanation	The file archive exceeds the maximum allowed depth. Since Fail Mode is set to Allow the data transfer will be allowed to continue.
Firewall Action	allow_data
Recommended Action	Change Fail Mode parameter to Deny if files that fail decompression should be blocked. Increase the Max. Archive Depth parameter to allow deeper files to be scanned.
Revision	1
Parameters	filename max_depth [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.3.23. unknown_encoding (ID: 05800182)

Default Severity	WARNING
Log Message	SMTPALG: Content transfer encoding is unknown or not present
Explanation	Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is deny so data is blocked.
Firewall Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename unknown_content_transfer_encoding sender_email_address recipient_email_addresses:
Context Parameters	ALG Module Name ALG Session ID

2.3.24. unknown_encoding (ID: 05800183)

Default Severity	WARNING
Log Message	SMTPALG: Content transfer encoding is unknown or not present.
Explanation	Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is allow so data is allowed without scanning.

Firewall Action	allow_data_without_scan
Recommended Action	Research the Content Transfer Encoding format.
Revision	1
Parameters	filename unknown_content_transfer_encoding sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.3.25. unknown_encoding (ID: 05800184)

Default Severity	WARNING
Log Message	POP3ALG: Content transfer encoding is unknown or not present
Explanation	Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is deny so data is blocked.
Firewall Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename unknown_content_transfer_encoding sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.3.26. unknown_encoding (ID: 05800185)

Default Severity	WARNING
Log Message	POP3ALG: Content transfer encoding is unknown or not present.
Explanation	Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is allow so data is allowed without scanning.
Firewall Action	allow_data_without_scan
Recommended Action	Research the Content Transfer Encoding format.
Revision	1
Parameters	filename unknown_content_transfer_encoding sender_email_address

Context Parameters ALG Module Name
ALG Session ID

2.3.27. unknown_encoding (ID: 05800654)

Default Severity WARNING

Log Message IMAPALG: Content transfer encoding is unknown or not present

Explanation Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is deny so data is blocked.

Firewall Action block_data

Recommended Action None.

Revision 2

Parameters filename
unknown_content_transfer_encoding
sender_email_address

Context Parameters ALG Module Name
ALG Session ID

2.3.28. unknown_encoding (ID: 05800655)

Default Severity WARNING

Log Message IMAPALG: Content transfer encoding is unknown or not present.

Explanation Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is allow so data is allowed without scanning.

Firewall Action allow_data_without_scan

Recommended Action Research the Content Transfer Encoding format.

Revision 2

Parameters imap_userid
imap_mailbox
imap_msg_uid
imap_msg_sequence_number
imap_mail_size
filename
unknown_content_transfer_encoding
sender_email_address

Context Parameters ALG Module Name
ALG Session ID

2.4. APPCONTROL

These log messages refer to the **APPCONTROL (Application Control events)** category.

2.4.1. application_identified (ID: 07200001)

Default Severity	INFORMATIONAL
Log Message	Application identified. Application: <application>.
Explanation	An application protocol has been recognized by the application control function.
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	application applicationrule applicationruleset
Context Parameters	Connection Rule Information

2.4.2. application_identified (ID: 07200002)

Default Severity	INFORMATIONAL
Log Message	Application identified. Application: <application>.
Explanation	An application protocol has been recognized by the application control function.
Firewall Action	close
Recommended Action	None.
Revision	3
Parameters	application applicationrule applicationruleset
Context Parameters	Connection Rule Information

2.4.3. application_end (ID: 07200003)

Default Severity	INFORMATIONAL
Log Message	Application ended. Application: <application>.

Explanation	The end of an application protocol has been recognized by the application control function.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	application family risk ssl_inspected
Context Parameters	Connection UINT64 UINT64

2.4.4. no_valid_license (ID: 07200004)

Default Severity	CRITICAL
Log Message	Application Control disabled
Explanation	Application Control has been disabled due to license restriction.
Firewall Action	application_control_disabled
Recommended Action	Extend valid time for Application Control.
Revision	3

2.4.5. application_control_disabled (ID: 07200005)

Default Severity	CRITICAL
Log Message	Application Control disabled
Explanation	Application Control has been disabled due fatal subsystem failure. Traffic will be treated as 'unknown' by Application Control.
Firewall Action	treat_traffic_as_unknown
Recommended Action	Restart the device or restore the system from a full system backup to restore Application Control functionality. It is also possible to configure the device to automatically restart if Application Control is disabled due to fatal failure through the Application Control setting 'Restart On Fatal Failure'.
Revision	1

2.4.6. application_control_disabled (ID: 07200006)

Default Severity	CRITICAL

Log Message	Application Control disabled
Explanation	Application Control has been disabled due fatal subsystem failure. The device will restart itself to try to restore Application Control functionality.
Firewall Action	restart
Recommended Action	It is also possible to configure the device continue with Application Control disabled through the Application Control setting 'Restart On Fatal Failure'.
Revision	1

2.4.7. appctl_memory_optimized (ID: 07200008)

Default Severity	NOTICE
Log Message	Cleaning up Application Control memory
Explanation	The application control subsystem cleaned up memory usage in order to free memory. The AppCtl_FreeMemOptLevel setting can be used to tweak the limit when memory cleanup should be triggered.
Firewall Action	none
Recommended Action	None.
Revision	1

2.4.8. application_content (ID: 07200015)

Default Severity	INFORMATIONAL
Log Message	Application attribute found. Application: <application> Attribute: <attribute> Value: <value>
Explanation	An application attribute has been identified by Application Content Control.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	application attribute value
Context Parameters	Connection

2.4.9. application_content_allowed (ID: 07200016)

Default Severity	WARNING
Log Message	Application content allowed. Application: <application> Attribute: <attribute> Value: <value>
Explanation	The identified application attribute and its value is allowed by the Application Content Control policy.
Firewall Action	None
Recommended Action	Modify the Application Content Control policy if this traffic should be denied.
Revision	1
Parameters	application attribute value
Context Parameters	Connection

2.4.10. application_content_denied (ID: 07200017)

Default Severity	WARNING
Log Message	Application content denied. Application: <application> Attribute: <attribute> Value: <value>
Explanation	The configured Application Content Control policy does not allow the identified attribute or its value. The connection is closed.
Firewall Action	close
Recommended Action	Modify the Application Content Control policy if this traffic should be allowed.
Revision	1
Parameters	application attribute value
Context Parameters	Connection

2.4.11. out_of_memory (ID: 07200018)

Default Severity	ERROR
Log Message	Out of memory
Explanation	Failed to allocate memory for Application Content Control.
Firewall Action	None
Recommended Action	Modify the units configuration to make more RAM available.
Revision	1

Context Parameters Connection

2.4.12. application_content_limit_reached (ID: 07200019)

Default Severity ERROR

Log Message Maximum number of concurrent non-classified (in progress) application control connections (50.000) reached.

Explanation There is a maximum of 50.000 Application Content Control attributes to store until connections have been fully classified. This limit has been reached. Application Content Control is disabled for this connection until the connection has been fully classified.

Firewall Action None

Recommended Action None.

Revision 1

Context Parameters Connection

2.5. ARP

These log messages refer to the **ARP (ARP events)** category.

2.5.1. unsolicited_reply_drop (ID: 00300001)

Default Severity	NOTICE
Log Message	Unsolicited ARP reply received and dropped
Explanation	An ARP reply was received even though no reply was currently expected for this IP.
Firewall Action	None
Recommended Action	If this is not the wanted behavior, change the setting UnsolicitedARPReplies.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.2. no_sender_ip (ID: 00300002)

Default Severity	NOTICE
Log Message	ARP query sender IP is 0.0.0.0
Explanation	The source IP-address of an ARP query is 0.0.0.0. Allowing.
Firewall Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.3. no_sender_ip (ID: 00300003)

Default Severity	NOTICE
Log Message	ARP query sender IP is 0.0.0.0. Dropping
Explanation	The source IP-address of an ARP query is 0.0.0.0. Dropping packet.
Firewall Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1

Context Parameters	Rule Name Packet Buffer

2.5.4. arp_response_broadcast (ID: 00300004)

Default Severity	NOTICE
Log Message	ARP response is a broadcast address
Explanation	The ARP response has a sender address which is a broadcast address. Allowing.
Firewall Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.5. arp_response_multicast (ID: 00300005)

Default Severity	NOTICE
Log Message	ARP response is a multicast address
Explanation	The ARP response has a sender address which is a multicast address. This might be the case if there are load balancing network equipment in the network. Allowing.
Firewall Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.6. mismatching_hwaddrs (ID: 00300006)

Default Severity	NOTICE
Log Message	ARP hw sender does not match Ethernet hw sender
Explanation	The hardware sender address specified in the ARP data does not match the Ethernet hardware sender address. Allowing.
Firewall Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1

Context Parameters	Rule Name Packet Buffer

2.5.7. mismatching_hwaddrs_drop (ID: 00300007)

Default Severity	NOTICE
Log Message	ARP hw sender does not match Ethernet hw sender. Dropping
Explanation	The hardware sender address specified in the ARP data does not match the Ethernet hardware sender address. Dropping packet.
Firewall Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.8. hwaddr_change (ID: 00300008)

Default Severity	NOTICE
Log Message	<knownip> has a different address <newhw> compared to the known hardware address <knownhw>. Allow packet for further processing.
Explanation	A known dynamic ARP entry has a different hardware address than the one in the ARP packet. Allowing packet for further processing.
Firewall Action	allow_processing
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Parameters	knownip knownhw newhw
Context Parameters	Rule Name Packet Buffer

2.5.9. arp_resolution_failed (ID: 00300009)

Default Severity	WARNING
Log Message	ARP resolution failed
Explanation	ARP query was not resolved before the ARP cache entry expired.
Firewall Action	remove_entry

Recommended Action	None.
Revision	1
Parameters	ipaddr iface

2.5.10. unsolicited_reply_accept (ID: 00300010)

Default Severity	NOTICE
Log Message	Unsolicited ARP reply received and accepted
Explanation	An ARP reply was received even though no reply was currently expected for this IP.
Firewall Action	None
Recommended Action	If this is not the wanted behavior, change the setting UnsolicitedARPReplies.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.11. arp_resolution_success (ID: 00300020)

Default Severity	NOTICE
Log Message	ARP entry was added to the ARP cache.
Explanation	ARP entry was added to the ARP cache.
Firewall Action	added_entry
Recommended Action	None.
Revision	1
Parameters	enetaddr ipaddr iface

2.5.12. arp_cache_size_limit_reached (ID: 00300030)

Default Severity	NOTICE
Log Message	ARP cache size limit reached
Explanation	The ARP cache size limit has been reached. Current license limit is [limit].
Firewall Action	None

Recommended Action	Update your license to allow a greater amount of concurrent ARP entries.
Revision	1
Parameters	limit

2.5.13. invalid_arp_sender_ip_address (ID: 00300049)

Default Severity	WARNING
Log Message	Failed to verify ARP sender IP address. Dropping
Explanation	The ARP sender IP address could not be verified according to the "access" section, and the packet is dropped.
Firewall Action	drop
Recommended Action	If all ARP sender IP addresses should be accepted without validation, modify the configuration.
Revision	2
Context Parameters	Rule Name Packet Buffer

2.5.14. arp_access_allowed_expect (ID: 00300050)

Default Severity	NOTICE
Log Message	Allowed by expect rule in access section
Explanation	The ARP sender IP address is verified by an expect rule in the access section.
Firewall Action	access_allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.15. impossible_hw_address (ID: 00300051)

Default Severity	NOTICE
Log Message	Impossible hardware address 0000:0000:0000 in ARP response. Dropping
Explanation	The ARP response has sender hardware address 0000:0000:0000, which is illegal. Dropping packet.

Firewall Action	drop
Recommended Action	Verify that no fault network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.16. arp_response_broadcast_drop (ID: 00300052)

Default Severity	WARNING
Log Message	ARP response is a broadcast address. Dropping
Explanation	The ARP response has a sender address which is a broadcast address. Dropping packet.
Firewall Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.17. arp_response_multicast_drop (ID: 00300053)

Default Severity	NOTICE
Log Message	ARP response is a multicast address. Dropping
Explanation	The ARP response has a sender address which is a multicast address. This might be the case if there are load balancing network equipment in the network. Dropping packet.
Firewall Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.5.18. arp_collides_with_static (ID: 00300054)

Default Severity	WARNING
Log Message	Known entry is <knowntype> <knownip>=<knownhw>. Dropping
Explanation	The hardware sender address does not match the static entry in the ARP table. Static ARP changes are not allowed. Dropping packet.

Firewall Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Parameters	reason knowntype knownip knownhw
Context Parameters	Rule Name Packet Buffer

2.5.19. hwaddr_change_drop (ID: 00300055)

Default Severity	NOTICE
Log Message	<knownip> has a different address <newhw> compared to the known hardware address <knownhw>. Dropping packet.
Explanation	A known dynamic ARP entry has a different hardware address than the one in the ARP packet. Dropping packet.
Firewall Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Parameters	knownip knownhw newhw
Context Parameters	Rule Name Packet Buffer

2.6. AUTHAGENTS

These log messages refer to the **AUTHAGENTS (Authentication Agent events)** category.

2.6.1. authagent_connected (ID: 06500001)

Default Severity	INFORMATIONAL
Log Message	Connected to Authentication Agent at <name>:<ipaddr>:<port>
Explanation	Connected to Authentication Agent.
Firewall Action	connected
Recommended Action	None.
Revision	2
Parameters	name ipaddr port

2.6.2. authagent_disconnected (ID: 06500002)

Default Severity	INFORMATIONAL
Log Message	Disconnected from Authentication Agent at <name>:<ipaddr>:<port>
Explanation	A Authentication Agent connection was disconnected.
Firewall Action	connected
Recommended Action	None.
Revision	2
Parameters	name ipaddr port

2.6.3. authagent_internal_error (ID: 06500003)

Default Severity	INFORMATIONAL
Log Message	Internal error while comunicating with Agent <name>:<ipaddr>.
Explanation	Internal error.
Firewall Action	internal_error
Recommended Action	None.
Revision	2

Parameters	name ipaddr

2.6.4. authagent_rekeying_error (ID: 06500004)

Default Severity	INFORMATIONAL
Log Message	Agent <name>:<ipaddr> does not accept new key.
Explanation	Rekeying error.
Firewall Action	rekeying_error
Recommended Action	None.
Revision	2
Parameters	name ipaddr

2.6.5. authagent_protocol_mistmatch (ID: 06500005)

Default Severity	INFORMATIONAL
Log Message	SGW protocol <sgwproto> and Agent <name>:<ipaddr> protocol <agentproto> do not match.
Explanation	Protocol mistmatch.
Firewall Action	protocol_mistmatch
Recommended Action	Update SGW or Agent.
Revision	2
Parameters	name ipaddr sgwproto agentproto

2.6.6. authagent_negotiation_error (ID: 06500006)

Default Severity	INFORMATIONAL
Log Message	Negotiation error with Agent <name>:<ipaddr>.
Explanation	Negotiation error.
Firewall Action	negotiation_error
Recommended Action	None.
Revision	2

Parameters	name ipaddr

2.6.7. authagent_decryption_error (ID: 06500007)

Default Severity	INFORMATIONAL
Log Message	Error while decrypting message from Agent <name>:<ipaddr>.
Explanation	Decryption error.
Firewall Action	decryption_error
Recommended Action	None.
Revision	2
Parameters	name ipaddr

2.6.8. authagent_challenge_error (ID: 06500008)

Default Severity	INFORMATIONAL
Log Message	Challenge error with Agent <name>:<ipaddr>.
Explanation	Challenge error.
Firewall Action	challenge_error
Recommended Action	Check PSK.
Revision	2
Parameters	name ipaddr

2.6.9. authagent_seqnumber_error (ID: 06500009)

Default Severity	INFORMATIONAL
Log Message	Received bad sequence number from Authentication Agent <name>:<ipaddr>.
Explanation	Received bad sequence number from Authentication Agent.
Firewall Action	seqnumber_error
Recommended Action	None.
Revision	2
Parameters	name ipaddr

2.6.10. authagent_adduser_error (ID: 06500010)

Default Severity	INFORMATIONAL
Log Message	Error adding user <name> at <ip>.
Explanation	Add user error.
Firewall Action	adduser_error
Recommended Action	None.
Revision	1
Parameters	name ip

2.6.11. authagent_initial_error (ID: 06500011)

Default Severity	INFORMATIONAL
Log Message	Error fetching initial data.
Explanation	Initial data error.
Firewall Action	initial_error
Recommended Action	None.
Revision	1

2.6.12. authagent_removeuser_error (ID: 06500012)

Default Severity	INFORMATIONAL
Log Message	Error removing user <name> at <ip>.
Explanation	Remove user error.
Firewall Action	removeuser_error
Recommended Action	None.
Revision	1
Parameters	name ip

2.6.13. authagent_password_error (ID: 06500013)

Default Severity	INFORMATIONAL

Log Message	Password error with Agent <name>:<ipaddr>.
Explanation	Password error.
Firewall Action	password_error
Recommended Action	None.
Revision	2
Parameters	name ipaddr

2.6.14. authagent_user_login (ID: 06500014)

Default Severity	NOTICE
Log Message	User logged in. Idle timeout: <idle_timeout>, Session timeout: <session_timeout>
Explanation	A user logged in and has been granted access, according to the group membership or user name information.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	idle_timeout session_timeout groups
Context Parameters	User Authentication

2.6.15. authagent_failed_session_update (ID: 06500015)

Default Severity	ERROR
Log Message	Failed to update session timeout. Session timeout: <session_timeout>
Explanation	Failed to update session timeout.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	session_timeout groups
Context Parameters	User Authentication

2.6.16. authagent_adduser_error (ID: 06500040)

Default Severity	INFORMATIONAL
Log Message	Error adding user <username> at <iface> <ip>.
Explanation	Add user error.
Firewall Action	adduser_error
Recommended Action	None.
Revision	1
Parameters	username iface ip

2.6.17. authagent_removeuser_error (ID: 06500042)

Default Severity	INFORMATIONAL
Log Message	Error removing user <iface> <ip>.
Explanation	Remove user error.
Firewall Action	removeuser_error
Recommended Action	None.
Revision	1
Parameters	iface ip

2.7. AVSE

These log messages refer to the **AVSE (Events from Anti Virus Scan Engine)** category.

2.7.1. av_db_digital_signature (ID: 05100001)

Default Severity	ALERT
Log Message	Could not start Anti-virus engine because of <reason>
Explanation	The unit tried to read the anti-virus database, but failed. The reason for this is specified in the "reason" parameter.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.8. AVUPDATE

These log messages refer to the **AVUPDATE (Antivirus Signature update)** category.

2.8.1. av_db_update_failure (ID: 05000001)

Default Severity	ALERT
Log Message	Update of the Anti-virus database failed, because of <reason>
Explanation	The unit tried to update the anti-virus database, but failed. The reason for this is specified in the "reason" parameter.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.8.2. av_database_downloaded (ID: 05000002)

Default Severity	NOTICE
Log Message	New anti-virus database downloaded
Explanation	An updated version of the anti-virus database has been downloaded, which will now be used.
Firewall Action	using_new_database
Recommended Action	None.
Revision	2

2.8.3. av_db_already_up_to_date (ID: 05000003)

Default Severity	NOTICE
Log Message	Anti-virus database is up-to-date
Explanation	The current anti-virus database is up-to-date, and does not need to be updated.
Firewall Action	None
Recommended Action	None.
Revision	1

2.8.4. av_db_update_denied (ID: 05000004)

Default Severity	NOTICE
Log Message	Anti-virus database could not be updated, as no valid subscription exist
Explanation	The current license does not allow the anti-virus database to be updated.
Firewall Action	None
Recommended Action	Check the system's time and/or purchase a subscription.
Revision	1

2.8.5. av_detects_invalid_system_time (ID: 05000005)

Default Severity	ERROR
Log Message	System clock is not properly set. Invalid date (<date>) in antivirus signature file. Antivirus Disabled
Explanation	The system clock is not up to date. The system clock must be set correctly in order to use the antivirus features. Antivirus features remains disabled until clock is correct and a manual antivirus update has been performed.
Firewall Action	antivirus_disabled
Recommended Action	Check and set the system time correct and perform a manual antivirus update.
Revision	1
Parameters	date

2.8.6. downloading_new_database (ID: 05000007)

Default Severity	NOTICE
Log Message	Downloading new antivirus database
Explanation	A new antivirus database is available. The database is being downloaded.
Firewall Action	downloading_new_database
Recommended Action	None.
Revision	1

2.8.7. unsynced_databases (ID: 05000008)

Default Severity	WARNING

Log Message	Unsynchronized hardware and software databases detected
Explanation	The anti-virus hardware and software databases are not synchronized. A full update is automatically initiated.
Firewall Action	downloading_new_database
Recommended Action	None.
Revision	1

2.8.8. downloading_new_database (ID: 05000009)

Default Severity	NOTICE
Log Message	Downloading new antivirus database <ss2db>
Explanation	A new antivirus database is available. The database is being downloaded.
Firewall Action	downloading_new_database
Recommended Action	None.
Revision	1
Parameters	ss2db

2.9. BLACKLIST

These log messages refer to the **BLACKLIST (Blacklist events)** category.

2.9.1. failed_to_write_list_of_blocked_hosts_to_media (ID: 04600001)

Default Severity	CRITICAL
Log Message	Failed to write list of blocked hosts to media
Explanation	Failed to write list of blocked hosts to media. The media might be corrupted.
Firewall Action	none
Recommended Action	Verify that the media is intact.
Revision	1

2.9.2. unable_to_allocate_static_entry (ID: 04600002)

Default Severity	WARNING
Log Message	Unable to allocate static entry for <host>
Explanation	Unable to allocate static entry. Unit is low on memory.
Firewall Action	no_block
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	host

2.9.3. unable_to_allocate_host_entry (ID: 04600003)

Default Severity	WARNING
Log Message	Unable to allocate dynamic entry for <host>
Explanation	Unable to allocate dynamic entry. Unit is low on memory.
Firewall Action	no_block
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	host

2.9.4. host_unblacklisted (ID: 04600004)

Default Severity	NOTICE
Log Message	Blacklist entry removed. Protocol: <proto>, Src Net: <srcnet>, Dst Net: <dstnet>, Port: <port>.
Explanation	A blacklist entry has been removed.
Firewall Action	None
Recommended Action	None.
Revision	4
Parameters	proto srcnet dstnet port

2.9.5. host_blacklisted (ID: 04600006)

Default Severity	NOTICE
Log Message	Blacklist entry added. Reason: <reason>, Protocol: <proto>, Src Net: <srcnet>, Dst Net: <dstnet>, Port: <port>.
Explanation	A blacklist entry was added.
Firewall Action	None
Recommended Action	None.
Revision	4
Parameters	reason proto srcnet dstnet port

2.9.6. botnet_src_detected (ID: 04600010)

Default Severity	NOTICE
Log Message	Source IP <ipaddr> has a low IP Reputation score (<reputation>) and is associated with botnets.
Explanation	The source IP address has a low reputation and is associated with botnets. The dynamic blacklist will temporarily block all communcation with that address.
Firewall Action	blacklist

Recommended Action	None.
Revision	1
Parameters	ipaddr reputation
Context Parameters	Rule Name Packet Buffer

2.9.7. botnet_dst_detected (ID: 04600011)

Default Severity	NOTICE
Log Message	Destination IP <ipaddr> has a low IP Reputation score (<reputation>) and is associated with botnets.
Explanation	The destination IP address has a low reputation and is associated with botnets. The dynamic blacklist will temporarily block all communcation with that address.
Firewall Action	blacklist
Recommended Action	None.
Revision	1
Parameters	ipaddr reputation
Context Parameters	Rule Name Packet Buffer

2.9.8. dos_src_detected (ID: 04600020)

Default Severity	NOTICE
Log Message	Source IP <ipaddr> has a low IP Reputation score (<reputation>) and is associated with Denial of Service attacks.
Explanation	The source IP address has a low reputation and is associated with Denial of Service attacks. The dynamic blacklist will temporarily block all traffic from that address.
Firewall Action	blacklist
Recommended Action	None.
Revision	1
Parameters	ipaddr reputation
Context Parameters	Rule Name Packet Buffer

2.9.9. disallowed_src_geo_detected (ID: 04600021)

Default Severity	NOTICE
Log Message	Source IP <ipaddr> originates from disallowed region <region>.
Explanation	The source IP address originates from a geographical region that is not allowed according to the configuration. The dynamic blacklist will temporarily block all traffic from that address.
Firewall Action	blacklist
Recommended Action	None.
Revision	1
Parameters	ipaddr region
Context Parameters	Rule Name Packet Buffer

2.9.10. scanner_src_detected (ID: 04600030)

Default Severity	NOTICE
Log Message	Source IP <ipaddr> has a low IP Reputation score (<reputation>) and is associated with malicious scanner activity.
Explanation	The source IP address has a low reputation and is associated with malicious scanner activity. The dynamic blacklist will temporarily block all traffic from that address.
Firewall Action	blacklist
Recommended Action	None.
Revision	1
Parameters	ipaddr reputation
Context Parameters	Rule Name Packet Buffer

2.9.11. malformed_request (ID: 04600040)

Default Severity	WARNING
Log Message	Malformed request sent to the blacklist handler in REST API
Explanation	The request was malformed, parameter missing, out of range or too long.

Firewall Action	None
Recommended Action	Review request data against documention.
Revision	1

2.10. BUFFERS

These log messages refer to the **BUFFERS (Events regarding buffer usage)** category.

2.10.1. buffers_flooded (ID: 00500001)

Default Severity	WARNING
Log Message	The buffers were flooded for <duration> seconds. Current usage is <buf_usage> percent
Explanation	The unit was temporarily out of buffers for a period of time. This could be a result of a period of heavy network traffic load.
Firewall Action	None
Recommended Action	If this is a reoccurring event, try increasing the number of HighBuffers.
Revision	1
Parameters	duration buf_usage

2.10.2. buffers_profile (ID: 00500002)

Default Severity	DEBUG
Log Message	Buffer requested by <reason> used at total of <duration> ticks and was touched <numstop> times
Explanation	A buffer associated with a profiling request has been identified. This log message will only be generated by special built firmware for the purpose of debugging.
Firewall Action	None
Recommended Action	Nothing.
Revision	1
Parameters	numstop duration reason
Context Parameters	Packet Buffer

2.11. CONN

These log messages refer to the **CONN (State engine events, e.g. open/close connections)** category.

2.11.1. conn_open (ID: 00600001)

Default Severity	INFORMATIONAL
Log Message	Connection opened
Explanation	A connection has been opened.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Connection Packet Buffer

2.11.2. conn_close (ID: 00600002)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Firewall Action	close
Recommended Action	None.
Revision	3
Parameters	reason
Context Parameters	Rule Information Connection

2.11.3. connection_table_full (ID: 00600003)

Default Severity	WARNING
Log Message	Closing (replacing) this connection; connection table full
Explanation	The connection table is currently full, and the unit needs to open a new connection. This specific connection is closed, and replaced with the new connection.
Firewall Action	replacing_conn

Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection

2.11.4. conn_open_natsat (ID: 00600004)

Default Severity	INFORMATIONAL
Log Message	Connection opened
Explanation	A connection has been opened.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Connection Packet Buffer

2.11.5. conn_close_natsat (ID: 00600005)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Firewall Action	close
Recommended Action	None.
Revision	3
Parameters	reason
Context Parameters	Rule Information Connection

2.11.6. out_of_connections (ID: 00600010)

Default Severity	WARNING
Log Message	Out of connections. Rejecting connection attempt
Explanation	The connection table is currently full, and this new connection attempt will be rejected.
Firewall Action	reject

Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.11.7. out_of_connections (ID: 00600011)

Default Severity	WARNING
Log Message	Out of connections. Dropping connection attempt
Explanation	The connection table is currently full, and this new connection attempt will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.11.8. no_new_conn_for_this_packet (ID: 00600012)

Default Severity	WARNING
Log Message	State inspector would not open a new connection for this TCP packet, rejecting
Explanation	State inspector would not open a new connection for this TCP packet since the combination of TCP flags is wrong. Only packets with the SYN TCP-flag set as the only TCP flag are allowed to open a new TCP connection.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	protocol
Context Parameters	Rule Name Packet Buffer

2.11.9. no_new_conn_for_this_packet (ID: 00600013)

Default Severity	WARNING
Log Message	State inspector would not open a new connection for this ICMP packet, dropping packet

Explanation	State inspector would not open a new connection for this ICMP packet since it is not an ICMP Echo Request. Only Echo Requests are allowed to open a new ICMP connection.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	protocol
Context Parameters	Rule Name Packet Buffer

2.11.10. no_return_route (ID: 00600014)

Default Severity	WARNING
Log Message	Failed to open a new connection since a return route to the sender address cant be found. Dropping packet
Explanation	There was no return route found to the sender address of the packet. Therefore, a new connection could not be opened and the packet is dropped.
Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.11.11. reverse_connect_attempt (ID: 00600015)

Default Severity	WARNING
Log Message	Disallowed reverse connect attempt from peer. Dropping
Explanation	State inspector does not allow this packet in reverse direction on the already opened connection. This type of packet is only allowed to be sent by the originator of a connection. Dropping the packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.11.12. unknown_icmpv6_type (ID: 00600016)

Default Severity	WARNING
Log Message	State inspector would not open a new connection for this ICMPv6 packet, dropping packet
Explanation	State inspector would not open a new connection for this ICMPb6 packet since it is not an ICMPv6 Echo Request. Only Echo Requests are allowed to open a new ICMPv6 connection.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	protocol
Context Parameters	Rule Name Packet Buffer

2.11.13. port_0_illegal (ID: 00600020)

Default Severity	WARNING
Log Message	TCP/UDP destination port or TCP source port was set to 0. Dropping
Explanation	The TCP/UDP destination or TCP source port was set to 0, which is not allowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.11.14. udp_src_port_0_illegal (ID: 00600021)

Default Severity	WARNING
Log Message	UDP source port is set to 0. Dropping
Explanation	The UDP source port was set to 0. This can be used by UDP streams not expecting return traffic. Dropping packet.
Firewall Action	drop
Recommended Action	If the packet is wanted, change the UDP source port 0 setting.
Revision	1

Context Parameters	Rule Name Packet Buffer

2.11.15. udp_src_port_0_forwarded (ID: 00600022)

Default Severity	WARNING
Log Message	UDP source port is set to 0. Forwards packet
Explanation	The UDP source port was set to 0. This can be used by UDP streams not expecting return traffic. Forwarding packet.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.11.16. conn_usage (ID: 00600023)

Default Severity	INFORMATIONAL
Log Message	Connection used to forward a packet.
Explanation	A packet has passed through the connection.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	Packet Buffer

2.11.17. conn_close (ID: 00600032)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	reason
Context Parameters	Rule Information

Connection

2.11.18. conn_close (ID: 00600033)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Firewall Action	close
Recommended Action	None.
Revision	3
Parameters	reason
Context Parameters	Rule Information Connection

2.11.19. conn_close_natsat (ID: 00600035)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	reason
Context Parameters	Rule Information Connection

2.11.20. active_data (ID: 00600100)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Incoming active data channel
Explanation	An active data channel connection has been established.
Firewall Action	None
Recommended Action	None.
Revision	1

Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.11.21. passive_data (ID: 00600101)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Incoming passive data channel
Explanation	A passive data channel connection has been established.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.11.22. active_data (ID: 00600102)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Active data channel closed
Explanation	An active data channel was closed.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.11.23. passive_data (ID: 00600103)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Passive data channel closed
Explanation	A passive data channel was closed.
Firewall Action	None
Recommended Action	None.

Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.11.24. ip_reputation (ID: 00600120)

Default Severity	INFORMATIONAL
Log Message	IP address reputation query result.
Explanation	The reputation and possibly threat category association of the public IP address.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	ip score categories
Context Parameters	Connection

2.11.25. ip_reputation_query_failed (ID: 00600121)

Default Severity	WARNING
Log Message	IP address reputation query failed.
Explanation	The IP reputation query failed. The reason for this is specified in the "reason" parameter.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	ip reason
Context Parameters	Connection

2.11.26. ip_reputation_query_timeout (ID: 00600122)

Default Severity	WARNING
Log Message	IP address reputation query timed out.

Explanation	The IP reputation query failed. The connection timed out.
Firewall Action	none
Recommended Action	Verify that the unit has been configured with Internet access.
Revision	1
Parameters	ip
Context Parameters	Connection

2.12. DHCP

These log messages refer to the **DHCP (DHCP client events)** category.

2.12.1. offered_ip_occupied (ID: 00700001)

Default Severity	NOTICE
Log Message	Interface <iface> received a lease with an offered IP that appear to be occupied (<ip4addr>)
Explanation	Received a DHCP lease which appears to be in use by someone else.
Firewall Action	restart
Recommended Action	Check network for statically configured hosts or incorrectly proxy ARPed routes.
Revision	1
Parameters	iface ip4addr

2.12.2. lease_changed (ID: 00700002)

Default Severity	WARNING
Log Message	Some vital parameter(s) in the lease on interface <iface> have changed, restarting DHCP-process
Explanation	The DHCP server have updated some information considered vital. This will result in the DHCP process being restarted.
Firewall Action	reconfiguration
Recommended Action	None.
Revision	2
Parameters	iface lease_changes
Context Parameters	Packet Buffer

2.12.3. lease_acquired (ID: 00700003)

Default Severity	NOTICE
Log Message	Interface <iface> have successfully acquired a lease
Explanation	An interface have successfully acquired a lease.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	iface ip netmask bcast gw
Context Parameters	Packet Buffer

2.12.4. renewed_lease (ID: 00700004)

Default Severity	NOTICE
Log Message	Interface <iface> have renewed its lease. The new lease is valid for <valid_seconds> seconds
Explanation	An interface have successfully renewed its lease.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface valid_seconds
Context Parameters	Packet Buffer

2.12.5. lease_expired (ID: 00700005)

Default Severity	NOTICE
Log Message	Interface <iface> lease expired
Explanation	A lease have expired and the ip data for this interface are no longer valid.
Firewall Action	restart
Recommended Action	Check connection and DHCP server reachability.
Revision	1
Parameters	iface

2.12.6. invalid_lease_time (ID: 00700007)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with a leasetime (<lease_time>)

	which is lower then the minimum allowed (<minimum_lease_time>)
Explanation	An interface received a lease with a leasetime which is lower then the configured minimum.
Firewall Action	drop
Recommended Action	Check the DHCP server configuration or adjust the minimum leasetime limit.
Revision	1
Parameters	iface lease_time minimum_lease_time
Context Parameters	Packet Buffer

2.12.7. invalid_server_id (ID: 00700008)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid server ID (<server_id>)
Explanation	An interface received a lease with an invalid server ID parameter.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface server_id
Context Parameters	Packet Buffer

2.12.8. invalid_netmask (ID: 00700009)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid netmask (<netmask>)
Explanation	An interface received a lease with an invalid netmask.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface netmask

Context Parameters	Packet Buffer

2.12.9. invalid_broadcast (ID: 00700010)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid broadcast address (<broadcast>)
Explanation	An interface received a lease with an invalid broadcast address.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface broadcast
Context Parameters	Packet Buffer

2.12.10. invalid_offered_ip (ID: 00700011)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid offered IP (<offered_ip>)
Explanation	An interface received a lease with an invalid offered IP address.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface offered_ip
Context Parameters	Packet Buffer

2.12.11. invalid_gateway (ID: 00700012)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid gateway (<gateway>)
Explanation	An interface received a lease with an invalid gateway address.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.

Revision	1
Parameters	iface gateway
Context Parameters	Packet Buffer

2.12.12. offered_broadcast_equals_gateway (ID: 00700013)

Default Severity	WARNING
Log Message	Interface <iface> received a lease where the offered broadcast equals the offered gateway
Explanation	An interface received a lease where the offered broadcast address is equal with the offered gateway address.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface
Context Parameters	Packet Buffer

2.12.13. ip_collision (ID: 00700014)

Default Severity	WARNING
Log Message	Interface <iface> received a lease which if used will cause an IP collision (DHCP IP: <dhcp_ip> collides with configured route: <configured_route>)
Explanation	An interface received a lease which if used will cause an IP collision with a configured route.
Firewall Action	drop
Recommended Action	Check DHCP server configuration and the SG interface configuration.
Revision	1
Parameters	iface dhcp_ip configured_route
Context Parameters	Packet Buffer

2.12.14. route_collision (ID: 00700015)

Default Severity	WARNING

Log Message	Interface <iface> received a lease which if used will cause a route collision (DHCP route: <dhcp_route> collides with configured route <configured_route>)
Explanation	An interface received a lease which if used will cause a route collision with a configured route.
Firewall Action	drop
Recommended Action	Check DHCP server configuration and SG interface configuration.
Revision	1
Parameters	iface dhcp_route configured_route
Context Parameters	Packet Buffer

2.13. DHCPRELAY

These log messages refer to the **DHCPRELAY (DHCP relayer events)** category.

2.13.1. unable_to_save_dhcp_relay_list (ID: 00800001)

Default Severity	WARNING
Log Message	Unable to auto save the DHCP relay list to disk
Explanation	Unable to autosave the DHCP relay list to disk.
Firewall Action	None
Recommended Action	Check disk usage and health.
Revision	1

2.13.2. dhcp_relay_list_saved (ID: 00800002)

Default Severity	NOTICE
Log Message	DHCP relay list was successfully auto saved to disk
Explanation	The DHCP relay list was successfully written to disk.
Firewall Action	None
Recommended Action	None.
Revision	1

2.13.3. dhcp_pkt_too_small (ID: 00800003)

Default Severity	NOTICE
Log Message	Received DHCP packet which is smaller then the minimum allowed 300 bytes.
Explanation	Received a DHCP packet which is smaller then the minimum allowed 300 bytes.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.13.4. incorrect_bootp_dhcp_cookie (ID: 00800004)

Default Severity	WARNING
Log Message	Incorrect BOOTP/DHCP cookie. Dropping
Explanation	Received a packet with an incorrect BOOTP/DHCP cookie.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.13.5. maximum_ppm_for_relayer_reached (ID: 00800005)

Default Severity	WARNING
Log Message	The maximum packets-per-minute limit have been reached. Requests will be denied for a period of time
Explanation	The maximum DHCP packets-per-minute limit for the relayer have been reached.
Firewall Action	None
Recommended Action	Verify packets-per-minute limit.
Revision	1
Context Parameters	Packet Buffer

2.13.6. relayer_resuming (ID: 00800006)

Default Severity	NOTICE
Log Message	The relayer is now resuming, <packets_dropped> packets were dropped while the relayer was inactive
Explanation	The relayer is now resuming its duties since being temporary halted by the packets-per-minute limit.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	packets_dropped
Context Parameters	Packet Buffer

2.13.7. hop_limit_exceeded (ID: 00800007)

Default Severity	WARNING
Log Message	Hop limit exceeded. Dropping
Explanation	The maxmimum hop limit for the DHCP packet have been reached.
Firewall Action	None
Recommended Action	Verify maximum-hop-limit setting.
Revision	1
Context Parameters	Packet Buffer

2.13.8. client_release (ID: 00800008)

Default Severity	WARNING
Log Message	Client <client_ip> requested release. Relay canceled
Explanation	A client requested that lease should be canceled.
Firewall Action	relay_canceled
Recommended Action	None.
Revision	1
Parameters	client_ip
Context Parameters	Packet Buffer

2.13.9. got_reply_without_transaction_state (ID: 00800009)

Default Severity	WARNING
Log Message	Got server reply without transaction state for client <client_hw>. Dropping
Explanation	Received a server reply without a matching transaction state.
Firewall Action	drop
Recommended Action	Check the network environment for errors.
Revision	1
Parameters	client_hw
Context Parameters	Packet Buffer

2.13.10. maximum_dhcp_client_relay_routes_reached (ID: 00800010)

Default Severity	WARNING
Log Message	The limit for concurrent DHCP relay routes have been reached. Dropping
Explanation	The DHCP relay routes limit have been reached.
Firewall Action	drop
Recommended Action	Verify max-relay-routes-limit.
Revision	1
Context Parameters	Rule Name

2.13.11. unable_to_add_relay_route_since_out_of_memory (ID: 00800011)

Default Severity	ERROR
Log Message	Internal Error: Out of memory: Can't add DHCP relay route. Dropping
Explanation	Unable to add DHCP relay route since out of memory.
Firewall Action	drop
Recommended Action	Check firewall memory consumption.
Revision	1
Context Parameters	Rule Name

2.13.12. ignored_relay_request (ID: 00800012)

Default Severity	WARNING
Log Message	Request ignored according to the ruleset
Explanation	A DHCP relay request was ignored according to the rules.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.13. no_message_type (ID: 00800013)

Default Severity	WARNING

Log Message	No message type. Dropping
Explanation	Received DHCP packet without the required message type parameter.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.14. bad_inform_pkt_with_mismatching_source_ip_and_client_ip (ID: 00800014)

Default Severity	WARNING
Log Message	INFORM packet did not pass through a relayer but the packet source ip and the client ip doesnt match. Dropping
Explanation	Received non relayed INFORM DHCP packet with illegally mismatching source and client IP.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.15. received_relayed_inform_packet_without_client_ip (ID: 00800015)

Default Severity	WARNING
Log Message	INFORM packet passed a relayer but the client ip isnt set. Dropping
Explanation	Received relayed INFORM DHCP packet with illegally missing client IP.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.16. maximum_current_dhcp_relays_for_iface (ID:

00800016)

Default Severity	WARNING
Log Message	The maximum number <max_relays> of current DHCP relays for this interface have been reached. Dropping
Explanation	The maximum number of DHCP relayed through a specified interface have been reached.
Firewall Action	drop
Recommended Action	Verify max-relay-per-interface setting.
Revision	1
Parameters	max_relays
Context Parameters	Rule Name Packet Buffer

2.13.17. dhcp_server_is_unroutable (ID: 00800017)

Default Severity	WARNING
Log Message	BOOTP/DHCP-server at <dest_ip> is unroutable. Dropping
Explanation	Unable to find route to specified DHCP server.
Firewall Action	drop
Recommended Action	Update routing table with a route to the DHCP server.
Revision	1
Parameters	dest_ip
Context Parameters	Rule Name Packet Buffer

2.13.18. unable_to_get_free_transaction_state (ID: 00800018)

Default Severity	WARNING
Log Message	Unable to get free transaction state for client <client_hw>. Dropping
Explanation	Unable to get a free transaction state to handle client request.
Firewall Action	drop
Recommended Action	Verify max-transaction-count setting.
Revision	1
Parameters	client_hw

Context Parameters	Rule Name Packet Buffer

2.13.19. invalid_gateway (ID: 00800019)

Default Severity	WARNING
Log Message	Received request with invalid gateway (<gateway_ip>). Dropping
Explanation	Received DHCP request with an invalid gateway.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name Packet Buffer

2.13.20. relayed_request (ID: 00800020)

Default Severity	NOTICE
Log Message	Relayed DHCP-request <type> from client <client_hw> to <dest_ip>
Explanation	Relayed a DHCP request.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	type client_hw dest_ip
Context Parameters	Rule Name Packet Buffer

2.13.21. relayed_request (ID: 00800021)

Default Severity	NOTICE
Log Message	Relayed BOOTP-request from client <client_hw> to <dest_ip>
Explanation	Relayed a BOOTP request.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	client_hw dest_ip
Context Parameters	Rule Name Packet Buffer

2.13.22. got_reply_on_a_non_security_equivalent_interface (ID: 00800022)

Default Severity	WARNING
Log Message	Received reply for client <client_hw> on a non security equivalent interface. Dropping
Explanation	Received a reply for a client on a non security equivalent interface.
Firewall Action	drop
Recommended Action	Verify security-equivalent-interface setting.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.13.23. assigned_ip_not_allowed (ID: 00800023)

Default Severity	WARNING
Log Message	DHCP/BOOTP-Server <server_ip> gave out an IP <ip> which isn't accepted. Dropping
Explanation	Received a lease with an IP which is not accepted according to the rules.
Firewall Action	drop
Recommended Action	Verify allowed-lease-addresses setting.
Revision	1
Parameters	iface server_ip ip
Context Parameters	Rule Name Packet Buffer

2.13.24. illegal_client_ip_assignment (ID: 00800024)

Default Severity	WARNING
Log Message	DHCP/BOOTP-Server <server_ip> tried to assign a client with an illegal IP <ip>. Dropping
Explanation	Received a lease with an illegal client assignment IP.
Firewall Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	server_ip ip
Context Parameters	Rule Name Packet Buffer

2.13.25. ambiguous_host_route (ID: 00800025)

Default Severity	WARNING
Log Message	A host route for <dest_ip> already exists which points to another interface. Dropping
Explanation	An ambiguous host route indicating another interface was detected trying to setup a dynamic hostroute for a client.
Firewall Action	drop
Recommended Action	Review previous configured host route for client.
Revision	1
Parameters	dest_ip
Context Parameters	Rule Name Packet Buffer

2.13.26. relayed_dhcp_reply (ID: 00800026)

Default Severity	NOTICE
Log Message	Relayed DHCP-reply <type> to client <client_hw>
Explanation	Relayed DHCP reply to client.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	type client_hw

Context Parameters	Rule Name Packet Buffer

2.13.27. relayed_bootp_reply (ID: 00800027)

Default Severity	NOTICE
Log Message	Relayed BOOTP-reply to client <client_hw>
Explanation	Relayed BOOTP reply to client.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.13.28. relayed_dhcp_reply (ID: 00800028)

Default Severity	NOTICE
Log Message	Relayed DHCP-reply <type> to gateway <gateway_ip>
Explanation	Relayed DHCP reply to a gateway.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	type gateway_ip
Context Parameters	Rule Name Packet Buffer

2.13.29. relayed_bootp_reply (ID: 00800029)

Default Severity	NOTICE
Log Message	Relayed BOOTP-reply to gateway <gateway_ip>
Explanation	Relayed BOOTP reply to a gateway.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name Packet Buffer

2.14. DHCPSERVER

These log messages refer to the **DHCPSERVER (DHCP server events)** category.

2.14.1. unable_to_send_response (ID: 00900001)

Default Severity	WARNING
Log Message	Failed to get buffer for sending. Unable to reply
Explanation	Unable to get a buffer for sending.
Firewall Action	None
Recommended Action	Check buffer consumption.
Revision	1

2.14.2. option_section_is_too_big_unable_to_reply (ID: 00900002)

Default Severity	WARNING
Log Message	The option section is too big, unable to reply. Dropping
Explanation	Unable to send reply since the DHCP option section is too big.
Firewall Action	drop
Recommended Action	Reduce the number of used DHCP options.
Revision	1

2.14.3. unable_to_save_lease_db (ID: 00900003)

Default Severity	WARNING
Log Message	Unable to auto save the lease database to disk
Explanation	Some sort of error occurred saving the lease database to disk.
Firewall Action	None
Recommended Action	Make sure that there is sufficient diskspace available.
Revision	1

2.14.4. lease_db_successfully_saved (ID: 00900004)

Default Severity	NOTICE

Log Message	Lease database was successfully auto saved to disk
Explanation	The lease database was successfully saved to disk.
Firewall Action	None
Recommended Action	None.
Revision	1

2.14.5. dhcp_packet_too_small (ID: 00900005)

Default Severity	WARNING
Log Message	Received DHCP packet which is smaller then the minimum allowed 300 bytes. Dropping
Explanation	Received a DHCP packet which is smaller then the minimum allowed 300 bytes.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.14.6. request_for_ip_from_non_bound_client_without_state (ID: 00900006)

Default Severity	WARNING
Log Message	Received a request from client(not in bound) <client> for IP <client_ip> without state. Rejecting
Explanation	Received a request from a non bound client without state.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.14.7. request_for_ip_from_bound_client_without_state (ID: 00900007)

Default Severity	WARNING

Log Message	Received a request from client(in bound) <client> for IP <client_ip> without state. Rejecting
Explanation	Received a request from a bound client without state.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.14.8. request_for_ip_from_non_bound_client_without_state (ID: 00900008)

Default Severity	WARNING
Log Message	Received a request from client(not in bound) <client> for IP <client_ip> without state. Ignoring
Explanation	Received a request from an unbound client without state.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.14.9. all_ip_pools_depleted (ID: 00900010)

Default Severity	WARNING
Log Message	All IP pools are depleted. Unable to handle request. Ignoring
Explanation	All IP pools have been depleted.
Firewall Action	None
Recommended Action	Extend the pools to support more clients.
Revision	1
Context Parameters	Packet Buffer

2.14.10. request_with_bad_udp_checksum (ID: 00900011)

Default Severity	WARNING
Log Message	Received request with bad UDP checksum. Dropping
Explanation	Received request with bad UDP checksum.
Firewall Action	drop
Recommended Action	Check network equipment for errors.
Revision	1
Context Parameters	Packet Buffer

2.14.11. lease_timeout (ID: 00900012)

Default Severity	NOTICE
Log Message	Lease for IP <client_ip> timed out. Was bound to client <client_hw>
Explanation	A client lease wasn't renewed and timed out.
Firewall Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip client_hw
Context Parameters	Rule Name

2.14.12. lease_timeout (ID: 00900013)

Default Severity	NOTICE
Log Message	Offer for IP <client_ip> timed out. Was offered to client <client_hw>
Explanation	An offer to a client was never accepted and timed out.
Firewall Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip client_hw
Context Parameters	Rule Name

2.14.13. pool_depleted (ID: 00900014)

Default Severity	WARNING
Log Message	All IPs in the pool are in use. Request cannot be fulfilled
Explanation	A request cannot be fullfilled since all pools are in use.
Firewall Action	None
Recommended Action	Extend the pools to support more clients.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.14.14. sending_offer (ID: 00900015)

Default Severity	NOTICE
Log Message	Received DISCOVER from client <client_hw>. Sending IP offer <offer_ip>
Explanation	Received discover (initial IP query) from a client.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	client_hw offer_ip client_hostname client_vendorclass client_params
Context Parameters	Rule Name Packet Buffer

2.14.15. pool_depleted (ID: 00900016)

Default Severity	NOTICE
Log Message	All IPs in the pool are now in use
Explanation	All IPs the the pool have been consumed.
Firewall Action	None
Recommended Action	Extend the pool to support more clients.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.14.16. request_for_non_offered_ip (ID: 00900017)

Default Severity	WARNING
Log Message	Client <client_hw> requested non offered IP. Rejecting
Explanation	Client sent a request for a non offered IP.
Firewall Action	nak
Recommended Action	None.
Revision	1
Parameters	client_hw client_wanted client_offered
Context Parameters	Rule Name Packet Buffer

2.14.17. request_for_non_bound_ip (ID: 00900018)

Default Severity	WARNING
Log Message	Client <client_hw> requested non bound IP. Rejecting
Explanation	Client requested a non bound IP.
Firewall Action	reject
Recommended Action	None.
Revision	1
Parameters	client_hw client_wanted bound
Context Parameters	Rule Name Packet Buffer

2.14.18. client_bound (ID: 00900019)

Default Severity	NOTICE
Log Message	Client <client_hw> accepted IP <client_ip>. Client is now bound
Explanation	Client accepted the IP address and are now bound.
Firewall Action	new_lease
Recommended Action	None.
Revision	3

Parameters	client_hw client_ip client_hostname client_vendorclass client_params
Context Parameters	Rule Name Packet Buffer

2.14.19. client_renewed (ID: 00900020)

Default Severity	NOTICE
Log Message	Client <client_hw> renewed IP <client_ip>
Explanation	Client successfully renewed its lease.
Firewall Action	renew
Recommended Action	None.
Revision	3
Parameters	client_hw client_ip client_hostname client_vendorclass client_params
Context Parameters	Rule Name Packet Buffer

2.14.20. got_inform_request (ID: 00900021)

Default Severity	NOTICE
Log Message	Got INFORM request from client <client_hw>. Acknowledging
Explanation	Got an inform (client already got an IP and asks for configuration parameters) request from a client.
Firewall Action	acknowledging
Recommended Action	None.
Revision	2
Parameters	client_hw client_ip client_hostname client_vendorclass client_params
Context Parameters	Rule Name Packet Buffer

2.14.21. decline_for_ip_on_wrong_iface (ID: 00900022)

Default Severity	NOTICE
Log Message	Got decline for ip <client_ip> on wrong interface (recv: <recv_if>, lease: <client_if>). Decline is ignored
Explanation	Got decline from a client on the wrong interface.
Firewall Action	None
Recommended Action	Check network for inconsistent routes.
Revision	1
Parameters	client_hw client_ip recv_if client_if
Context Parameters	Rule Name Packet Buffer

2.14.22. decline_for_non_offered_ip (ID: 00900023)

Default Severity	NOTICE
Log Message	Client <client_hw> declined non offered IP. Decline is ignored
Explanation	Client rejected non a offered IP.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.14.23. declined_by_client (ID: 00900024)

Default Severity	WARNING
Log Message	Client <client_hw> declined IP <client_ip>. IP blacklisted
Explanation	A client declined (indicated that the IP is already in use someone else) offered IP.
Firewall Action	blacklist
Recommended Action	Check network for statically configured hosts or incorrectly proxy

ARPed routes.

Revision 1

Parameters client_hw
client_ip

Context Parameters Rule Name
Packet Buffer

2.14.24. request_for_ip_from_bound_client_without_state (ID: 00900025)

Default Severity WARNING

Log Message Received a request from client(bound) <client> for IP <client_ip> without state. Ignoring

Explanation Received a request from a bound client without state.

Firewall Action None

Recommended Action None.

Revision 1

Parameters client
client_ip

Context Parameters Packet Buffer

2.14.25. release_for_ip_on_wrong_iface (ID: 00900026)

Default Severity WARNING

Log Message Got release for ip <client_ip> on wrong interface (recv: <recv_if>, lease: <client_if>). Decline is ignored

Explanation Got release from a client on the wrong interface.

Firewall Action None

Recommended Action Check network for inconsistent routes.

Revision 1

Parameters client_hw
client_ip
recv_if
client_if

Context Parameters Rule Name
Packet Buffer

2.14.26. released_by_client (ID: 00900027)

Default Severity	NOTICE
Log Message	Client <client_hw> released IP <client_ip>.
Explanation	A client released (prematuraly ended) its lease.
Firewall Action	lease_released
Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.15. DHCPV6CLIENT

These log messages refer to the **DHCPV6CLIENT (DHCPv6 Client Events)** category.

2.15.1. offered_ip_occupied (ID: 07300001)

Default Severity	NOTICE
Log Message	Interface <iface> received a lease with an offered IP that appear to be occupied (<ip6addr>)
Explanation	Received a DHCPv6 lease which appears to be in use by someone else.
Firewall Action	restart
Recommended Action	Check network for statically configured hosts.
Revision	1
Parameters	iface ip6addr

2.15.2. lease_acquired (ID: 07300003)

Default Severity	NOTICE
Log Message	Interface <iface> have successfully acquired a lease
Explanation	An interface have successfully acquired a lease.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	iface ip dns1 dns2
Context Parameters	Packet Buffer

2.15.3. renewed_lease (ID: 07300004)

Default Severity	NOTICE
Log Message	Interface <iface> have renewed its lease. The new lease is valid for <valid_seconds> seconds
Explanation	An interface have successfully renewed its lease.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	iface valid_seconds
Context Parameters	Packet Buffer

2.15.4. lease_expired (ID: 07300005)

Default Severity	NOTICE
Log Message	Interface <iface> lease expired
Explanation	A lease have expired and the ip data for this interface are no longer valid.
Firewall Action	restart
Recommended Action	Check connection and DHCP6 server reachability.
Revision	1
Parameters	iface

2.15.5. adv_bad_status (ID: 07300006)

Default Severity	WARNING
Log Message	DHCPv6 server Advertisment unsuccessful status on <iface>. Status: <code>.
Explanation	A DHCPv6 Advertisment was received containing a bad status code.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	code iface

2.15.6. reply_bad_status (ID: 07300007)

Default Severity	WARNING
Log Message	DHCPv6 server Reply unsuccessful status on <iface>. Status: <code>.
Explanation	A DHCPv6 Reply was received containing a bad status code.
Firewall Action	drop

Recommended Action	None.
Revision	1
Parameters	code iface

2.15.7. bad_server_address (ID: 07300008)

Default Severity	WARNING
Log Message	DHCPv6 server Reply contained a bad server address <address> on <iface>.
Explanation	A DHCPv6 Reply was received containing a bad server address.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	address iface

2.15.8. bad_address_offered (ID: 07300009)

Default Severity	WARNING
Log Message	DHCPv6 server Reply offered a bad address <address> on <iface>.
Explanation	A DHCPv6 Reply was received containing a bad ip address.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	address iface

2.15.9. bad_timers (ID: 07300010)

Default Severity	WARNING
Log Message	DHCPv6 server Reply IA_NA option timer T1 <t1> is erroneously larger than T2 <t2> on <iface>.
Explanation	A DHCPv6 Reply IA_NA option with faulty timers was received.
Firewall Action	drop
Recommended Action	None.

Revision	1
Parameters	t1 t2 iface

2.15.10. low_life_time (ID: 07300011)

Default Severity	WARNING
Log Message	DHCPv6 server Reply IA_NA offered address lifetime too low on <iface>. Preferred lifetime <preferred>, valid lifetime <valid>.
Explanation	A DHCPv6 Reply IA_NA option was received containing an address life time too low.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	preferred valid iface

2.15.11. ip_collision (ID: 07300012)

Default Severity	WARNING
Log Message	Interface <iface> received an offer which if used will cause an IP collision (DHCPv6 IP: <dhcpv6_ip> collides with configured route: <configured_route>)
Explanation	An interface received an offer which if used will cause an IP collision with a configured route.
Firewall Action	drop
Recommended Action	Check DHCPv6 server configuration and the SG interface configuration.
Revision	1
Parameters	iface dhcpv6_ip configured_route

2.16. DHCPV6SERVER

These log messages refer to the **DHCPV6SERVER (DHCPv6 Server Events)** category.

2.16.1. client_id_missing (ID: 07400001)

Default Severity	WARNING
Log Message	Client ID option missing in received message.
Explanation	The received packet is missing vital information.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.16.2. server_id_missing (ID: 07400002)

Default Severity	WARNING
Log Message	Server ID option missing in received message.
Explanation	The received packet is missing vital information.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.16.3. client_id_unexpected (ID: 07400003)

Default Severity	WARNING
Log Message	Unexpected Client ID option in received message.
Explanation	The received message contains unexpected information.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used. Dropping.
Revision	1
Context Parameters	Packet Buffer

2.16.4. server_id_unexpected (ID: 07400004)

Default Severity	WARNING
Log Message	Unexpected Server ID option in received message.
Explanation	The received message contains unexpected information.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used. Dropping.
Revision	1
Context Parameters	Packet Buffer

2.16.5. unable_to_send_response (ID: 07400005)

Default Severity	WARNING
Log Message	Failed to get buffer for reply message.
Explanation	Unable to get a buffer for sending.
Firewall Action	None
Recommended Action	Check buffer consumption.
Revision	1

2.16.6. sending_reply (ID: 07400006)

Default Severity	NOTICE
Log Message	Received SOLICIT with Rapid Commit option from client <client_hw> on <iface>. Sending IP offer <offer_ip>.
Explanation	Received Solicit message with Rapid Commit option from a client.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	client_hw iface offer_ip

2.16.7. sending_reply (ID: 07400007)

Default Severity	NOTICE
Log Message	Received REQUEST from client <client_hw> on <iface>. Sending IP offer <offer_ip>.

Explanation	Received Request message from a client.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	client_hw iface offer_ip

2.16.8. client_renewed (ID: 07400008)

Default Severity	NOTICE
Log Message	Client <client_hw> on <iface> renewed IP <client_ip>.
Explanation	Client successfully renewed its address lease.
Firewall Action	renew
Recommended Action	None.
Revision	1
Parameters	client_hw iface client_ip

2.16.9. client_rebound (ID: 07400009)

Default Severity	NOTICE
Log Message	Client <client_hw> on <iface> renewed IP <client_ip>.
Explanation	Client successfully rebound its address lease.
Firewall Action	rebind
Recommended Action	None.
Revision	1
Parameters	client_hw iface client_ip

2.16.10. lease_timeout (ID: 07400010)

Default Severity	NOTICE
Log Message	Lease for IP <client_ip> timed out.

Explanation	A client lease wasn't renewed and timed out.
Firewall Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.16.11. pool_depleted (ID: 07400011)

Default Severity	WARNING
Log Message	All IPs in the pool are now in use. Request for new IP address cannot be fulfilled.
Explanation	A request for new IP address cannot be fulfilled since all addresses are in use.
Firewall Action	none
Recommended Action	Extend the pool to support more IP addresses.
Revision	1
Context Parameters	Rule Name

2.16.12. bad_udp_checksum (ID: 07400012)

Default Severity	WARNING
Log Message	Received DHCPv6 packet with bad UDP checksum. Dropping.
Explanation	Received DHCPv6 packet with bad UDP checksum.
Firewall Action	drop
Recommended Action	Check network equipment for errors.
Revision	1
Context Parameters	Packet Buffer

2.16.13. dhcpv6_packet_too_small (ID: 07400013)

Default Severity	WARNING
Log Message	Received DHCPv6 packet which is smaller then the minimum allowed bytes. Dropping.
Explanation	Received a DHCPv6 packet which is smaller then the minimum

	allowed bytes.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.16.14. dhcpv6_faulty_length (ID: 07400014)

Default Severity	WARNING
Log Message	Received DHCPv6 packet with faulty length. Dropping.
Explanation	Received a DHCPv6 packet with mismatching lengths calculated from IP- and UDP-layers.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.16.15. invalid_options_length (ID: 07400015)

Default Severity	WARNING
Log Message	Received DHCPv6 packet with faulty options size. Dropping.
Explanation	Received a DHCPv6 packet with unexpected option sizes.
Firewall Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.16.16. lease_db_successfully_saved (ID: 07400016)

Default Severity	NOTICE
Log Message	Lease database was successfully auto saved to disk
Explanation	The lease database was successfully saved to disk.
Firewall Action	None
Recommended Action	None.

Revision	1

2.16.17. unable_to_save_lease_db (ID: 07400017)

Default Severity	WARNING
Log Message	Unable to auto save the lease database to disk
Explanation	Some sort of error occurred saving the lease database to disk.
Firewall Action	None
Recommended Action	Make sure that there is sufficient diskspace available.
Revision	1

2.16.18. unexpected_advertise_message (ID: 07400018)

Default Severity	NOTICE
Log Message	Unexpected message type (Advertise) in received packet.
Explanation	Received DHCPv6 packet with unexpected message type (Advertise).
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Packet Buffer

2.16.19. unexpected_reply_message (ID: 07400019)

Default Severity	NOTICE
Log Message	Unexpected message type (Reply) in received packet.
Explanation	Received DHCPv6 packet with unexpected message type (Reply).
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Packet Buffer

2.16.20. unexpected_reconfigure_message (ID: 07400020)

Default Severity	NOTICE
Log Message	Unexpected message type (Reconfigure) in received packet.
Explanation	Received DHCPv6 packet with unexpected message type (Reconfigure).
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Packet Buffer

2.16.21. unexpected_relay_reply_message (ID: 07400021)

Default Severity	NOTICE
Log Message	Unexpected message type (Relay-reply) in received packet.
Explanation	Received DHCPv6 packet with unexpected message type (Relay-reply).
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Packet Buffer

2.16.22. unexpected_unknown_message (ID: 07400022)

Default Severity	NOTICE
Log Message	Unexpected message type <message_type> in received packet.
Explanation	Received DHCPv6 packet with unexpected message type (message_type).
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	message_type
Context Parameters	Packet Buffer

2.17. DNSCACHE

These log messages refer to the **DNSCACHE (DNS Cache)** category.

2.17.1. ipv6_max_addresses (ID: 08000001)

Default Severity	WARNING
Log Message	FQDN object <name> reached the limit for IPv6 addresses.
Explanation	Maximum number of IP addresses for the FQDN has been exceeded.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	name

2.17.2. ipv4_max_addresses (ID: 08000002)

Default Severity	WARNING
Log Message	FQDN object <name> reached the limit for IPv4 addresses.
Explanation	Maximum number of IP addresses for the FQDN has been exceeded.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	name

2.17.3. update_matched_wfqdn (ID: 08000003)

Default Severity	NOTICE
Log Message	Matched an FQDN object with a Wildcard FQDN and adding an IP address.
Explanation	Matched an FQDN object with a Wildcard FQDN and adding an IP address.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	matched_name matched_address

address

2.17.4. dns_cache_freeip4entry (ID: 08000004)

Default Severity	NOTICE
Log Message	Removing an IP address from an FQDN object.
Explanation	Removing an IP address from an FQDN object.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	fqdn removed_address

2.18. DOWNLOAD

These log messages refer to the **DOWNLOAD (File Download)** category.

2.18.1. download_verification_error (ID: 08300001)

Default Severity	WARNING
Log Message	Download verification failed.
Explanation	A file downloaded could not be verfied.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	url file error

2.18.2. download_failed (ID: 08300002)

Default Severity	WARNING
Log Message	Download failed.
Explanation	A file downloaded failed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	url file error

2.18.3. download_start_failure (ID: 08300003)

Default Severity	WARNING
Log Message	Download start failure.
Explanation	A file downloaded could not be started.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters	url file error

2.18.4. download_resumed (ID: 08300004)

Default Severity	WARNING
Log Message	Resumed Download.
Explanation	A file downloaded was resumed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	url file

2.19. DYNROUTING

These log messages refer to the **DYNROUTING (Dynamic routing)** category.

2.19.1. failed_to_export_route_to_ospf_process_failed_to_alloc (ID: 01100001)

Default Severity	CRITICAL
Log Message	Failed to export route to OSPF process (unable to alloc export node)
Explanation	Unable to export route to a OSPF process since out of memory.
Firewall Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.19.2. route_exported_to_ospf_as (ID: 01100002)

Default Severity	NOTICE
Log Message	Route exported to OSPF AS
Explanation	A route was just exported to a OSPF AS.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.19.3. route_unexported_from_ospf_as (ID: 01100003)

Default Severity	NOTICE
Log Message	Route unexported from OSPF AS
Explanation	A route was just unexported from a OSPF AS.
Firewall Action	None
Recommended Action	None.

Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.19.4. failed_to_add_route_unable_to_alloc (ID: 01100004)

Default Severity	CRITICAL
Log Message	Failed to add route (unable to alloc route)
Explanation	Failed to create a route since out of memory.
Firewall Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.19.5. route_added (ID: 01100005)

Default Severity	NOTICE
Log Message	Route added
Explanation	A route was just added.
Firewall Action	None
Recommended Action	None.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.19.6. route_removed (ID: 01100006)

Default Severity	NOTICE
Log Message	Route removed
Explanation	A route was just removed.
Firewall Action	None
Recommended Action	None.

Revision 1

Context Parameters Dynamic Route
Rule Name
Route

2.20. FRAG

These log messages refer to the **FRAG (Fragmentation events)** category.

2.20.1. individual_frag_timeout (ID: 02000001)

Default Severity	WARNING
Log Message	Individual fragment timed out.
Explanation	A fragment of an IP packet timed out, and is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.2. fragact_contains_frags (ID: 02000002)

Default Severity	CRITICAL
Log Message	Internal Error: A failed active fragment contained fragments. Dropping
Explanation	An Internal Error occured when freeing an active fragment. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Dropped Fragments Rule Name

2.20.3. fail_suspect_out_of_resources (ID: 02000003)

Default Severity	CRITICAL
Log Message	Out of reassembly resources for suspect. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Out of fragmentation-reassembly resources when processing the IP packet, which may contain illegal fragments. Dropping packet and freeing resources.
Firewall Action	drop
Recommended Action	None.

Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.4. fail_out_of_resources (ID: 02000004)

Default Severity	CRITICAL
Log Message	Out of reassembly resources. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Out of fragmentation-reassembly resources when processing the IP packet. Dropping packet and freeing resources.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.5. fail_suspect_timeout (ID: 02000005)

Default Severity	CRITICAL
Log Message	Time out reassembling suspect. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Timed out when reassembling a fragmented IP packet, which may contain illegal fragments. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip

	ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.6. fail_timeout (ID: 02000006)

Default Severity	CRITICAL
Log Message	Time out reassembling. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Timed out when reassembling a fragmented IP packet. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.7. disallowed_suspect (ID: 02000007)

Default Severity	WARNING
Log Message	Dropping stored fragments of disallowed suspect packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	The fragments of a disallowed IP packet, which may contain illegal fragments, were dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact

	frags
Context Parameters	Dropped Fragments Rule Name

2.20.8. drop_frags_of_disallowed_packet (ID: 02000008)

Default Severity	WARNING
Log Message	Dropping stored fragments of disallowed packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	The fragments of a disallowed IP packet were dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.9. drop_frags_of_illegal_packet (ID: 02000009)

Default Severity	WARNING
Log Message	Dropping fragments of illegal packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	The fragments of an illegal IP packet were dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.10. drop_extraneous_frags_of_completed_packet (ID: 02000010)

Default Severity	WARNING
Log Message	Dropping extraneous fragments of completed packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	A completed reassembled IP packet contains extraneous fragments, which are dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.20.11. learn_state (ID: 02000011)

Default Severity	ERROR
Log Message	Internal Error: Invalid state <state>
Explanation	Internal Error, the fragmented IP packet has an invalid state.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	state
Context Parameters	Dropped Fragments Rule Name

2.20.12. drop_duplicate_frag_suspect_packet (ID: 02000012)

Default Severity	WARNING
Log Message	Dropping duplicate fragment of suspect packet
Explanation	A duplicate fragment of an IP packet, which may contain illegal

	fragments, was received. Dropping the duplicate fragment.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.13. drop_duplicate_frag (ID: 02000013)

Default Severity	WARNING
Log Message	Dropping duplicate fragment
Explanation	A duplicate fragment of an IP packet was received. Dropping the duplicate fragment.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.14. frag_offset_plus_length_not_in_range (ID: 02000014)

Default Severity	ERROR
Log Message	Fragment offset+length not in range <minipdatalen>-<maxipdatalen>
Explanation	The fragment offset and length would be outside of the allowed IP size range. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	minipdatalen maxipdatalen
Context Parameters	Rule Name Packet Buffer

2.20.15. no_available_fragacts (ID: 02000015)

Default Severity	WARNING

Log Message	Internal Error: No available resources (out of memory?).
Explanation	An Internal Error occured. Failed to create necessary fragmentation reassembly resources. This could be a result of the unit being out of memory.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.16. bad_ipdatalen (ID: 02000016)

Default Severity	ERROR
Log Message	Bad IPDataLen=<ipdatalen>
Explanation	The partly reassembled IP packet has an invalid IP data length. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen
Context Parameters	Rule Name Packet Buffer

2.20.17. bad_ipdatalen (ID: 02000017)

Default Severity	ERROR
Log Message	Fragment offset+length is greater than the configured maximum <maxipdatalen>
Explanation	The fragment offset plus length would result in a greater length than the configured maximum length of an IP packet. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	maxipdatalen
Context Parameters	Rule Name Packet Buffer

2.20.18. overlapping_frag (ID: 02000018)

Default Severity	ERROR
Log Message	Overlapping fragment
Explanation	This fragment would overlap the next fragment offset. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.19. bad_offs (ID: 02000019)

Default Severity	ERROR
Log Message	Bad fragment offset
Explanation	The fragment has an invalid offset. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.20. duplicate_frag_with_different_length (ID: 02000020)

Default Severity	ERROR
Log Message	Duplicate fragment with different length received
Explanation	The fragment is a duplicate of an already received fragment, but the fragment lengths differ. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.21. duplicate_frag_with_different_data (ID: 02000021)

Default Severity	ERROR
Log Message	Duplicate fragment with different data received
Explanation	The fragment is a duplicate of an already received fragment, but the fragment data differs. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.22. partial_overlap (ID: 02000022)

Default Severity	ERROR
Log Message	Fragments partially overlap
Explanation	Two fragments partially overlap. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.23. drop_frag_disallowed_suspect_packet (ID: 02000023)

Default Severity	WARNING
Log Message	Dropping fragment of disallowed suspect packet
Explanation	A fragment of a disallowed IP packet, which may contain illegal fragments, is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.24. drop_frag_disallowed_packet (ID: 02000024)

Default Severity	WARNING
Log Message	Dropping fragment of disallowed packet
Explanation	A fragment of a disallowed IP packet is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.25. already_completed (ID: 02000025)

Default Severity	ERROR
Log Message	Dropping extraneous fragment of completed packet
Explanation	A completed reassembled IP packet contains a extraneous fragment, which is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.26. drop_frag_failed_suspect_packet (ID: 02000026)

Default Severity	WARNING
Log Message	Dropping fragment of failed suspect packet
Explanation	A fragment of a failed IP packet, which may contain illegal fragments, is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.27. drop_frag_failed_packet (ID: 02000027)

Default Severity	WARNING
Log Message	Dropping fragment of failed packet
Explanation	A fragment of a failed IP packet is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.28. drop_frag_illegal_packet (ID: 02000028)

Default Severity	WARNING
Log Message	Dropping fragment of illegal packet
Explanation	A fragment of an illegal IP packet is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.29. fragments_available_freeing (ID: 02000100)

Default Severity	CRITICAL
Log Message	Internal Error: Contains fragments even when freeing. Dropping
Explanation	An Internal Error occured when freeing an active fragment. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Dropped Fragments Rule Name

2.20.30. bad_ipdatalen (ID: 02000116)

Default Severity	ERROR
Log Message	Bad IPDataLen=<ipdatalen>
Explanation	The partly reassembled IP packet has an invalid IP data length. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen
Context Parameters	Rule Name Packet Buffer

2.20.31. single_frag (ID: 02000117)

Default Severity	ERROR
Log Message	Illegal fragment, last fragment with zero offset. Dropping packet.
Explanation	A fragment with More Fragments flag cleared and an Offset of zero is not a legal fragment. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.20.32. bad_offs (ID: 02000119)

Default Severity	ERROR
Log Message	Bad fragment offset
Explanation	The fragment has an invalid offset. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.21. GEOIP

These log messages refer to the **GEOIP (GeoIP Events)** category.

2.21.1. database_load_failed (ID: 08100001)

Default Severity	WARNING
Log Message	Unable to load IPv4 Geolocation database, because of <reason>
Explanation	The unit failed to load the IPv4 Geolocation database.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	protocol reason

2.21.2. database_load_failed (ID: 08100002)

Default Severity	WARNING
Log Message	Unable to load IPv6 Geolocation database, because of <reason>
Explanation	The unit failed to load the IPv6 Geolocation database.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	protocol reason

2.22. GRE

These log messages refer to the **GRE (GRE events)** category.

2.22.1. failed_to_setup_gre_tunnel (ID: 02200001)

Default Severity	WARNING
Log Message	Failed to setup open tunnel from <local_ip> to <remote_ip>
Explanation	Unable to setup GRE tunnel with endpoint.
Firewall Action	drop
Recommended Action	Check CONN usage and local routing.
Revision	1
Parameters	local_ip remote_ip

2.22.2. gre_bad_flags (ID: 02200002)

Default Severity	WARNING
Log Message	GRE packet with bad flag(s). Packet dropped
Explanation	Received GRE packet with a bad flag combination.
Firewall Action	drop
Recommended Action	Check GRE endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.22.3. gre_bad_version (ID: 02200003)

Default Severity	WARNING
Log Message	GRE packet with bad version (not 0). Packet dropped
Explanation	Received GRE packet with bad version.
Firewall Action	drop
Recommended Action	Check GRE endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.22.4. gre_checksum_error (ID: 02200004)

Default Severity	WARNING
Log Message	GRE packet with checksum error. Packet dropped
Explanation	Received GRE packet with checksum errors.
Firewall Action	drop
Recommended Action	Check network equipment for errors.
Revision	1
Context Parameters	Packet Buffer

2.22.5. gre_length_error (ID: 02200005)

Default Severity	WARNING
Log Message	GRE packet length error. Packet dropped
Explanation	Received GRE packet with length error.
Firewall Action	drop
Recommended Action	Check GRE endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.22.6. gre_send_routing_loop_detected (ID: 02200006)

Default Severity	WARNING
Log Message	Routing loop detected. GRE packet send failed
Explanation	Routing loop to the GRE endpoint detected.
Firewall Action	drop
Recommended Action	Check local routing.
Revision	1
Context Parameters	Packet Buffer

2.22.7. unmatched_session_key (ID: 02200007)

Default Severity	WARNING

Log Message	Received GRE packet with unmatched session key. Packet dropped
Explanation	Received GRE packet with unmatched session key.
Firewall Action	drop
Recommended Action	Check GRE session key settings on the remote gateway.
Revision	1
Parameters	session_key
Context Parameters	Packet Buffer

2.22.8. gre_routing_flag_set (ID: 02200008)

Default Severity	WARNING
Log Message	Received GRE packet with routing flag set. Packet dropped
Explanation	Received GRE packet with unsupported routing option enabled.
Firewall Action	drop
Recommended Action	Check GRE configuration on remote gateway.
Revision	1
Context Parameters	Packet Buffer

2.23. HA

These log messages refer to the **HA (High Availability events)** category.

2.23.1. peer_gone (ID: 01200001)

Default Severity	NOTICE
Log Message	Peer firewall disappeared. Going active
Explanation	The peer firewall (which was active) is not available anymore. This firewall will now go active instead.
Firewall Action	activate
Recommended Action	None.
Revision	2

2.23.2. peer_gone (ID: 01200002)

Default Severity	NOTICE
Log Message	Peer firewall disappeared.
Explanation	The peer firewall (which was inactive) is not available anymore. This firewall will continue to stay active.
Firewall Action	None
Recommended Action	None.
Revision	2

2.23.3. conflict_both_peers_active (ID: 01200003)

Default Severity	NOTICE
Log Message	Conflict: Both peers are active! Resolving...
Explanation	A conflict occured as both peers are active at the same time. The conflict will automatically be resolved.
Firewall Action	resolving
Recommended Action	None.
Revision	1

2.23.4. peer_has_higher_local_load (ID: 01200004)

Default Severity	NOTICE
Log Message	Both active, peer has higher local load; staying active
Explanation	Both memebrs are active, but the peer has higher local load. This firewall will stay active.
Firewall Action	stay_active
Recommended Action	None.
Revision	2

2.23.5. peer_has_lower_local_load (ID: 01200005)

Default Severity	NOTICE
Log Message	Both active, peer has lower local load; deactivating
Explanation	Both members are active, but the peer has lower local load. This firewall will de-activate.
Firewall Action	deactivate
Recommended Action	None.
Revision	2

2.23.6. peer_has_more_connections (ID: 01200006)

Default Severity	NOTICE
Log Message	Both active, peer has more connections; deactivating
Explanation	Both members are active, but the peer has more connections. This firewall will de-activate.
Firewall Action	deactivate
Recommended Action	None.
Revision	2

2.23.7. peer_has_fewer_connections (ID: 01200007)

Default Severity	NOTICE
Log Message	Both active, peer has fewer connections; staying active
Explanation	Both members are active, but the peer has fewer connections. This firewall will stay active.
Firewall Action	stay_active

Recommended Action	None.
Revision	2

2.23.8. conflict_both_peers_inactive (ID: 01200008)

Default Severity	NOTICE
Log Message	Conflict: Both peers are inactive! Resolving...
Explanation	A conflict occured as both peers are inactive at the same time. The conflict will automatically be resolved.
Firewall Action	None
Recommended Action	None.
Revision	1

2.23.9. peer_has_more_connections (ID: 01200009)

Default Severity	NOTICE
Log Message	Both inactive, peer has more connections; staying inactive...
Explanation	Both members are inactive, but the peer has more connections. This firewall will stay inactive.
Firewall Action	stay_deactivated
Recommended Action	None.
Revision	2

2.23.10. peer_has_fewer_connections (ID: 01200010)

Default Severity	NOTICE
Log Message	Both inactive, peer has fewer connections; going active...
Explanation	Both members are inactive, but the peer has fewer connections. This firewall will go active.
Firewall Action	activate
Recommended Action	None.
Revision	2

2.23.11. peer_alive (ID: 01200011)

Default Severity	NOTICE
Log Message	Peer firewall is alive
Explanation	The peer firewall is alive.
Firewall Action	None
Recommended Action	None.
Revision	2

2.23.12. heartbeat_from_unknown (ID: 01200043)

Default Severity	WARNING
Log Message	Received HA heartbeat from unknown IP. Dropping
Explanation	The received HA heartbeat packet was originating from an unknown IP. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.23.13. should_have_arrived_on_sync_iface (ID: 01200044)

Default Severity	WARNING
Log Message	This packet should have arrived on the sync iface. Dropping
Explanation	The HA packet did not arrive on the sync interface. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.23.14. activate_failed (ID: 01200050)

Default Severity	WARNING
Log Message	Failed to activate the configuration merged from HA partner

Explanation	The firewall failed to activate the merged configuration that was received from the peer.
Firewall Action	ha_activate_conf
Recommended Action	None.
Revision	2

2.23.15. merge_failed (ID: 01200051)

Default Severity	WARNING
Log Message	Failed to merge configuration from HA partner
Explanation	The firewall failed to merge the configuration that was received from the peer.
Firewall Action	ha_merge_conf
Recommended Action	None.
Revision	2

2.23.16. ha_commit_error (ID: 01200052)

Default Severity	WARNING
Log Message	The merged HA configuration contains errors
Explanation	The merged HA configuration contains errors, and can not be commited.
Firewall Action	ha_commitchanges
Recommended Action	Resolve the errors and commit the changes again.
Revision	1

2.23.17. ha_write_failed (ID: 01200053)

Default Severity	WARNING
Log Message	Could not write HA configuration to disk
Explanation	The HA configuration could not be written to the storate media.
Firewall Action	ha_commitchanges
Recommended Action	Verify that the storage media is not write protected or damaged.
Revision	1

2.23.18. ha_commit_unknown_error (ID: 01200054)

Default Severity	WARNING
Log Message	An unknown error occured while saving the HA configuration
Explanation	An unknown error occured when the HA configuration was to be saved. It has not been commited.
Firewall Action	ha_commitchanges
Recommended Action	None.
Revision	1

2.23.19. linkmon_triggered_failover (ID: 01200055)

Default Severity	NOTICE
Log Message	HA node going inactive. <reason>
Explanation	Linkmon requested the node to go inactive.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.23.20. resync_conns_to_peer (ID: 01200100)

Default Severity	WARNING
Log Message	Initiating complete resynchronization of <numconns> connections to peer firewall
Explanation	All current connections will be re-synchronized to peer, as the peer has been restarted. Initializing re-synchronization process.
Firewall Action	resync_conns_init
Recommended Action	None.
Revision	1
Parameters	reason numconns

2.23.21. hasync_connection_established (ID: 01200200)

Default Severity	NOTICE
Log Message	HASync connection to peer firewall established
Explanation	HA synchronization connection to peer has been establihsed. Supported events will now be synchronized between the members of the HA cluster.
Firewall Action	None
Recommended Action	None.
Revision	2

2.23.22. hasync_connection_disconnected_lifetime_expired (ID: 01200201)

Default Severity	NOTICE
Log Message	HASync connection lifetime expired. Reconnecting...
Explanation	The HA synchronization connection lifetime has expired. A new connection will be establised by reconnecting to the peer.
Firewall Action	reconnect
Recommended Action	None.
Revision	2

2.23.23. hasync_connection_failed_timeout (ID: 01200202)

Default Severity	NOTICE
Log Message	HASync connection to peer firewall failed. Reconnecting...
Explanation	The HA synchronization connection attempt failed. Reconnecting to peer.
Firewall Action	reconnect
Recommended Action	None.
Revision	2

2.23.24. resync_conns_to_peer_complete (ID: 01200300)

Default Severity	NOTICE
Log Message	Connection resynchronization to peer complete
Explanation	The connection resynchronization process to peer is complete. All connections has been synchronized.

Firewall Action	None
Recommended Action	None.
Revision	1

2.23.25. disallowed_on_sync_iface (ID: 01200400)

Default Severity	WARNING
Log Message	Received non-HA traffic on sync iface. Dropping
Explanation	A packet which is not a HA-related packet was received on the sync interface. This should not happend, and the packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.23.26. sync_packet_on_nonsync_iface (ID: 01200410)

Default Severity	WARNING
Log Message	Received state sync packet on non-sync iface. Dropping
Explanation	A HA state sync packet was recieved on a non-sync interface. This should never happend, and the packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.23.27. ttl_too_low (ID: 01200411)

Default Severity	WARNING
Log Message	Received HA heartbeat with too low TTL. Dropping
Explanation	The received HA heartbeat packet had a TTL (Time-To-Live) field which is too low. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.23.28. heartbeat_from_myself (ID: 01200412)

Default Severity	WARNING
Log Message	Received HA heartbeat from the firewall itself. Dropping
Explanation	The received HA heartbeat packet was originating from the firewall itself. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Context Parameters	Rule Name Packet Buffer

2.23.29. config_sync_failure (ID: 01200500)

Default Severity	CRITICAL
Log Message	Tried to synchronize configuration to peer 3 times without success. Giving up.
Explanation	The firewall tried to synchronize the configuration to peer three times, but failed. It will now give up trying to do so.
Firewall Action	give_up_synching
Recommended Action	None.
Revision	2
Parameters	numretries

2.23.30. both_active (ID: 01200616)

Default Severity	NOTICE
Log Message	Both active, deactivation in progress.
Explanation	Both active, deactivation in progress.
Firewall Action	deactivate
Recommended Action	None.
Revision	2

2.23.31. both_inactive (ID: 01200617)

Default Severity	NOTICE
Log Message	Both not active, activation in progress.
Explanation	Both not active, activation in progress.
Firewall Action	activate
Recommended Action	None.
Revision	2

2.23.32. going_online (ID: 01200618)

Default Severity	NOTICE
Log Message	Ha unit going online.
Explanation	Ha unit going online.
Firewall Action	going_online
Recommended Action	None.
Revision	3
Parameters	previous_event=

2.24. HWM

These log messages refer to the **HWM (Hardware monitor events)** category.

2.24.1. temperature_alarm (ID: 04000011)

Default Severity	WARNING
Log Message	Temperature monitor <index> (<name>) is outside the specified limit. Current value is <current_temp> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The unit may be overheating, this may be because the cooling is failing or to hot enviroment.
Firewall Action	none
Recommended Action	Shutdown the unit and determine the problem.
Revision	1
Parameters	index name unit current_temp min_limit max_limit

2.24.2. temperature_normal (ID: 04000012)

Default Severity	WARNING
Log Message	Temperature monitor <index> (<name>) is outside the specified limit. Current value is <current_temp> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The sensor reports that the temperature value is back in the normal range.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	index name unit current_temp min_limit max_limit

2.24.3. voltage_alarm (ID: 04000021)

Default Severity	WARNING
Log Message	Voltage monitor <index> (<name>) is outside the specified limit. Current value is <current_voltage> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The powersupply of this unit may be failing.
Firewall Action	none
Recommended Action	Change powersupply unit.
Revision	1
Parameters	index name unit current_voltage min_limit max_limit

2.24.4. voltage_normal (ID: 04000022)

Default Severity	WARNING
Log Message	Voltage monitor <index> (<name>) is outside the specified limit. Current value is <current_voltage> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The sensor reports that the voltage value is back in the normal range.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	index name unit current_voltage min_limit max_limit

2.24.5. fanrpm_alarm (ID: 04000031)

Default Severity	WARNING
Log Message	Fan RPM monitor <index> (<name>) is outside the specified limit. Current value is <current_fanrpm> <unit>, value is <current_fanrpm> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The fan is behaving strange, this may because it is failing or blocked.

Firewall Action none

Recommended Action Unblock or change the corresponding fan.

Revision 1

Parameters index
name
unit
current_fanrpm
min_limit
max_limit

2.24.6. fanrpm_normal (ID: 04000032)

Default Severity WARNING

Log Message Fan RPM monitor <index> (<name>) is outside the specified limit. Current value is <current_fanrpm> <unit>, lower limit is <min_limit>, upper limit is <max_limit>

Explanation The sensor reports that the fan rpm value is back in the normal range.

Firewall Action None

Recommended Action None.

Revision 1

Parameters index
name
unit
current_fanrpm
min_limit
max_limit

2.24.7. gpio_alarm (ID: 04000041)

Default Severity WARNING

Log Message GPIO monitor <index> (<name>) is outside the specified limit. Current value is <current_gpio> <unit>, value is <current_gpio> <unit>, lower limit is <min_limit>, upper limit is <max_limit>

Explanation This varies depending on hardware model and what the GPIO is connected to.

Firewall Action none

Recommended Action Depends on what the GPIO is connected to.

Revision 1

Parameters index
name

unit
current_gpio
min_limit
max_limit

2.24.8. gpio_normal (ID: 04000042)

Default Severity WARNING

Log Message Temperature monitor <index> (<name>) is outside the specified limit. Current value is <current_gpio> <unit>, lower limit is <min_limit>, upper limit is <max_limit>

Explanation The sensor reports that the GPIO value is back inte the normal range.

Firewall Action None

Recommended Action None.

Revision 1

Parameters index
name
unit
current_gpio
min_limit
max_limit

2.24.9. free_memory_warning_level (ID: 04000101)

Default Severity WARNING

Log Message Free memory has fallen below the specified limit of <limit_percentage> percent, limit classified is <severity>, free <free_mem> MB of total <total_mem> MB, percentage free <free_percentage>

Explanation The amount of free memory is getting low.

Firewall Action None

Recommended Action Review the configuration and disable or lower settings to reduce memory consumption.

Revision 1

Parameters limit_percentage
total_mem
free_mem
free_percentage
severity

2.24.10. free_memory_warning_level (ID: 04000102)

Default Severity WARNING

Log Message Free memory has fallen below the specified limit of <limit_megabyte> megabyte, limit classified is <severity>, free <free_mem> MB of total <total_mem> MB, percentage free <free_percentage>

Explanation The amount of free memory is getting low.

Firewall Action None

Recommended Action Review the configuration and disable or lower settings to reduce memory consumption.

Revision 1

Parameters limit_megabyte
total_mem
free_mem
free_percentage
severity

2.24.11. free_memory_normal_level (ID: 04000103)

Default Severity NOTICE

Log Message The amount of free memory is in the normal range, free <free_mem> MB of total <total_mem> MB, percentage free <free_percentage>

Explanation The memory usage is in the normal range.

Firewall Action None

Recommended Action None.

Revision 1

Parameters total_mem
free_mem
free_percentage

2.25. IDP

These log messages refer to the **IDP (Intrusion Detection & Prevention events)** category.

2.25.1. scan_detected (ID: 01300001)

Default Severity NOTICE

Log Message Scan detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>. Closing connection.

Explanation A scan signature mapped to the "protect" action matched the traffic, closing connection.

Firewall Action close

Recommended Action Research the advisory (searchable by the unique ID), if you suspect an attack.

Revision 2

Parameters
description
signatureid
idrule
ipproto
srcip
srcport
destip
destport
internalid

Context Parameters
Rule Name
Deep Inspection

2.25.2. idp_notice (ID: 01300002)

Default Severity WARNING

Log Message IDP Notice: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>. Closing connection.

Explanation A notice signature mapped to the "protect" action matched the traffic, closing connection.

Firewall Action close

Recommended Action This is probably not an attack, but you may research the advisory (searchable by the unique ID).

Revision 2

Parameters description

	signatureid idrule ipproto srcip srcport destip destport internalid
Context Parameters	Rule Name Deep Inspection

2.25.3. intrusion_detected (ID: 01300003)

Default Severity	WARNING
Log Message	Intrusion detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>. Closing connection.
Explanation	An attack signature mapped to the "protect" action matched the traffic.
Firewall Action	close
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	2
Parameters	description signatureid idrule ipproto srcip srcport destip destport internalid
Context Parameters	Rule Name Deep Inspection

2.25.4. virus_detected (ID: 01300004)

Default Severity	WARNING
Log Message	Virus/worm detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>. Closing connection.
Explanation	A virus signature mapped to the "protect" action matched the traffic.
Firewall Action	close

Recommended Action Research the advisory (searchable by the unique ID).

Revision 2

Parameters
description
signatureid
idrule
ipproto
srcip
srcport
destip
destport
internalid

Context Parameters
Rule Name
Deep Inspection

2.25.5. scan_detected (ID: 01300005)

Default Severity NOTICE

Log Message Scan detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>.

Explanation A scan signature matched the traffic.

Firewall Action None

Recommended Action Research the advisory (searchable by the unique ID).

Revision 2

Parameters
description
signatureid
idrule
ipproto
srcip
srcport
destip
destport
internalid

Context Parameters
Rule Name
Deep Inspection

2.25.6. idp_notice (ID: 01300006)

Default Severity NOTICE

Log Message IDP Notice: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>.

Explanation	A notice signature matched the traffic.
Firewall Action	None
Recommended Action	This is probably not an attack, but you may research the advisory (searchable by the unique ID).
Revision	2
Parameters	description signatureid idrule ipproto srcip srcport destip destport internalid
Context Parameters	Rule Name Deep Inspection

2.25.7. intrusion_detected (ID: 01300007)

Default Severity	NOTICE
Log Message	Intrusion detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>
Explanation	An attack signature matched the traffic.
Firewall Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	2
Parameters	description signatureid idrule ipproto srcip srcport destip destport internalid
Context Parameters	Rule Name Deep Inspection

2.25.8. virus_detected (ID: 01300008)

Default Severity	NOTICE

Log Message	Virus/Worm detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Internal ID: <internalid>.
Explanation	A virus signature matched the traffic.
Firewall Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	2
Parameters	description signatureid idrule ipproto srcip srcport destip destport internalid
Context Parameters	Rule Name Deep Inspection

2.25.9. invalid_url_format (ID: 01300009)

Default Severity	ERROR
Log Message	Failed to parse the HTTP URL. ID Rule: <idrule>. URL: <url>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	The unit failed parsing an URL. The reason for this is problaby because the URL has an invalid format, or it contains invalid UTF8 formatted characters.
Firewall Action	close
Recommended Action	Make sure that the URL is formatted correctly.
Revision	1
Parameters	idrule url srcip srcport destip destport
Context Parameters	Rule Name

2.25.10. invalid_url_format (ID: 01300010)

Default Severity	WARNING

Log Message	Failed to parse the HTTP URL. ID Rule: <idrule>. URL: <url>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Ignoring the URL.
Explanation	The unit failed parsing an URL. The reason for this is problaby because the URL has an invalid format, or it contains invalid UTF8 formatted characters.
Firewall Action	ignore
Recommended Action	Make sure that the URL is formatted correctly.
Revision	1
Parameters	idrule url srcip srcport destip destport
Context Parameters	Rule Name

2.25.11. idp_evasion (ID: 01300011)

Default Severity	ERROR
Log Message	Failed to reassemble data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	The unit failed to reassemble data. The reason for this is problaby due to an IDP engine evasion attack.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.25.12. idp_evasion (ID: 01300012)

Default Severity	ERROR
Log Message	Failed to reassemble data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.

Explanation	The unit failed to reassemble data. The reason for this is problaby due to an IDP engine evasion attack.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.25.13. idp_outofmem (ID: 01300013)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	The unit failed to scan data. The reason for this is due to low amount of memory.
Firewall Action	close
Recommended Action	Review your configuration.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.25.14. idp_outofmem (ID: 01300014)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	The unit failed to scan data. The reason for this is due to low amount of memory.
Firewall Action	ignore
Recommended Action	Review your configuration.

Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.25.15. idp_failscan (ID: 01300015)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Reason: <reason>. Closing connection.
Explanation	The unit failed to scan data.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport reason
Context Parameters	Rule Name

2.25.16. idp_failscan (ID: 01300016)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Reason: <reason>.
Explanation	The unit failed to scan data.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport

	reason
Context Parameters	Rule Name

2.25.17. no_valid_license_or_no_signature_file (ID: 01300017)

Default Severity	CRITICAL
Log Message	IDP: No signatures loaded, skipping IDP filtering
Explanation	IDP scanning is aborted since the signature file has been disabled or no signature file was found.
Firewall Action	idp_scanning_aborted
Recommended Action	For IDP scanning, a valid license with IDP enabled must be installed. If already installed, manually initiate downloading of the latest signature file. IDP scanning can be disabled to avoid this log message.
Revision	1
Context Parameters	ALG Session ID

2.26. IDPPIPES

These log messages refer to the **IDPPIPES (IDP Traffic Shaping events)** category.

2.26.1. conn_idp_piped (ID: 06100001)

Default Severity	WARNING
Log Message	IDP Pipe event triggered. Throughput limited to <limit>
Explanation	An IDP rule with Pipe event triggered on the specified connection. The connection is piped to [limit] kbps.
Firewall Action	limit_throughput
Recommended Action	None.
Revision	1
Parameters	limit
Context Parameters	Connection

2.26.2. host_idp_piped (ID: 06100002)

Default Severity	NOTICE
Log Message	Dynamic pipe state added for host <host>. Throughput limited to <limit> for all new connections for <ttl> seconds
Explanation	An IDP Pipe event triggered. The host [host] will be dynamically piped with a total throughput of [limit] kbps. All new connections to and from this host will be piped for [ttl] seconds.
Firewall Action	host_idp_piped
Recommended Action	None.
Revision	1
Parameters	host limit ttl
Context Parameters	Connection

2.26.3. out_of_memory (ID: 06100003)

Default Severity	ALERT
Log Message	Out of memory
Explanation	An attempt to allocate memory failed.

Firewall Action	host_state_creation_aborted
Recommended Action	Issue the "memory" CLI command and check for modules with abnormal memory consumption. Otherwise, revise configuration in order to free more RAM.
Revision	1

2.26.4. idp_piped_state_replaced (ID: 06100004)

Default Severity	DEBUG
Log Message	Replaced IDP pipe host entry <replaced_host>
Explanation	An old dynamic pipe entry was removed and replaced since the maximum number of pipe states were reached.
Firewall Action	state_replaced
Recommended Action	None.
Revision	1
Parameters	replaced_host old_host_ttl

2.26.5. idp_piped_state_expire (ID: 06100005)

Default Severity	DEBUG
Log Message	Removed IDP dynamic pipe state for host <host> due to TTL expire
Explanation	An old dynamic pipe entry was removed since its TTL expired. Connections to and from this host are no longer piped.
Firewall Action	state_removed
Recommended Action	None.
Revision	1
Parameters	host

2.26.6. conn_idp_unpiped (ID: 06100006)

Default Severity	NOTICE
Log Message	IDP Pipe disabled. Throughput no longer limited to <limit>
Explanation	A configuration change regarding the dynamic pipes' throughput parameters have occured. The dynamic piping for this connection is disabled.
Firewall Action	pipe_removed

Recommended Action	None.
Revision	1
Parameters	limit
Context Parameters	Connection

2.26.7. conn_idp_piped (ID: 06100007)

Default Severity	WARNING
Log Message	IDP dynamic pipe state found. Throughput limited to <limit>
Explanation	A new connection is piped to [limit] kbps since either the source or destination IP is dynamically throttled by IDP dynamic pipe state. New connections to and from the IP will be throttled as long as an IDP Pipe state exist.
Firewall Action	limit_throughput
Recommended Action	None.
Revision	1
Parameters	limit
Context Parameters	Connection

2.27. IDPUPDATE

These log messages refer to the **IDPUPDATE (Intrusion Detection & Prevention Database update)** category.

2.27.1. idp_db_update_failure (ID: 01400001)

Default Severity	ALERT
Log Message	Update of the Intrusion Detection & Prevention database failed, because of <reason>
Explanation	The unit tried to update the Intrusion Detection & Prevention database, but failed. The reason for this is specified in the "reason" parameter.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.27.2. idp_database_downloaded (ID: 01400002)

Default Severity	NOTICE
Log Message	New Intrusion Detection & Prevention database downloaded
Explanation	An updated version of the Intrusion Detection & Prevention database has been downloaded, which will now be used.
Firewall Action	using_new_database
Recommended Action	None.
Revision	2

2.27.3. idp_db_already_up_to_date (ID: 01400003)

Default Severity	NOTICE
Log Message	Intrusion Detection & Prevention database is up-to-date
Explanation	The current Intrusion Detection & Prevention database is up-to-date, and does not need to be updated.
Firewall Action	None
Recommended Action	None.
Revision	1

2.27.4. idp_db_update_denied (ID: 01400004)

Default Severity	NOTICE
Log Message	Intrusion Detection & Prevention database could not be updated, as no valid subscription exist
Explanation	The current license does not allow Intrusion Detection & Prevention database to be updated.
Firewall Action	None
Recommended Action	Check the system's time and/or purchase a subscription.
Revision	1

2.27.5. idp_detects_invalid_system_time (ID: 01400005)

Default Severity	ERROR
Log Message	System clock is not properly set. Invalid date (<date>) in IDP signature file. IDP disabled
Explanation	The system clock is not up to date. The system clock must be set correctly in order to use the IDP features. IDP features remains disabled until clock is correct and a manual IDP update has been performed.
Firewall Action	idp_disabled
Recommended Action	Check and set the system time correct and perform a manual IDP update.
Revision	1
Parameters	date

2.27.6. downloading_new_database (ID: 01400007)

Default Severity	NOTICE
Log Message	Downloading new IDP database
Explanation	A new IDP database is availible. The database is being downloaded.
Firewall Action	downloading_new_database
Recommended Action	None.
Revision	1

2.27.7. unsynced_databases (ID: 01400009)

Default Severity	WARNING
Log Message	Unsynchronized hardware and software databases detected
Explanation	The IDP hardware and software databases are not synchronized. A full update is automatically initiated.
Firewall Action	downloading_new_database
Recommended Action	None.
Revision	1

2.27.8. sigfile_parser_error (ID: 01400018)

Default Severity	WARNING
Log Message	Signature file is corrupted and will be removed.
Explanation	An error occured while parsing signature file. Thus, it needs to be removed and new file will be downloaded from update servers.
Firewall Action	sigfile_delete
Recommended Action	None.
Revision	1

2.28. IFACEMON

These log messages refer to the **IFACEMON (Interface monitor events)** category.

2.28.1. ifacemon_status_bad_rereport (ID: 03900001)

Default Severity	NOTICE
Log Message	IfaceMon reset interface <iface> 10 seconds ago. Link status: <linkspeed> Mbps <duplex> duplex
Explanation	The Interface Monitor reset the interface 10 seconds ago.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	delay iface [linkspeed] [duplex]

2.28.2. ifacemon_status_bad (ID: 03900003)

Default Severity	WARNING
Log Message	IfaceMon reports interface problems on <iface>. Resetting interface. Link status: <linkspeed> Mbps <duplex> duplex
Explanation	The Interface Monitor has discovered problems on an interface, and will reset it.
Firewall Action	nic_reset
Recommended Action	None.
Revision	1
Parameters	iface linkspeed duplex

2.28.3. ifacemon_status_bad (ID: 03900004)

Default Severity	WARNING
Log Message	IfaceMon reports interface problems on <iface> Resetting interface
Explanation	The Interface Monitor has discovered problems on an interface, and will reset it.
Firewall Action	nic_reset

Recommended Action	None.
Revision	1
Parameters	iface [linkspeed] [duplex]

2.28.4. ifacemon_attach_failed (ID: 03900005)

Default Severity	WARNING
Log Message	IfaceMon failed to attach interface <iface>
Explanation	The Interface Monitor failed to attach the interface during interface reset.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface

2.29. IGMP

These log messages refer to the **IGMP (IGMP events)** category.

2.29.1. querier_election_won (ID: 04200001)

Default Severity	NOTICE
Log Message	Taking on the role of Querier at interface <iface>.
Explanation	This router is now the IGMP Querier at the specified interface.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	iface

2.29.2. querier_election_lost (ID: 04200002)

Default Severity	NOTICE
Log Message	Lost Querier election to <dest> at interface <iface>.
Explanation	"I" am no longer the IMGP Querier at the specified interface.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	dest iface

2.29.3. invalid_dest_ip_address (ID: 04200003)

Default Severity	WARNING
Log Message	Rejected IGMP message directed to unicast IP <ip_dest> at interface <recv_if>.
Explanation	Rejected IGMP message directed to a unicast IP. Possible IGMP DoS attack. Note that sending IGMP messages to a unicast IP is legal with IGMPv1 and IGMPv2, but not recommended.
Firewall Action	drop
Recommended Action	Identify the offending application, upgrade if possible.
Revision	1

Parameters	recv_if ip_dest
Context Parameters	Packet Buffer

2.29.4. invalid_destination_ethernet_address (ID: 04200004)

Default Severity	WARNING
Log Message	Rejected IGMP message with inconsistent IP/ethernet addresses (<ipdest>/<edest>) at interface <recv_if>.
Explanation	Rejected IGMP message directed to a unicast ethernet. Known IGMP DoS attack.
Firewall Action	drop
Recommended Action	Identify the offending application or user, isolate or upgrade if possible.
Revision	1
Parameters	recv_if ipdest edest
Context Parameters	Packet Buffer

2.29.5. failed_restarting_igmp_conn (ID: 04200006)

Default Severity	EMERG
Log Message	Could not restart the IGMP listening conn. Reason: Out of memory
Explanation	Could not restart the IGMP listening conn. The IGMP system is no longer functional since it cannot handle IGMP requests.
Firewall Action	None
Recommended Action	Reboot the system.
Revision	1

2.29.6. invalid_size_query_packet (ID: 04200007)

Default Severity	WARNING
Log Message	Broken IGMP Query at interface <recv_if> (payload exceeds packet size).
Explanation	Harmful condition that potentially could give an attacker full access to the system. May indicate faulty hardware, an attack or experimental software.

Firewall Action	drop
Recommended Action	None, but keep an eye open for malfunctional software/hardware somewhere on the network.
Revision	1
Parameters	recv_if
Context Parameters	Packet Buffer

2.29.7. invalid_query_group_address (ID: 04200008)

Default Severity	ERROR
Log Message	IGMP group specific query at interface <recv_if> about group <grp> (<grp_sat> after being SAT'ed) includes unicast ip address.
Explanation	Unicast IP address found inside group specific query. This is most likely a faulty SAT config.
Firewall Action	drop
Recommended Action	Check your IGMP ruleset to see if a muticast group somehow might be translated into a unicast address.
Revision	1
Parameters	recv_if grp grp_sat
Context Parameters	Packet Buffer

2.29.8. igmp_query_dropped (ID: 04200009)

Default Severity	NOTICE
Log Message	Rule <name> dropped IGMP Query about group <grp> and source <src> at interface <if> from router <rip>.
Explanation	Dropped IGMP Query.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	if rip igmpver grp src name

2.29.9. igmp_query_received (ID: 04200010)

Default Severity NOTICE

Log Message Rule <name> <action> IGMP Query about group <grp> and source <src> at interface <if> from router <rip>. Group <grp> is translated into <sgrp> and source <src> into <ssrc>.

Explanation Got IGMP Query.

Firewall Action allow

Recommended Action None.

Revision 1

Parameters
if
rip
igmpver
grp
src
sgrp
ssrc
name
action

2.29.10. bad_src (ID: 04200011)

Default Severity WARNING

Log Message Rule <name> drops multicast sender <src> (SAT'ed into <sats>) in group <grp> (SAT'ed into <satg>) specific IGMP Query at interface <iface>.

Explanation This is most likely a faulty IGMP configuration, but may also indicate faulty software on the network. Under special circumstances this could be an active attempt to scan the network for information.

Firewall Action drop

Recommended Action Specifically check your IGMP ruleset for incorrect SAT information (IGMP support requires at least one "REPORT" (Member Report) rule and one matching "QUERY" rule). Make sure both multicast groups and source addresses map one-to-one between Member Reports and Queries. Finally check the network for for other anomalies that could indicate broken equipment or installed "spyware".

Revision 1

Parameters
name
src
grp
sats
satg
iface

2.29.11. igmp_report_received (ID: 04200012)

Default Severity	NOTICE
Log Message	Rule <name> <action> IGMP Member Report concerning group <grp> and source <src> at interface <if> from host <hip>. Group <grp> is translated into <sgrp> and source <src> into <ssrc>
Explanation	Got IGMP Report.
Firewall Action	allow
Recommended Action	None.
Revision	1
Parameters	if hip igmpver grp src sgrp ssrc name action

2.29.12. packet_includes_aux_data (ID: 04200013)

Default Severity	WARNING
Log Message	IGMP Group record <grp> from interface <recv_if> contains auxilliary data.
Explanation	This software support IGMPv1, IGMPv2 and IGMPv3 and none of them support the feature known as "Auxilliary Data". This is a broken packet.
Firewall Action	drop
Recommended Action	If this is a legal situation and the administrator have no reason to suspect an attack, upgrading this software may solve the problem.
Revision	1
Parameters	recv_if grp
Context Parameters	Packet Buffer

2.29.13. invalid_size_report_packet (ID: 04200014)

Default Severity	ERROR
Log Message	Broken IGMP Member Report at interface <recv_if>. Group record

	<grp> makes payload larger than IGMP packet size.
Explanation	Harmful condition that potentially could give an attacker full access to the system. May indicate faulty hardware, an attack or experimental software.
Firewall Action	drop
Recommended Action	None, but keep an eye open for for broken hardware somewhere in the network.
Revision	1
Parameters	recv_if grp
Context Parameters	Packet Buffer

2.29.14. bad_grp (ID: 04200015)

Default Severity	WARNING
Log Message	Bad IGMP Member Report at interface <iface>: Group record request group <grp> (which is not a multicast group).
Explanation	This is most likely a faulty IGMP config.
Firewall Action	drop
Recommended Action	Specifically check for inconsistent SAT/NAT information in the IGMP config.
Revision	1
Parameters	grp iface

2.29.15. invalid_report_grp_record (ID: 04200016)

Default Severity	WARNING
Log Message	Bad IGMP Member Report received. Group record <grp> of unknown type <type>.
Explanation	This indicates faulty software/hardware somewhere on the network.
Firewall Action	drop
Recommended Action	None, but keep an eye open for for broken hardware somewhere in the network.
Revision	1
Parameters	grp type
Context Parameters	Packet Buffer

2.29.16. igmp_report_dropped (ID: 04200017)

Default Severity	NOTICE
Log Message	Rule <name> drops IGMP Member Report concerning group <grp> and source <src> at interface <if> from host <hip>.
Explanation	Dropped IGMP Report.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	if hip igmpver grp src sat_grp sat_src name

2.29.17. igmp_ruleset_rejects_report (ID: 04200018)

Default Severity	WARNING
Log Message	Rule <name> drops multicast sender <src> for group record <grp> in Member Report at interface <iface>.
Explanation	IGMP Member Report contains an unwanted IP sender.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	name src grp iface

2.29.18. bad_inet (ID: 04200019)

Default Severity	WARNING
Log Message	Rejected IGMP message from incorrect IP <src> at interface <iface>.
Explanation	Rejected IGMP message because it claims to have been sent by "me", but I know I did not send any. Possible IGMP DoS attack, but more likely an IP conflict. .

Firewall Action	drop
Recommended Action	Assign a different IP to the offending application.
Revision	1
Parameters	src iface
Context Parameters	Packet Buffer

2.29.19. max_global_requests_per_second_reached (ID: 04200020)

Default Severity	WARNING
Log Message	Rejected IGMP message. Global requests per second rate reached
Explanation	Too many IGMP requests received per second. Possible IGMP DoS attack.
Firewall Action	drop
Recommended Action	Increase global IGMPMaxReqs per second limit if more requests are wanted.
Revision	1
Parameters	ipsrc iface

2.29.20. max_if_requests_per_second_reached (ID: 04200021)

Default Severity	WARNING
Log Message	Rejected IGMP message. Max requests per second and interface rate reached
Explanation	Too many IGMP requests received per second. Possible IGMP DoS attack.
Firewall Action	drop
Recommended Action	Increase IGMPMaxReqsIf per second limit if more requets are wanted.
Revision	1
Parameters	ipsrc iface

2.29.21. disallowed_igmp_version (ID: 04200022)

Default Severity	NOTICE
Log Message	Disallowed IGMP Version
Explanation	A system is using a too old IGMP version.
Firewall Action	drop
Recommended Action	Upgrade the host/router running the disallowed version, or lower LowestIGMPVer limit.
Revision	1
Parameters	recv_ver required_ver
Context Parameters	Packet Buffer

2.29.22. received_unknown_igmp_type (ID: 04200023)

Default Severity	NOTICE
Log Message	Dropped IGMP message with unknown type.
Explanation	Invalid IGMP message type received.
Firewall Action	drop
Recommended Action	None, but keep an eye open for malfunctional software/hardware on the network.
Revision	1
Parameters	MSGType
Context Parameters	Packet Buffer

2.29.23. older_querier_present (ID: 04200024)

Default Severity	NOTICE
Log Message	Entering IGMPv<igmpver> Older Querier Present compatibility mode on interface <iface> because of a received General Query from <rip>.
Explanation	The router will use IGMPv[igmpver] when it is snooping/proxying IGMP messages upstream.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface rip igmpver

2.29.24. older_querier_gone (ID: 04200025)

Default Severity	NOTICE
Log Message	No IGMPv<igmpver> querier present. Older Querier Present (IGMPv<igmpver>) compatibility mode on interface <iface> has ended. Entering IGMPv<nigmpver> mode.
Explanation	The router has not heard any IGMPv[igmpver] general queries and will switch and use IGMPv[nigmpver] version when snooping/proxying IGMP messages upstream.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface igmpver nigmpver

2.30. IP6IN4

These log messages refer to the **IP6IN4 (6in4 Tunnel Events)** category.

2.30.1. failed_to_setup_6in4_tunnel (ID: 07800001)

Default Severity	WARNING
Log Message	Failed to setup open tunnel from <local_ip> to <remote_ip>
Explanation	Unable to setup 6in4 tunnel with endpoint.
Firewall Action	drop
Recommended Action	Check CONN usage and local routing.
Revision	1
Parameters	local_ip remote_ip

2.30.2. 6in4_resolve_successful (ID: 07800002)

Default Severity	NOTICE
Log Message	6in4 tunnel <iface> resolved <remotegwname> to <remotegw>
Explanation	The 6in4 tunnel succesfully resolved the DNS name of remote endpoint.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.30.3. 6in4_resolve_failed (ID: 07800003)

Default Severity	WARNING
Log Message	6in4 tunnel <iface> failed to resolve <remotegwname>
Explanation	The 6in4 tunnel failed to resolve the DNS name of the remote endpoint.
Firewall Action	None
Recommended Action	Make sure you have configured the DNS name of the remote endpoint and the DNS servers correctly.

Revision	1
Parameters	iface remotegwname

2.30.4. 6in4_invalid_sender_encap (ID: 07800004)

Default Severity	WARNING
Log Message	Invalid IPv6 sender entering 6in4 tunnel <senderip>. Packet dropped
Explanation	Packet should be dropped according to RFC 4213 since the source IP address is invalid.
Firewall Action	drop
Recommended Action	Check routing configuration or modify the IPv6 addresses of the clients.
Revision	1
Parameters	senderip
Context Parameters	Packet Buffer

2.30.5. 6in4_length_error (ID: 07800005)

Default Severity	WARNING
Log Message	6in4 packet length error. Packet dropped
Explanation	Received 6in4 packet with length error.
Firewall Action	drop
Recommended Action	Check 6in4 endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.30.6. 6in4_send_routing_loop_detected (ID: 07800006)

Default Severity	WARNING
Log Message	Routing loop detected. 6in4 packet send failed
Explanation	Routing loop to the 6in4 tunnel endpoint detected.
Firewall Action	drop
Recommended Action	Check local routing.

Revision	1
Context Parameters	Packet Buffer

2.30.7. 6in4_invalid_sender_decap (ID: 07800007)

Default Severity	WARNING
Log Message	Invalid IPv6 sender in 6in4 tunnel <senderip>. Packet dropped
Explanation	Packet should be dropped according to RFC 4213 since the source IP address is invalid.
Firewall Action	drop
Recommended Action	Check 6in4 endpoint configuration.
Revision	1
Parameters	senderip
Context Parameters	Packet Buffer

2.31. IPPOOL

These log messages refer to the **IPPOOL (IPPool events)** category.

2.31.1. no_offer_received (ID: 01900001)

Default Severity	ERROR
Log Message	No offers were received
Explanation	No DHCP offers where received by the IP pool general query.
Firewall Action	None
Recommended Action	Review DHCP server parameters and IP pool configuration.
Revision	1
Parameters	waited
Context Parameters	Rule Name

2.31.2. no_valid_dhcp_offer_received (ID: 01900002)

Default Severity	ERROR
Log Message	No valid DHCP offers were received
Explanation	No valid DHCP offers were received.
Firewall Action	no_new_client_created
Recommended Action	Review DHCP server parameters and IP pool filters.
Revision	1
Context Parameters	Rule Name

2.31.3. too_many_dhcp_offers_received (ID: 01900003)

Default Severity	WARNING
Log Message	Too many DHCP offers received. This and subsequent offers will be ignored
Explanation	Too many DHCP offers received.
Firewall Action	ignoring_offer
Recommended Action	Limit the number of DHCP servers on the locally attached network.
Revision	1
Context Parameters	Rule Name

2.31.4. lease_disallowed_by_lease_filter (ID: 01900004)

Default Severity	WARNING
Log Message	The lease was rejected due to a lease filter
Explanation	A lease was rejected by a lease filter.
Firewall Action	lease_rejected
Recommended Action	Verify the lease filters.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.31.5. lease_disallowed_by_server_filter (ID: 01900005)

Default Severity	WARNING
Log Message	The lease was rejected due to a server filter
Explanation	A lease was rejected by a server filter.
Firewall Action	lease_rejected
Recommended Action	Verify the server filters.
Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.31.6. lease_have_bad_dhcp_server (ID: 01900006)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad DHCP-server address
Explanation	A lease was rejected due to a bad DHCP server address.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.31.7. lease_have_bad_netmask (ID: 01900007)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered netmask address
Explanation	A lease was rejected due to a bad offered netmask address.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	netmask
Context Parameters	Rule Name

2.31.8. lease_have_bad_offered_broadcast (ID: 01900008)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered broadcast address
Explanation	A lease was rejected due to a bad offered broadcast address.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	broadcast
Context Parameters	Rule Name

2.31.9. lease_have_bad_offered_ip (ID: 01900009)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered IP address
Explanation	A lease was rejected due to a bad offered IP address.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.31.10. lease_have_bad_gateway_ip (ID: 01900010)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered gateway address
Explanation	A lease was rejected due to a bad offered gateway address.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name

2.31.11. lease_ip_is_already_occupied (ID: 01900011)

Default Severity	WARNING
Log Message	The lease was rejected since it seem to be occupied
Explanation	A lease was rejected since it seem to be occupied.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration and statically configured hosts.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.31.12. lease_rejected_by_server (ID: 01900012)

Default Severity	WARNING
Log Message	The lease was rejected by server
Explanation	A lease was rejected by the DHCP server.
Firewall Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.31.13. ip_offer_already_exist_in_the_pool (ID: 01900013)

Default Severity	WARNING
Log Message	The lease was rejected since the offered IP already exist in the pool
Explanation	A lease was rejected since the offered IP already exists in the pool.
Firewall Action	lease_rejected
Recommended Action	Check IP pool configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.31.14. pool_reached_max_dhcp_clients (ID: 01900014)

Default Severity	ERROR
Log Message	The maximum number of clients for this IP pool have been reached
Explanation	The maximum number of clients for this pool have been reached.
Firewall Action	no_new_client_created
Recommended Action	Verify max clients limitation for the pool.
Revision	1
Context Parameters	Rule Name

2.31.15. macrange_depleted (ID: 01900015)

Default Severity	ERROR
Log Message	The range of MAC addresses for the DHCPClients have been depleted
Explanation	The configured range of MAC addresses for the DHCP clients have been depleted.
Firewall Action	no_new_client_created
Recommended Action	Expand the MAC address range.
Revision	1
Context Parameters	Rule Name

2.31.16. ip_fetched_pool (ID: 01900016)

Default Severity	NOTICE
Log Message	Subsystem fetched a IP from the pool
Explanation	A subsystem fetched an IP from the pool.
Firewall Action	inform
Recommended Action	None.
Revision	1
Parameters	client_ip subsystem
Context Parameters	Rule Name

2.31.17. ip_returned_to_pool (ID: 01900017)

Default Severity	NOTICE
Log Message	Subsystem returned an IP to the pool
Explanation	A subsystem returned an IP to the pool.
Firewall Action	inform
Recommended Action	None.
Revision	1
Parameters	client_ip subsystem
Context Parameters	Rule Name

2.32. IPREPUTATION

These log messages refer to the **IPREPUTATION (IP REPUTATION)** category.

2.32.1. ipreputation_started (ID: 08200001)

Default Severity	INFORMATIONAL
Log Message	IP Reputation started.
Explanation	The IP Reputation system has been started.
Firewall Action	none
Recommended Action	None.
Revision	1

2.32.2. ipreputation_db_update (ID: 08200002)

Default Severity	INFORMATIONAL
Log Message	IP Reputation database full update.<update>
Explanation	The IP Reputation database has been fully updated.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	update

2.32.3. ipreputation_db_partial (ID: 08200003)

Default Severity	INFORMATIONAL
Log Message	IP Reputation database partial update. <update>
Explanation	The system has performed a partial update of the IP Reputation database.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	update

2.32.4. ipreputation_resumed_update (ID: 08200004)

Default Severity	INFORMATIONAL
Log Message	IP Reputation resumed update. <update>
Explanation	IP Reputation has resumed a previously aborted update.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	update

2.32.5. ipreputation_server_connect (ID: 08200005)

Default Severity	INFORMATIONAL
Log Message	Connected to IP Reputation server <server>.
Explanation	The system is connected to a IP Reputation server.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	server

2.32.6. ipreputation_no_db (ID: 08200006)

Default Severity	WARNING
Log Message	IP Reputation database file missing.
Explanation	The IP Reputation database file could not be found on the media on system start. The system will start a full database download.
Firewall Action	none
Recommended Action	Examine why the IP Reputation database file was missing.
Revision	1

2.32.7. ipreputation_db_failopen (ID: 08200007)

Default Severity	ERROR
Log Message	IP Reputation database file could not be loaded.
Explanation	The IP Reputation database file could not be loaded into the system. The system will start a full database download.

Firewall Action	db_disabled
Recommended Action	Examine why the IP Reputation database file could not be read.
Revision	1
Parameters	reason error

2.32.8. ipreputation_update_failed (ID: 08200008)

Default Severity	ERROR
Log Message	IP Reputation update failed. <file>
Explanation	The IP Reputation system failed to perform a full Database update.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	reason file error

2.32.9. ipreputation_server_noconnect (ID: 08200009)

Default Severity	ERROR
Log Message	No connection to IP Reputation server.
Explanation	The system does not have a connection to a IP Reputation server. IP Reputation database updates will be disabled.
Firewall Action	updates_disabled
Recommended Action	None.
Revision	1

2.32.10. ipreputation_novalid_license (ID: 08200010)

Default Severity	WARNING
Log Message	No valid IP Reputation license.
Explanation	The system does not have a valid IP Reputation license. IP Reputation will be disabled.
Firewall Action	ipreputation_disabled
Recommended Action	None.

Revision	1

2.32.11. ipreputation_trial_license (ID: 08200011)

Default Severity	NOTICE
Log Message	Running Trial IP Reputation license.
Explanation	The system is running a Trial IP Reputation license. Trial expires [expire_date].
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	expire_date

2.32.12. ipreputation_database_loaded (ID: 08200012)

Default Severity	NOTICE
Log Message	IP Reputation Database loaded.
Explanation	IP Reputation Database loaded.
Firewall Action	none
Recommended Action	None.
Revision	1

2.32.13. ipreputation_partupdate_failed (ID: 08200013)

Default Severity	ERROR
Log Message	IP Reputation partial update failed. <source>
Explanation	The IP Reputation system failed to perform a partial Database update.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	reason source error

2.32.14. ipreputation_query_timeout (ID: 08200014)

Default Severity	WARNING
Log Message	IP Reputation Cloud query timeout.
Explanation	IP Reputation Cloud Query timed out. A new connection attempt is in progress.
Firewall Action	reconnecting
Recommended Action	None.
Revision	1

2.32.15. ipreputation_server_disconnect (ID: 08200015)

Default Severity	INFORMATIONAL
Log Message	Disconnected from IP Reputation server <server>.
Explanation	The system is disconnected from the IP Reputation server.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	server

2.32.16. ipreputation_server_reply_error (ID: 08200016)

Default Severity	WARNING
Log Message	Failed to parse IP Reputation server response.
Explanation	Response from IP Reputation Cloud Query server could not be parsed. A new connection will be established.
Firewall Action	restarting
Recommended Action	None.
Revision	1

2.32.17. ipreputation_server_unreachable (ID: 08200017)

Default Severity	WARNING
Log Message	Failed to connect to IP Reputation Query server <failedserver>.
Explanation	IP Reputation was unable to connect to a IP Reputation Query server. The system will try to contact one of the backup servers.

Firewall Action	switching_server
Recommended Action	None.
Revision	1
Parameters	failedserver

2.32.18. ipreputation_server_fallback (ID: 08200018)

Default Severity	INFORMATIONAL
Log Message	Falling back from secondary IP Reputation Cloud Query servers to primary server.
Explanation	IP Reputation Cloud Query falls back to primary server after 60 minutes or when a better server has been detected.
Firewall Action	none
Recommended Action	None.
Revision	1

2.32.19. ipreputation_update_error (ID: 08200019)

Default Severity	ERROR
Log Message	IP Reputation update status retrieve error. <server>
Explanation	The IP Reputation system failed to retrieve update status from IP Reputation server.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	reason server error

2.32.20. ipreputation_servers_unreachable (ID: 08200020)

Default Severity	WARNING
Log Message	Failed to connect to IP Reputation Query servers.
Explanation	IP Reputation was unable to connecto to any of the IP Reputation Query servers.
Firewall Action	none

Recommended Action	Verify that the unit has been configured with Internet access.
Revision	1

2.32.21. ipreputation_stopped (ID: 08200021)

Default Severity	INFORMATIONAL
Log Message	IP Reputation stopped.
Explanation	The IP Reputation system has been stopped.
Firewall Action	none
Recommended Action	None.
Revision	1

2.32.22. ipreputation_full_download_failed (ID: 08200022)

Default Severity	ERROR
Log Message	IP Reputation full update failed to download. <file>
Explanation	The IP Reputation system failed to download a full Database update.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	file error

2.32.23. ipreputation_partial_download_failed (ID: 08200023)

Default Severity	ERROR
Log Message	IP Reputation partial update failed to download. <file>
Explanation	The IP Reputation system failed to download a partial Database update.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	file error

2.33. IPSEC

These log messages refer to the **IPSEC (IPsec (VPN) events)** category.

2.33.1. fatal_ipsec_event (ID: 01800100)

Default Severity	ALERT
Log Message	Fatal event occured, because of <reason>
Explanation	Fatal event occured in IPsec stack.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.33.2. warning_ipsec_event (ID: 01800101)

Default Severity	WARNING
Log Message	Warning event occured, because of <reason>
Explanation	Warning event from IPsec stack.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.33.3. audit_event (ID: 01800103)

Default Severity	NOTICE
Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	An audit event occured in the IPsec stack.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	srcip destip spi

seq
protocol
reason

2.33.4. audit_flood (ID: 01800104)

Default Severity	NOTICE
Log Message	<reason>.
Explanation	The rate limit for audit messages was reached.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.33.5. ike_delete_notification (ID: 01800105)

Default Severity	NOTICE
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.33.6. ike_invalid_payload (ID: 01800106)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters	local_ip remote_ip cookies reason

2.33.7. ike_invalid_proposal (ID: 01800107)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	The proposal for the security association could not be accepted.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.33.8. ike_retry_limit_reached (ID: 01800108)

Default Severity	NOTICE
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	The retry limit for transmitting ISAKMP messages was reached.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.33.9. ike_quickmode_failed (ID: 01800109)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.

Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.33.10. packet_corrupt (ID: 01800110)

Default Severity	NOTICE
Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Received a corrupt packet.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	srcip destip spi seq protocol reason

2.33.11. icv_failure (ID: 01800111)

Default Severity	NOTICE
Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The computed and ICV of the received packet did not match.
Firewall Action	drop
Recommended Action	None.
Revision	3
Parameters	srcip destip spi seq protocol reason packet_data

2.33.12. sequence_number_failure (ID: 01800112)

Default Severity	NOTICE
Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet did not fall within the sliding window.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	srcip destip spi seq protocol reason

2.33.13. sa_lookup_failure (ID: 01800113)

Default Severity	NOTICE
Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet could not be mapped to an appropriate SA.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	srcip destip spi seq protocol reason

2.33.14. ip_fragment (ID: 01800114)

Default Severity	NOTICE
Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The packet offered to AH/ESP processing appears to be an IP fragment.

Firewall Action None

Recommended Action None.

Revision 3

Parameters srcip
destip
spi
seq
protocol
reason
packet_data

2.33.15. sequence_number_overflow (ID: 01800115)

Default Severity NOTICE

Log Message Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.

Explanation An attempt to transmit a packet that would result in sequence number overflow.

Firewall Action None

Recommended Action None.

Revision 2

Parameters srcip
destip
spi
seq
protocol
reason

2.33.16. bad_padding (ID: 01800116)

Default Severity NOTICE

Log Message Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.

Explanation The received packet has incorrect padding.

Firewall Action drop

Recommended Action None.

Revision 3

Parameters srcip
destip
spi
seq

protocol
reason
packet_data

2.33.17. hardware_accelerator_congested (ID: 01800117)

Default Severity NOTICE

Log Message Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.

Explanation Hardware accleration failed due to resource shortage.

Firewall Action drop

Recommended Action None.

Revision 2

Parameters srcip
destip
spi
seq
protocol
reason

2.33.18. hardware_acceleration_failure (ID: 01800118)

Default Severity NOTICE

Log Message Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.

Explanation Hardware acceleration failed due to resource shortage, a corrupt packet or other hardware related error.

Firewall Action drop

Recommended Action None.

Revision 3

Parameters srcip
destip
spi
seq
protocol
reason
packet_data

2.33.19. ip_validation_failure (ID: 01800119)

Default Severity NOTICE

Log Message	Source IP: <srcip>, Destination IP: <destip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, ID: <id>, Reason: <reason>.
Explanation	The source or destination address/port did not match the traffic selectors for the SA.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	srcip destip spi seq protocol id reason

2.33.20. commit_failed (ID: 01800200)

Default Severity	CRITICAL
Log Message	Failed to commit IPsec configuration
Explanation	Failed to commit IPsec configuration.
Firewall Action	IPsec_configuration_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.21. commit_succeeded (ID: 01800201)

Default Severity	INFORMATIONAL
Log Message	Commit succeeded - recalculating flows and reapplying routes
Explanation	Succeeded to commit IPsec configuration. Flows will be recalculated and reapplied.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.22. x509_init_failed (ID: 01800203)

Default Severity	CRITICAL
Log Message	Failed to initilaze x509 library

Explanation	Failed to initilaze x509 library.
Firewall Action	IPsec_configuration_disabled
Recommended Action	None.
Revision	1

2.33.23. pm_create_failed (ID: 01800204)

Default Severity	ERROR
Log Message	Failed to create policymanager
Explanation	Failed to create policymanager. Out of memory.
Firewall Action	reduce_number_of_tunnels
Recommended Action	None.
Revision	1

2.33.24. failed_to_start_ipsec (ID: 01800205)

Default Severity	CRITICAL
Log Message	Failed to start IPsec
Explanation	Failed to start IPsec. Policy Manager create did not complete.
Firewall Action	ipsec_disabled
Recommended Action	Restart.
Revision	1

2.33.25. failed_to_start_ipsec (ID: 01800206)

Default Severity	ERROR
Log Message	Disable all IPsec tunnels
Explanation	Disable all IPsec tunnels due to memory limitations.
Firewall Action	disable_all_ipsec_interfaces
Recommended Action	None.
Revision	1

2.33.26. failed_create_audit_module (ID: 01800207)

Default Severity	ERROR
Log Message	Failed to create audit module.
Explanation	Failed to create audit module.
Firewall Action	IPsec_audit_disabled
Recommended Action	None.
Revision	1

2.33.27. failed_attach_audit_module (ID: 01800208)

Default Severity	ERROR
Log Message	Failed to attach audit module.
Explanation	Failed to attach audit module.
Firewall Action	IPsec_audit_disabled
Recommended Action	None.
Revision	1

2.33.28. failed_to_configure_IPsec (ID: 01800209)

Default Severity	CRITICAL
Log Message	Failed during configuration with error: <error_msg> for tunnel: <tunnel>
Explanation	Failed to set IPsec configuration.
Firewall Action	IPsec_configuration_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1
Parameters	error_msg tunnel

2.33.29. failed_to_configure_IPsec (ID: 01800210)

Default Severity	CRITICAL
Log Message	Failed during configuration with error: <error_msg>
Explanation	Failed to set IPsec configuration.
Firewall Action	IPsec_configuration_disabled

Recommended Action	Reconfigure_IPsec.
Revision	1
Parameters	error_msg

2.33.30. reconfig_IPsec (ID: 01800211)

Default Severity	INFORMATIONAL
Log Message	Reconfiguration of IPsec started
Explanation	Reconfiguration of IPsec started.
Firewall Action	ipsec_reconfigured
Recommended Action	None.
Revision	2

2.33.31. failed_to_reconfig_ipsec (ID: 01800212)

Default Severity	ERROR
Log Message	Failed to reconfigure IPsec
Explanation	Failed to reconfigure IPsec. No policymanager object.
Firewall Action	new_ipsec_configuration_disabled
Recommended Action	None.
Revision	2

2.33.32. IPsec_init_failed (ID: 01800213)

Default Severity	CRITICAL
Log Message	Failed to initialize IPsec
Explanation	Failed to start IPsec.
Firewall Action	IPsec_configuration_disabled
Recommended Action	Restart.
Revision	1

2.33.33. ipsec_started_successfully (ID: 01800214)

Default Severity	INFORMATIONAL

Log Message	IPsec started successfully
Explanation	Succeeded to create Policymanger and commit IPsec configuration.
Firewall Action	ipsec_started
Recommended Action	None.
Revision	2

2.33.34. Failed_to_set_local_ID (ID: 01800301)

Default Severity	ERROR
Log Message	Failed to configure Local ID <local_id> for tunnel <tunnel>
Explanation	Failed to configure tunnel with specified local id.
Firewall Action	LocalID_disabled
Recommended Action	None.
Revision	1
Parameters	local_id tunnel

2.33.35. Failed_to_add_certificate (ID: 01800302)

Default Severity	ERROR
Log Message	Failed add host certificate: <certificate>, for tunnel <tunnel>
Explanation	Failed to add specified host certificate.
Firewall Action	certificate_disabled
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	certificate tunnel

2.33.36. Default_IKE_DH_groups_will_be_used (ID: 01800303)

Default Severity	INFORMATIONAL
Log Message	Default configuration for IKE DH groups (2 and 5) will be used for tunnel: <tunnel>
Explanation	Inform that default DH groups settings will be used.
Firewall Action	Use_default_IKE_DH_groups

Recommended Action	None.
Revision	1
Parameters	tunnel

2.33.37. failed_to_set_algorithm_properties (ID: 01800304)

Default Severity	ERROR
Log Message	Failed to set properties IPsec alogorithm <alg>, for tunnel <tunnel>
Explanation	Failed to set specified properties (keysize, lifetimes) for IPsec algorithm.
Firewall Action	use_default_values_for_algorithm
Recommended Action	None.
Revision	2
Parameters	alg tunnel

2.33.38. failed_to_add_root_certificate (ID: 01800306)

Default Severity	ERROR
Log Message	Failed add root certificate: <certificate>, for tunnel <tunnel>
Explanation	Failed to set specified certificate as root certificate.
Firewall Action	disable_certificate
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	certificate tunnel

2.33.39. dns_resolve_failed (ID: 01800308)

Default Severity	WARNING
Log Message	Failed to resolve remote endpoint through DNS
Explanation	None.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters	endpoint ipsectunnel

2.33.40. dns_resolve_timeout (ID: 01800309)

Default Severity	WARNING
Log Message	DNS resolve timed out
Explanation	None.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	endpoint ipsectunnel

2.33.41. dns_no_record (ID: 01800311)

Default Severity	WARNING
Log Message	DNS query returned no records for remote endpoint <endpoint>.
Explanation	Configured remote endpoint DNS does not have any IP addresses.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	endpoint ipsectunnel

2.33.42. remote_endpoint_ip_added (ID: 01800313)

Default Severity	INFORMATIONAL
Log Message	Resolved remote-endpoint <endpoint> to IP <ip> for IPsec tunnel <ipsectunnel>.
Explanation	A new remote endpoint IP was added to IPsec tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	endpoint ipsectunnel

ip
TTL
TTR

2.33.43. failed_to_add_rules (ID: 01800314)

Default Severity	ERROR
Log Message	Failed to commit rules after remote endpoint <endpoint> have been resolved by DNS for IPsec tunnel: <ipsectunnel>
Explanation	Failed to add rules to tunnel after remote endpoint have been resolved by DNS.
Firewall Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	2
Parameters	endpoint ipsectunnel

2.33.44. no_policymanager (ID: 01800316)

Default Severity	CRITICAL
Log Message	No policymanager!! to free tunnel object from
Explanation	No policymanager to free tunnel from!!! IPsec does not work properly.
Firewall Action	ipsec_out_of_work
Recommended Action	Restart.
Revision	1

2.33.45. peer_is_dead (ID: 01800317)

Default Severity	INFORMATIONAL
Log Message	Peer <peer> has been detected dead
Explanation	A remote peer have been detected as dead. This will cause all tunnels associated with the peer to be taken down.
Firewall Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	peer

2.33.46. failed_to_set_dpd_cb (ID: 01800318)

Default Severity	ERROR
Log Message	Failed to set callback for Dead Peer Detection
Explanation	Failed to set callback for Dead Peer Detection User will not receive log message when a peer has been detected dead and the tunnel have been killed.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.47. failed_to_add_certificate (ID: 01800319)

Default Severity	ERROR
Log Message	Failed with error: <status_msg>, message <answermsg>, when adding certificate: <certificate>
Explanation	Failed to add endpoint certificate to external key provider.
Firewall Action	certificate_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	status_msg answermsg certificate

2.33.48. failed_to_remove_key_provider (ID: 01800320)

Default Severity	CRITICAL
Log Message	Try to read out external keyporvider object when no policymanager object avaliable!!
Explanation	Try to read out external keyporvider object when no policymanager object avaliable!.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.49. failed_to_add_key_provider (ID: 01800321)

Default Severity	CRITICAL
Log Message	Failed with error: <status_msg>, when adding external key provider for certificate handling
Explanation	Failed to add external key provider. All certificate authentication will be disabled.
Firewall Action	IPsec_disabled
Recommended Action	Restart.
Revision	1
Parameters	status_msg

2.33.50. failed_to_add_certificate (ID: 01800322)

Default Severity	ERROR
Log Message	Failed add certificate: <certificate>, for tunnel <tunnel>
Explanation	Failed to add certificate. Tunnel configured with this certificate for authentication will fail while negotiate.
Firewall Action	certificate_disabled
Recommended Action	None.
Revision	1
Parameters	certificate tunnel

2.33.51. remote_endpoint_ip_removed (ID: 01800327)

Default Severity	INFORMATIONAL
Log Message	Remote endpoint <endpoint> IP <ip> was removed from IPsec tunnel <ipsectunnel>.
Explanation	Remote endpoint IP was removed from DNS cache.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	endpoint ipsectunnel ip

2.33.52. Failed_to_set_Remote_ID (ID: 01800332)

Default Severity	ERROR
Log Message	Failed to configure Remote ID <remote_id> for tunnel <tunnel>
Explanation	Failed to configure tunnel with specified remote id.
Firewall Action	RemoteID_disabled
Recommended Action	None.
Revision	1
Parameters	remote_id tunnel

2.33.53. failed_to_set_certificate_trust (ID: 01800342)

Default Severity	ERROR
Log Message	Failed set trust for host certificate <certificate> for tunnel <tunnel>
Explanation	Failed to set trust for the specified host certificate.
Firewall Action	certificate_disabled
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	certificate tunnel

2.33.54. failed_to_set_crl_distribution_points (ID: 01800343)

Default Severity	ERROR
Log Message	Failed set CRL distribution points for certificate: <certificate>
Explanation	Failed to set CRL distribution points for the specified certificate.
Firewall Action	certificate_disabled
Recommended Action	None.
Revision	1
Parameters	certificate

2.33.55. dns_cache_removed (ID: 01800344)

Default Severity	WARNING
Log Message	Remote endpoint <endpoint> was removed from DNS cache.

Explanation	All IP address are removed from the DNS cache subsystem for this endpoint.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	endpoint ipsectunnel

2.33.56. ippool_does_not_exist (ID: 01800400)

Default Severity	WARNING
Log Message	IP pool does not exist: <ippool>
Explanation	The config mode pool refers to an IP pool that does not exist. As a result, IPsec clients using config mode will not be able lease IP addresses.
Firewall Action	None
Recommended Action	Update your config mode configuration.
Revision	1
Parameters	ippool

2.33.57. cfgmode_ip_allocated (ID: 01800401)

Default Severity	NOTICE
Log Message	Allocated IP <ip> for use in IKE config mode
Explanation	A dynamically allocated ip was allocated for use with IKE config.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	ip num_dhcp num_dns num_wins num_subnets

2.33.58. cfgmode_ip_freed_by_ippool (ID: 01800402)

Default Severity	NOTICE

Log Message	Returned a dynamic cfg mode IP <ip> to the IP pool
Explanation	A dynamically allocated ip used for IKE cfg mode was returned to the IP pool.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ip

2.33.59. cfgmode_ip_freed_by_ike (ID: 01800403)

Default Severity	NOTICE
Log Message	Freed IP <ip> from use in IKE config mode
Explanation	A dynamically allocated IP was freed from use with IKE config.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	ip

2.33.60. cfgmode_no_context (ID: 01800404)

Default Severity	ALERT
Log Message	No IP pool context could be allocated; out of memory.
Explanation	An attempt to allocate an IP pool context failed because the system ran out of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ippool

2.33.61. cfgmode_no_ip_fetched (ID: 01800405)

Default Severity	WARNING
Log Message	No IP address fetched from IP pool (<ippool>)
Explanation	No IP address could be fetched from the IP pool.

Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ippool

2.33.62. cfgmode_no_ip_data_acquired (ID: 01800406)

Default Severity	WARNING
Log Message	No IP address data acquired from IP pool (<ippool>)
Explanation	No IP address data could be acquired from the IP pool.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ippool

2.33.63. cfgmode_failed_to_add_ip (ID: 01800407)

Default Severity	WARNING
Log Message	Failed to add IP to address table
Explanation	The IP address could not be added to the internal address table (probably because the system ran out out of memory).
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ippool

2.33.64. recieved_packet_to_disabled_IPsec (ID: 01800500)

Default Severity	NOTICE
Log Message	received plaintext packet disabled IPsec. Packet will be dropped
Explanation	Received plain text packet to IPsec while disabled.
Firewall Action	packet_will_be_dropped
Recommended Action	None.
Revision	2

2.33.65. recieved_packet_to_disabled_IPsec (ID: 01800501)

Default Severity	NOTICE
Log Message	Received plain text packet to IPsec while shutting down. Packet will be dropped
Explanation	Received plain text packet to IPsec while shutting down.
Firewall Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.33.66. Recieved_plaintext_packet_for_disabled_IPsec_interface (ID: 01800502)

Default Severity	WARNING
Log Message	IPsec tunnel <ipsec_connection> is disabled. Packet will be dropped
Explanation	A packed was dropped due to the IPsec interface being disabled.
Firewall Action	packet_will_be_dropped
Recommended Action	This is usualy a consequence of low memory or a bad configuration. Look for previous log messages to find the cause for the interface being disabled.
Revision	1
Parameters	ipsec_connection

2.33.67. no_remote_gateway (ID: 01800503)

Default Severity	ERROR
Log Message	Remote gateway is null. No route is possible
Explanation	No remote gateway for packet, i.e no route defined.
Firewall Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.33.68. no_route (ID: 01800504)

Default Severity	ERROR

Log Message	Failed to lookup route. No route for packet.
Explanation	No remote gateway for packet, i.e no route defined.
Firewall Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.33.69. ipsec_interface_disabled (ID: 01800506)

Default Severity	ERROR
Log Message	IPsec interface disabled
Explanation	IPsec interface disabled.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.70. no_route (ID: 01800507)

Default Severity	WARNING
Log Message	Failed to lookup route. No route for packet to remote gateway: <remote_ip>
Explanation	No remote gateway for packet, i.e no route defined.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ipsec_if table remote_ip

2.33.71. no_userauth_specified_for_eap (ID: 01800600)

Default Severity	ERROR
Log Message	No EAP userauth rule found for eap authentication with remote ike peer: <srcif> <remote_peer>
Explanation	No user authentication rule avaliable for eap authentication.
Firewall Action	eap_protocols_disabled

Recommended Action	Reconfigure_tunnel.
Revision	2
Parameters	remote_peer srcif

2.33.72. no_radius_server_configured_for_eap (ID: 01800601)

Default Severity	ERROR
Log Message	No RADIUS server configured for EAP!
Explanation	No RADIUS server configured for EAP!.
Firewall Action	eap_authentication_will_fail
Recommended Action	Reconfigure.
Revision	1

2.33.73. insufficient_resources_for_eap (ID: 01800602)

Default Severity	ERROR
Log Message	Insufficient resources for EAP protocol
Explanation	Insufficient resources for EAP protocol.
Firewall Action	eap_authentication_will_fail
Recommended Action	None.
Revision	1

2.33.74. unknown_type_of_eap (ID: 01800603)

Default Severity	ERROR
Log Message	Unknown type of EAP protocol
Explanation	Type of EAP authentication protocol unknown. EAP protocol not accepted.
Firewall Action	eap_authentication_will_fail
Recommended Action	None.
Revision	1

2.33.75. unknown_eap_status (ID: 01800604)

Default Severity	ERROR
Log Message	Failed to add EAP-SIM as eap protocol
Explanation	Failed to add EAP-SIM as accepted eap protocol.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.76. eap_but_not_passthrough (ID: 01800605)

Default Severity	INFORMATIONAL
Log Message	Radius and EAP enabled, but PASS THROUGH is not set as authentication method
Explanation	Radius and EAP enabled, but PASS THROUGH is not set as authentication method.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.77. eap_not_supported (ID: 01800606)

Default Severity	ERROR
Log Message	No support for EAP/RADIUS: no EAP protocols can be enabled
Explanation	CORE sw does not support EAP/RADIUS. I.e EAP protocols can be enabled.
Firewall Action	eap_authentication_will_fail
Recommended Action	None.
Revision	1

2.33.78. can_not_add_eap_auth_type (ID: 01800607)

Default Severity	INFORMATIONAL
Log Message	Can't add EAP authentication: insufficient information
Explanation	Can't add EAP authentication: insufficient information.
Firewall Action	continue_with_next_eap_userauth_rule

Recommended Action	None.
Revision	1

2.33.79. eap_disabled (ID: 01800608)

Default Severity	NOTICE
Log Message	EAP is not set as authentication method
Explanation	EAP is not set as authentication method for phase 1.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.80. no_eap_identity (ID: 01800609)

Default Severity	ERROR
Log Message	Failed to get EAP identity for tunnel <tunnelname>
Explanation	Failed to get EAP identity.
Firewall Action	eap_authentication_will_fail
Recommended Action	None.
Revision	1
Parameters	tunnelname

2.33.81. eap_disabled (ID: 01800610)

Default Severity	ERROR
Log Message	No EAP secret for tunnel <tunnelname>
Explanation	No stored eap secret for tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelname

2.33.82. no_eapstate (ID: 01800611)

Default Severity	ERROR
Log Message	Eapstate/Phase1 not available
Explanation	No Eapstate/Phase1 to get eap identity from.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.83. IDi_used_as_eap_id (ID: 01800612)

Default Severity	INFORMATIONAL
Log Message	IKEv2 IDi will be used as EAP identity
Explanation	IKEv2 IDi will be used as EAP identity.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.84. no_eap_identity (ID: 01800613)

Default Severity	ERROR
Log Message	No EAP identity established
Explanation	No EAP identity established.
Firewall Action	eap_authentication_will_fail
Recommended Action	None.
Revision	1

2.33.85. no_userauth_specified_for_xauth (ID: 01800614)

Default Severity	ERROR
Log Message	No XAuth userauth rule found for eap authentication with remote ike peer: <srcif> <remote_peer>
Explanation	No user authentication rule avaliable for xauth authentication.
Firewall Action	xauth_protocols_disabled
Recommended Action	Reconfigure_tunnel.

Revision	1
Parameters	remote_peer srcif

2.33.86. attach_of_eap_radius_server_failed (ID: 01800630)

Default Severity	INFORMATIONAL
Log Message	Failed to attach up EAP RADIUS server. Internal error code: <error>
Explanation	Failed to attach EAP RADIUS server.
Firewall Action	radius_server_not_attached
Recommended Action	None.
Revision	1
Parameters	error

2.33.87. no_eap_identity_or_radius_username (ID: 01800631)

Default Severity	ERROR
Log Message	We did not get any EAP identity/ RADIUS username
Explanation	We did not get any EAP identity/ RADIUS username.
Firewall Action	continue_radius_message
Recommended Action	None.
Revision	1

2.33.88. radius_timeout (ID: 01800633)

Default Severity	ERROR
Log Message	Timeout/internal error received from RADIUS server
Explanation	Timeout/internal error received from RADIUS server.
Firewall Action	radius_communication_disabled
Recommended Action	None.
Revision	1

2.33.89. radius_reject (ID: 01800634)

Default Severity	ERROR
Log Message	Radius Access Reject received from RADIUS server
Explanation	Radius Access Reject received from RADIUS server.
Firewall Action	radius_communication_disabled
Recommended Action	None.
Revision	1

2.33.90. radius_access_accept (ID: 01800635)

Default Severity	INFORMATIONAL
Log Message	Radius Access Accept received from RADIUS server
Explanation	Radius Access Accept received from RADIUS server.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.91. outofmem_forward_eap_packet (ID: 01800636)

Default Severity	ERROR
Log Message	Cannot create EAP packet to be sent to client
Explanation	Out of memory. Cannot create EAP packet to be sent to client.
Firewall Action	eap_packet_dropped
Recommended Action	None.
Revision	1

2.33.92. eap_packet_discarded (ID: 01800637)

Default Severity	ERROR
Log Message	Inavlid EAP packet detected
Explanation	Length less than 4 indicates that the EAP packet was invalid.
Firewall Action	eap_packet_discarded
Recommended Action	None.
Revision	1

2.33.93. outofmem_forward_eap_packet (ID: 01800638)

Default Severity	ERROR
Log Message	Dropping EAP packet from RADIUS server due to internal error
Explanation	Dropping EAP packet from RADIUS server due to internal error Radius_GetEAPRequest returns inconsistent values: requested length=[length], actual length=[actuallen].
Firewall Action	eap_packet_dropped
Recommended Action	None.
Revision	1
Parameters	length actuallen

2.33.94. outofmem_forward_eap_packet (ID: 01800639)

Default Severity	ERROR
Log Message	Out of memory. Unable to create RADIUS request
Explanation	Out of memory. Unable to create RADIUS request.
Firewall Action	eap_packet_dropped
Recommended Action	None.
Revision	1

2.33.95. failed_to_send_eap_id_response_to_radius (ID: 01800640)

Default Severity	ERROR
Log Message	Failed to send the EAP identity response to the RADIUS server
Explanation	Failed to send the EAP identity response to the RADIUS server.
Firewall Action	eap_packet_dropped
Recommended Action	None.
Revision	1

2.33.96. no_imsi (ID: 01800641)

Default Severity	WARNING

Log Message	User IMSI could not be extracted
Explanation	No IMSI could be extracted from the user identity (IDi) or fetched from the RADIUS server.
Firewall Action	disallowed_login
Recommended Action	None.
Revision	1

2.33.97. maximum_allowed_tunnels_limit_reached (ID: 01800900)

Default Severity	WARNING
Log Message	Negotiation aborted due to license restrictions. Reached maximum of <allowed_tunnels> active IPsec tunnels
Explanation	More tunnels and/or unique peers than the license allow are trying to establish.
Firewall Action	negotiation_aborted
Recommended Action	None.
Revision	2
Parameters	allowed_tunnels

2.33.98. ipsec_sa_destroy_peer_imsi (ID: 01800902)

Default Severity	INFORMATIONAL
Log Message	IPsec SA destroyed: peer <peer> | IMSI <imsi>
Explanation	Inform about destroyed child SA remote peer and IMSI.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	peer imsi

2.33.99. ipsec_sa_peer_imsi (ID: 01800903)

Default Severity	INFORMATIONAL
Log Message	Child SA established with peer <peer> using IMSI <imsi>

Explanation	Inform about remote peer and IMSI used to establish the child SA.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	imsi peer

2.33.100. ike_sa_rekeyed (ID: 01800905)

Default Severity	INFORMATIONAL
Log Message	IKE SA rekeyed, Local IKE peer: <local_ip>:<local_port> <local_id>, Remote IKE peer: <remote_iface>:<remote_ip>:<remote_port> <remote_id>.
Explanation	An IKE SA rekeyed successfully.
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	ipsec_if local_ip local_port remote_iface remote_ip remote_port local_id remote_id local_ike_spi remote_ike_spi initiator algorithms lifetime local_behind_nat remote_behind_nat

2.33.101. ike_sa_deleted (ID: 01800906)

Default Severity	INFORMATIONAL
Log Message	IKE SA deleted, Local IKE peer: <local_ip>:<local_port> <local_id>, Remote IKE peer: <remote_iface>:<remote_ip>:<remote_port> <remote_id>.
Explanation	An IKE SA was deleted.
Firewall Action	None
Recommended Action	None.

Revision	3
Parameters	ipsec_if local_ip local_port remote_iface remote_ip remote_port local_id remote_id local_ike_spi remote_ike_spi peer_dead

2.33.102. ipsec_sa_created (ID: 01800907)

Default Severity	INFORMATIONAL
Log Message	IPsec SA created, Source IP: <local_ip>, Destination IP: <remote_ip>, Inbound SPI: <esp_spi_in> Outbound: <esp_spi_out>.
Explanation	An IPsec SA was successfully created.
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	ipsec_if local_ip remote_ip cfgmode_ip esp_spi_in esp_spi_out ike_spi_i ike_spi_r esp_cipher esp_cipher_keysize esp_mac esp_mac_keysize life_seconds life_kilobytes dh_group dh_bits local_ts remote_ts imsi

2.33.103. ipsec_sa_rekeyed (ID: 01800908)

Default Severity	INFORMATIONAL
Log Message	IPsec SA rekeyed, Source IP: <local_ip>, Destination IP: <remote_ip>, Inbound SPI: <esp_spi_in>, Outbound SPI: <esp_spi_out>).

Explanation An IPsec SA rekeyed successfully.

Firewall Action None

Recommended Action None.

Revision 3

Parameters
ipsec_if
local_ip
remote_ip
cfgmode_ip
esp_spi_in
esp_spi_out
old_spi
ike_spi_i
ike_spi_r
esp_cipher
esp_cipher_keysize
esp_mac
esp_mac_keysize
life_seconds
life_kilobytes
initiator
dh_group
dh_bits
local_ts
remote_ts
imsi

2.33.104. ipsec_sa_deleted (ID: 01800909)

Default Severity INFORMATIONAL

Log Message IPsec SA deleted, Inbound SPI: <esp_spi_in>, Outbound SPI: <esp_spi_out>).

Explanation An IPsec SA was deleted.

Firewall Action None

Recommended Action None.

Revision 2

Parameters
ipsec_if
esp_spi_in
esp_spi_out

2.33.105. ipsec_sa_keys (ID: 01800910)

Default Severity INFORMATIONAL

Log Message IPsec SA keys, Inbound SPI: <esp_spi_in>, Outbound SPI: <esp_spi_out>.

Explanation	Encryption and authentication keys for an IPsec SA.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ipsec_if esp_spi_in cipher_key_in mac_key_in esp_spi_out cipher_key_out mac_key_out

2.33.106. out_of_memory (ID: 01801100)

Default Severity	ALERT
Log Message	Out of memory while trying to report a connection to the UNC.
Explanation	System ran out of memory while allocating packet data.
Firewall Action	scip_connection_report_not_sent
Recommended Action	None.
Revision	1

2.33.107. out_of_memory (ID: 01801101)

Default Severity	ALERT
Log Message	Out of memory while trying to report load to the UNC.
Explanation	System ran out of memory while allocating packet data.
Firewall Action	scip_load_report_not_sent
Recommended Action	None.
Revision	1

2.33.108. out_of_memory (ID: 01801102)

Default Severity	ALERT
Log Message	Out of memory while allocating client context.
Explanation	System ran out of memory while allocating client context.
Firewall Action	scip_disabled_for_client

Recommended Action	None.
Revision	1

2.33.109. connected (ID: 01801104)

Default Severity	NOTICE
Log Message	SCIP connection established with <scip_server> on port <server_port>.
Explanation	A SCIP connection was established.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	scip_server server_port

2.33.110. disconnected (ID: 01801105)

Default Severity	NOTICE
Log Message	SCIP connection with <scip_server> on port <scip_port> closed.
Explanation	A SCIP connection was closed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	scip_server scip_port

2.33.111. send_to_closed_scip_connection (ID: 01801106)

Default Severity	NOTICE
Log Message	SCIP-packet dropped while trying to sen to a closed SCIP connection.
Explanation	SCIP-packet dropped while trying to sen to a closed SCIP connection.
Firewall Action	drop
Recommended Action	None.
Revision	2

2.33.112. send_failed_no_free_socket (ID: 01801107)

Default Severity	WARNING
Log Message	No more SCIP sockets available. Could not connect to address <ipaddress>:<port>.
Explanation	SCIP-packet dropped. Out of sockets. No new connection could be set up.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipaddress port

2.33.113. trigger_non_ip_packet (ID: 01802001)

Default Severity	WARNING
Log Message	Trigger for non-IP packet of protocol <proto>. Dropping request for policy
Explanation	Trigger for non IP packet, dropping request.
Firewall Action	dropping_request
Recommended Action	None.
Revision	1
Parameters	proto

2.33.114. rule_not_active (ID: 01802002)

Default Severity	WARNING
Log Message	The rule is not in the active configuration. Dropping request for policy
Explanation	The rule is not in the active configuration, dropping request.
Firewall Action	dropping_request
Recommended Action	None.
Revision	1

2.33.115. malformed_packet (ID: 01802003)

Default Severity	WARNING
Log Message	Malformed packet for trigger.Dropping request for policy
Explanation	Malformed packet for trigger, dropping request.
Firewall Action	dropping_request
Recommended Action	None.
Revision	1

2.33.116. max_ipsec_sa_negotiations_reached (ID: 01802004)

Default Severity	WARNING
Log Message	The maximum number of active Quick-Mode negotiations reached. Rekey not done.
Explanation	Maximum number of active Quick-Mode negotiations reached.
Firewall Action	rekey_not_done
Recommended Action	None.
Revision	1

2.33.117. run_out_of_ike_sa (ID: 01802010)

Default Severity	WARNING
Log Message	Running out of IKE SAs (<num_p1_negs_active> concurrent IKE negotiations). Dropped new IKE SA request from <ikestr>
Explanation	Running out of IKE SAs dropping new IKE SA request.
Firewall Action	drop_new_ike_sa_request
Recommended Action	None.
Revision	1
Parameters	num_p1_negs_active ikestr

2.33.118. PSK_length_invalid (ID: 01802012)

Default Severity	INFORMATIONAL
Log Message	Remote identity specifies PSK that is not usable for selected IKE SA MAC algorithm (xcbcmac-aes)
Explanation	PSK key length invalid for xcbcmac-aes (restriced to 16 chars).

Firewall Action	authentication_failed
Recommended Action	Reconfigure_VPN.
Revision	1
Parameters	maxtunnels

2.33.119. ike_sa_rekey_failed (ID: 01802020)

Default Severity	WARNING
Log Message	Rekey of IKE sa failed: <statusmsg> (<status>), Local IKE peer: <local_peer>, Remote IKE peer: <remote_peer>, Initiator SPI: <spi_i>, Responder SPI: <spi_r>.
Explanation	Rekey of IKE SA failed.
Firewall Action	no_new_ike_sa
Recommended Action	None.
Revision	3
Parameters	statusmsg status local_peer remote_peer spi_i spi_r old_spi_i old_spi_r initiator

2.33.120. ike_sa_statistics (ID: 01802021)

Default Severity	INFORMATIONAL
Log Message	IKE SA negotiations: <done> done, <success> successful, <failed> failed
Explanation	Ike SA statistics.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	done success failed

2.33.121. ike_sa_failed (ID: 01802022)

Default Severity	WARNING
Log Message	IKE SA negotiation failed: <statusmsg> <reason>, Local IKE peer: <local_peer>, Remote IKE peer: <remote_peer>, Initiator SPI: <spi_i>, Responder SPI: <spi_r>.
Explanation	Negotiation of IKE SA failed.
Firewall Action	no_ike_sa
Recommended Action	None.
Revision	6
Parameters	statusmsg reason local_peer remote_peer spi_i spi_r initiator ipsec_if

2.33.122. ike_sa_statistics (ID: 01802023)

Default Severity	INFORMATIONAL
Log Message	IKE SA negotiations: <done> done, <success> successful, <failed> failed
Explanation	Ike SA statistics.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	done success failed

2.33.123. ipsec_sa_failed (ID: 01802049)

Default Severity	INFORMATIONAL
Log Message	IPsec SA negotiation failed: <statusmsg> <reason> Local IKE peer: <local_peer> Remote IKE peer: <remote_peer> Initiator SPI: <ike_spi_i> Responder SPI: <ike_spi_r>.
Explanation	IPsec SA negotiation failed.
Firewall Action	ipsec_sa_disabled
Recommended Action	None.

Revision	2
Parameters	statusmsg reason local_peer remote_peer ike_spi_i ike_spi_r

2.33.124. nat_mapping_changed_ike (ID: 01802050)

Default Severity	INFORMATIONAL
Log Message	NAT mapping changed, Local endpoint: <local_endpoint>, Remote endpoint: <remote_endpoint>, Initiator SPI: <ike_spi_i>, Responder SPI: <ike_spi_r>, IP address: <ip_addr> New port: <port>.
Explanation	NAT mappings changed for an IKE SA.
Firewall Action	updating_ike_sa
Recommended Action	None.
Revision	2
Parameters	local_endpoint remote_endpoint ike_spi_i ike_spi_r ip_addr port

2.33.125. nat_mapping_change_not_allowed (ID: 01802051)

Default Severity	INFORMATIONAL
Log Message	NAT mapping change not allowed, Local endpoint: <local_endpoint>, Remote endpoint: <remote_endpoint>, Initiator SPI: <ike_spi_i>, Responder SPI: <ike_spi_r>, New IP address: <ip_addr> New port: <port>.
Explanation	NAT mappings changed for an IKE SA.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	local_endpoint remote_endpoint ike_spi_i ike_spi_r ip_addr port

2.33.126. ipsec_sa_negotiation_aborted (ID: 01802060)

Default Severity	ERROR
Log Message	IPsec SA Negotiation aborted: AH can not be initiated with NAT-T
Explanation	Negotiation aborted since AH can not be initiated with NAT-T.
Firewall Action	ipsec_sa_negotiation_aborted
Recommended Action	None.
Revision	1

2.33.127. could_not_narrow_traffic_selectors (ID: 01802061)

Default Severity	ERROR
Log Message	Could not narrow traffic selectors SA from policy rule
Explanation	Failed to narrow configured traffic selectors.
Firewall Action	ipsec_sa_negotiation_aborted
Recommended Action	Reconfigure_VPN.
Revision	1

2.33.128. failed_to_narrow_traffic_selectors (ID: 01802062)

Default Severity	ERROR
Log Message	Failed to narrow traffic selectors SA remote access clients
Explanation	Failed to narrow traffic selector for config mode client.
Firewall Action	ipsec_sa_negotiation_aborted
Recommended Action	None.
Revision	2

2.33.129. malformed_remote_id_configured (ID: 01802070)

Default Severity	ERROR
Log Message	Malformed Remote IKE identity <remoteid> configured for tunnel
Explanation	Malformed remote identity for PSK specified in configuration.
Firewall Action	VPN_tunnel_invalid

Recommended Action	Reconfigure_remote_id.
Revision	1
Parameters	remoteid

2.33.130. malformed_psk_configured (ID: 01802071)

Default Severity	ERROR
Log Message	Malformed IKE secret (PSK) configured for tunnel
Explanation	Malformed IKE secret specified in configuration.
Firewall Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_PSK.
Revision	1

2.33.131. nat_mapping_changed_ipsec (ID: 01802080)

Default Severity	INFORMATIONAL
Log Message	NAT mapping changed, Local endpoint: <local_endpoint>, Remote endpoint: <remote_endpoint>, New port: <port>, SPI: <esp_spi_in>.
Explanation	NAT mappings changed for an IPsec SA.
Firewall Action	updating_ipsec_sa
Recommended Action	None.
Revision	1
Parameters	local_endpoint remote_endpoint port esp_spi_in

2.33.132. no_authentication_method_specified (ID: 01802100)

Default Severity	ERROR
Log Message	Neither pre-shared keys nor CA certificates nor EAP are specified for a tunnel
Explanation	No authentication method is specified for the tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.133. invalid_authentication_algorithm_configured (ID: 01802101)

Default Severity	ERROR
Log Message	AES counter mode cannot be used without an authentication algorithm
Explanation	AES counter mode specified but no authentication algoritm specified for tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.134. no_key_method_configured_for tunnel (ID: 01802102)

Default Severity	ERROR
Log Message	Tunnel does not specify any keying method (IKE or manual)
Explanation	No keying method (IKE/manual) is configured for tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.135. invalid_configuration_of_force_open (ID: 01802103)

Default Severity	ERROR
Log Message	Auto-start rule specifies more than one traffic selector item and no IKE peer is specified
Explanation	Can not use Auto-start rule (force open) for roaming tunnels.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.136. invalid_configuration_of_force_open (ID: 01802104)

Default Severity	ERROR

Log Message	Auto-start rule does not specify single IP address or domain name for its remote peer
Explanation	Can not use Auto-start rule (force open) for roaming tunnels.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.137. invalid_rule_setting (ID: 01802105)

Default Severity	ERROR
Log Message	Both REJECT and PASS defined for a rule
Explanation	Can not specify both pass and reject for a rule.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.138. invalid_rule_setting (ID: 01802107)

Default Severity	ERROR
Log Message	To-tunnel specified for a REJECT rule
Explanation	To-tunnel can not be specified for REJECT rule.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.139. max_number_of_policy_rules_reached (ID: 01802110)

Default Severity	CRITICAL
Log Message	The maximum number of policy rules reached
Explanation	The maximum number of policy rules reached.
Firewall Action	VPN_configuration_disabled
Recommended Action	Review the advanced setting IPsecMaxRules.
Revision	2

2.33.140. input_traffic_selector_corrupt (ID: 01802111)

Default Severity	ERROR
Log Message	Input traffic selector is corrupt. Cannot parse input traffic selector
Explanation	No authentication method is specified for the tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.141. input_traffic_selector_corrupt (ID: 01802112)

Default Severity	ERROR
Log Message	Input traffic selector contains more than the built in maximum number of items
Explanation	Input traffic selector contains more than the built in maximum number of items: IPSEC_MAX_RULE_TRAFFIC_SELECTORS_ITEMS.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.142. invalid_traffic_selectors (ID: 01802113)

Default Severity	ERROR
Log Message	Specified traffic selectors for the rule's are invalid
Explanation	Invalid traffic selectors are configured for tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.33.143. suspicious_outbound_rule (ID: 01802114)

Default Severity	ERROR
Log Message	Detected suspicious outbound IPsec rule without any selectors
Explanation	Detected suspicious outbound IPsec rule without any selectors specified.

Firewall Action	the_rule_might_not_work
Recommended Action	Reconfigure_IPsec.
Revision	2

2.33.144. failed_to_add_rule_to_engine (ID: 01802115)

Default Severity	ERROR
Log Message	Failed to add rule to engine database
Explanation	Failed to add rule to engine database.
Firewall Action	tunnel_will_not_work_as_expected
Recommended Action	None.
Revision	1

2.33.145. no_algorithms_configured_for_tunnel (ID: 01802200)

Default Severity	ERROR
Log Message	ESP tunnel is missing encryption and authentication algorithms
Explanation	ESP tunnel [tunnel] not configured with encryption and authentication algorithms.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.33.146. no_encryption_algorithm_configured_for_tunnel (ID: 01802201)

Default Severity	ERROR
Log Message	ESP tunnel <tunnel> is missing encryption algorithm. Null encryption algorithm must be specified if no encryption is required
Explanation	ESP tunnel not configured with any encryption algorithm, not even Null.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1

Parameters	tunnel

2.33.147. esp_null-null_configuration (ID: 01802202)

Default Severity	ERROR
Log Message	ESP NULL-NULL is proposed for this tunnel <tunnel>. This is forbidden by RFC 2406.
Explanation	Tunnel is configured with invalid algorithm: ESP NULL-NULL.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.33.148. no_authentication_algorithm_specified (ID: 01802203)

Default Severity	ERROR
Log Message	No authentication algorithm configured for AH tunnel <tunnel>
Explanation	AH tunnel is configured without spetication algorithm.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.33.149. AH_not_supported (ID: 01802204)

Default Severity	ERROR
Log Message	AH configured but not supported
Explanation	Tunnel [tunnel] configured for AH, but AH is not supported.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.33.150. invalid_cipher_keysize (ID: 01802205)

Default Severity	ERROR
Log Message	Configured max cipher key size <keysize> for tunnel <tunnel> is bigger than the built-in maximum <max>
Explanation	Tunnel configured invalid key size for cipher.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize tunnel max

2.33.151. invalid_mac_keysize (ID: 01802206)

Default Severity	ERROR
Log Message	Configured max MAC key size <keysize> is bigger for tunnel <tunnel> than the built-in maximum <max>
Explanation	Tunnel configured with invalid key size for cipher.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize tunnel max

2.33.152. invalid_tunnel_configuration (ID: 01802207)

Default Severity	ERROR
Log Message	Misconfiguration for tunnel <tunnel> Anti-replay detection must be enabled when using 64 bit sequence numbers
Explanation	Anti-replay detection must be enabled when using 64 bit sequence numbers.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1

Parameters	tunnel

2.33.153. invalid_tunnel_configuration (ID: 01802208)

Default Severity	ERROR
Log Message	No IPsec transform (AH or ESP) specified for tunnel <tunnel>
Explanation	IPsec transform type must be specified for tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2
Parameters	tunnel

2.33.154. invalid_tunnel_configuration (ID: 01802209)

Default Severity	ERROR
Log Message	Auto-start tunnel <tunnel> configured for `per-port' or `per-host' SA.
Explanation	`per-port' or `per-host' SA can not be specified for auto-start tunnels [tunnel].
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.33.155. invalid_tunnel_configuration (ID: 01802210)

Default Severity	ERROR
Log Message	Both `auto-start' and `dont-initiate' specified for tunnel <tunnel>
Explanation	Both `auto-start' and `dont-initiate' can not be specified for a tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.33.156. out_of_memory_for_tunnel (ID: 01802211)

Default Severity	ERROR
Log Message	Out of memory. Could not allocate memory for tunnel name! <tunnel>
Explanation	Out of memory. Could not allocate memory for tunnel name!.
Firewall Action	VPN_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	tunnel

2.33.157. out_of_memory_for_tunnel (ID: 01802212)

Default Severity	ERROR
Log Message	Out of memory. Could not allocate memory tunnel <tunnel> endpoints
Explanation	Out of memory. Could not allocate memory for tunnel endpoints!.
Firewall Action	VPN_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	tunnel

2.33.158. invalid_length_of_PSK_when_used_with_AES-XCBC_MAC (ID: 01802213)

Default Severity	ERROR
Log Message	Invalid length of local secret for tunnel when configured to use AES-XCBC Mac algorithm
Explanation	Local secret must be 16 octets long to be usable for AES-XCBC Mac algorithm.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.33.159. invalid_key_size (ID: 01802214)

Default Severity	ERROR

Log Message	Invalid key sizes specified for algorithms
Explanation	Invalid key sizes specified for algorithms.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.33.160. invalid_key_size (ID: 01802215)

Default Severity	ERROR
Log Message	Algorithm key sizes specified for unknown algorithm
Explanation	Algorithm key sizes specified for unknown algorithm.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.33.161. invalid_key_size (ID: 01802216)

Default Severity	ERROR
Log Message	Algorithm key sizes specified for unknown algorithm
Explanation	Algorithm key sizes specified for unknown algorithm.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.33.162. invalid_key_size (ID: 01802217)

Default Severity	ERROR
Log Message	Specified key size limits for cipher <alg> with fixed key size
Explanation	Configuration specifies key size limits for cipher with fixed key size.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2
Parameters	alg

2.33.163. invalid_cipher_keysize (ID: 01802218)

Default Severity	ERROR
Log Message	Configured max cipher key size <keysize> is bigger than the built-in maximum <max>
Explanation	Tunnel configured invalid key size for cipher.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize max

2.33.164. invalid_key_size (ID: 01802219)

Default Severity	ERROR
Log Message	Tunnel specified key size limits for mac <alg> with fixed key size
Explanation	Configuration specifies key size limits for cipher with fixed key size.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	alg

2.33.165. invalid_cipher_keysize (ID: 01802220)

Default Severity	ERROR
Log Message	Configured max MAC key size <keysize> is bigger than the built-in maximum <max>
Explanation	Tunnel configured invalid key size for MAC.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize max

2.33.166. no_matching_tunnel_found (ID: 01802221)

Default Severity	ERROR
Log Message	No tunnel found matching the local address <localaddr> , remote address <remoteaddr> and source interface <srcif>
Explanation	No tunnel found matching the local address and remote address.
Firewall Action	packet_will_be_discarded
Recommended Action	None.
Revision	1
Parameters	localaddr remoteaddr srcif

2.33.167. no_tunnel_id_specified (ID: 01802222)

Default Severity	ERROR
Log Message	No tunnel identity specified for tunnel
Explanation	No tunnel identity specified in configuration.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_VPN.
Revision	1

2.33.168. several_local_id_specified_for_tunnel (ID: 01802223)

Default Severity	ERROR
Log Message	More than one local id specified for tunnel
Explanation	Cannot add more than one local identity to a tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_VPN.
Revision	1

2.33.169. several_local_id_specified_for_tunnel (ID: 01802224)

Default Severity	ERROR
Log Message	More than one remote id specified for tunnel
Explanation	Cannot add more than one remote identity to a tunnel.

Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_VPN.
Revision	1

2.33.170. malformed_tunnel_id_configured (ID: 01802225)

Default Severity	ERROR
Log Message	Malformed identity <id> configured for tunnel
Explanation	Malformed identity specified in configuration.
Firewall Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_remote_id.
Revision	1
Parameters	id

2.33.171. several_secrets_specified_for_tunnel (ID: 01802226)

Default Severity	ERROR
Log Message	More than one secret specified for tunnel
Explanation	Cannot add more configure more than one secret for a tunnel.
Firewall Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_VPN.
Revision	1

2.33.172. malformed_psk_configured (ID: 01802228)

Default Severity	ERROR
Log Message	Malformed IKE secret (PSK) configured for tunnel
Explanation	Malformed IKE secret specified in configuration.
Firewall Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_PSK.
Revision	1

2.33.173. max_ike_sa_reached (ID: 01802400)

Default Severity	WARNING
Log Message	The maximum number of active IKE SAs reached
Explanation	Maximum number of active IKE SAs reached.
Firewall Action	negotiation_aborted
Recommended Action	Review your configuration or upgrade license.
Revision	3

2.33.174. max_ike_rekeys_reached (ID: 01802401)

Default Severity	NOTICE
Log Message	The maximum number of active IKE rekeys reached
Explanation	Maximum number of active IKE rekeys reached.
Firewall Action	rekey_aborted
Recommended Action	None.
Revision	1

2.33.175. max_phase1_sa_reached (ID: 01802402)

Default Severity	NOTICE
Log Message	The maximum number of active Phase-1 negotiations reached
Explanation	Maximum number of active Phase-1 negotiations reached.
Firewall Action	negotiation_aborted
Recommended Action	None.
Revision	1

2.33.176. max_active_quickmode_negotiation_reached (ID: 01802403)

Default Severity	NOTICE
Log Message	The maximum number of active Quick-Mode negotiations reached
Explanation	Maximum number of active Quick-Mode negotiations reached.
Firewall Action	quick-mode_not_done
Recommended Action	None.

Revision	1

2.33.177. warning_level_active_ipsec_sas_reached (ID: 01802404)

Default Severity	WARNING
Log Message	The number of active IPsec SA:s reached 90%
Explanation	The number of active IPsec SA:s reached 90%.
Firewall Action	ipsec_sa_created
Recommended Action	None.
Revision	1

2.33.178. warning_level_ike_sa_reached (ID: 01802405)

Default Severity	WARNING
Log Message	The number of active IKE SAs reached 90% of the maximum allowed
Explanation	The number of active IKE SAs reached 90% of the maximum allowed.
Firewall Action	negotiation_done
Recommended Action	None.
Revision	1

2.33.179. max_ipsec_sa_reached (ID: 01802406)

Default Severity	WARNING
Log Message	The maximum number of active IPsec SAs reached
Explanation	Maximum number of active IPsec SAs reached.
Firewall Action	negotiation_aborted
Recommended Action	Review your configuration or upgrade license.
Revision	1

2.33.180. invalid_format_syslog_audit (ID: 01802500)

Default Severity	NOTICE
Log Message	Cannot use binary formatting for syslog auditing.

Explanation	Cannot use binary formatting for syslog auditing.
Firewall Action	None
Recommended Action	None.
Revision	1

2.33.181. cannot_create_audit_file_context (ID: 01802501)

Default Severity	NOTICE
Log Message	Cannot create audit file context. Filename for audit: <filename>
Explanation	Cannot create audit file context.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	filename

2.33.182. could_not_decode_certificate (ID: 01802600)

Default Severity	WARNING
Log Message	Could not decode Certificate to pem format. The certificate may be corrupted or it was given in unrecognized format.
Explanation	Could_not_decode_certificate.
Firewall Action	certificate_invalid
Recommended Action	None.
Revision	1

2.33.183. could_not_convert_certificate (ID: 01802601)

Default Severity	WARNING
Log Message	Could not convert CMi certificate to X.509 certificate
Explanation	Could not convert CMi certificate to X.509 certificate.
Firewall Action	certificate_invalid
Recommended Action	None.
Revision	1

2.33.184. could_not_get_subject_nam_from_ca_cert (ID: 01802602)

Default Severity	WARNING
Log Message	Could not get subject name from a CA certificate. This certificate is not usable as an IPsec authenticator, and is not inserted into loal list of trusted CAs
Explanation	Could not get subject name from a CA certificate.
Firewall Action	certificate_not_trusted
Recommended Action	None.
Revision	1

2.33.185. could_not_set_cert_to_non_CRL_issuer (ID: 01802603)

Default Severity	WARNING
Log Message	Could not set CA certificate to non-CRL issuer. This may cause authentication errors if valid CRLs are not available
Explanation	Could not set CA certificate to non-CRL issuer.
Firewall Action	certificate_not_usable_if_no_valid_CRLs
Recommended Action	None.
Revision	1

2.33.186. could_not_force_cert_to_be_trusted (ID: 01802604)

Default Severity	WARNING
Log Message	Could not force CA certificate as a point of trust
Explanation	Could not force CA certificate as a point of trust.
Firewall Action	certificate_disabled
Recommended Action	None.
Revision	1

2.33.187. could_not_trusted_set_for_cert (ID: 01802605)

Default Severity	WARNING

Log Message	Could not set the trusted set for a CA certificate
Explanation	Could not set the trusted set for a CA certificate.
Firewall Action	certificate_disabled
Recommended Action	None.
Revision	1

2.33.188. could_not_insert_cert_to_db (ID: 01802606)

Default Severity	ERROR
Log Message	Can not insert CA certificate into local database
Explanation	Can not insert CA certificate into local database.
Firewall Action	certificate_disabled
Recommended Action	None.
Revision	1

2.33.189. could_not_decode_certificate (ID: 01802607)

Default Severity	WARNING
Log Message	Could not decode Certificate to pem format. The certificate may be corrupted or it was given in unrecognized format.
Explanation	Could_not_decode_certificate.
Firewall Action	certificate_invalid
Recommended Action	None.
Revision	1

2.33.190. could_not_lock_certificate (ID: 01802608)

Default Severity	WARNING
Log Message	Could not lock certificate in cache
Explanation	Could not lock certificate in cache.
Firewall Action	certificate_invalid
Recommended Action	None.
Revision	1

2.33.191. could_not_insert_cert_to_db (ID: 01802609)

Default Severity	ERROR
Log Message	Could not insert certificate into local database
Explanation	Could not insert certificate into local database.
Firewall Action	certificate_disabled
Recommended Action	None.
Revision	1

2.33.192. could_not_decode_crl (ID: 01802610)

Default Severity	WARNING
Log Message	Could not decode CRL. The certificate may be corrupted or it was given in unrecognized format. File format may be wrong
Explanation	Could_not_decode_CRL.
Firewall Action	certificate_invalid
Recommended Action	None.
Revision	1

2.33.193. http_crl_failed (ID: 01802611)

Default Severity	ERROR
Log Message	Failed to get CRL over HTTP. <reason>
Explanation	CRL couldn't be fetched from the URL specified in the certificate.
Firewall Action	None
Recommended Action	Check your connectivity to the URL or disable CRL lookup on you certificates. Note that disabling the CRL lookup cause the gateway to accept certificates that may have been revoked by the certificate authority.
Revision	1
Parameters	reason url

2.33.194. Certificate_contains_bad_IP_address (ID: 01802705)

Default Severity	WARNING

Log Message	Certificate contains bad IP address: length=<len>
Explanation	Certificate contains bad IP address.
Firewall Action	try_next_certificate
Recommended Action	None.
Revision	1
Parameters	len

2.33.195. dn_name_as_subject_alt_name (ID: 01802706)

Default Severity	WARNING
Log Message	Directory names are not supported as subject alternative names. Skipping DN: <dn_name>
Explanation	Directory specified as subject alternative name.
Firewall Action	skip_dn_name
Recommended Action	None.
Revision	1
Parameters	dn_name

2.33.196. could_not_decode_certificate (ID: 01802707)

Default Severity	WARNING
Log Message	Could not decode Certificate to pem format. The certificate may be corrupted or it was given in unrecognized format.
Explanation	Could_not_decode_certificate.
Firewall Action	certificate_invalid
Recommended Action	None.
Revision	1

2.33.197. cfgmode_exchange_event (ID: 01802709)

Default Severity	INFORMATIONAL
Log Message	Event occured for config mode <cfgmode> exchange: <msg>. Internal severity level: <int_severity>
Explanation	Config mode exchange event.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	cfgmode msg int_severity

2.33.198. remote_access_address (ID: 01802710)

Default Severity	INFORMATIONAL
Log Message	Addresses for remote access attributes: <ipaddr> expires time <time>
Explanation	Addresses for remote access attributes.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ipaddr time

2.33.199. remote_access_dns (ID: 01802711)

Default Severity	INFORMATIONAL
Log Message	DNS for remote access attributes: <dns_server>
Explanation	DNS for remote access attributes.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	dns_server

2.33.200. remote_access_wins (ID: 01802712)

Default Severity	INFORMATIONAL
Log Message	WINS for remote access attributes: <win>
Explanation	WINS for remote access attributes.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	win

2.33.201. remote_access_dhcp (ID: 01802713)

Default Severity	INFORMATIONAL
Log Message	DHCP for remote access attributes: <dhcp_s>
Explanation	DHCP remote access attributes.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	dhcp_s

2.33.202. remote_access_subnets (ID: 01802714)

Default Severity	INFORMATIONAL
Log Message	Subnets remote access attributes: <subnets>
Explanation	Subnets remote access attributes.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	subnets

2.33.203. event_on_ike_sa (ID: 01802715)

Default Severity	WARNING
Log Message	Event: <msg> occured for IKE SA: <side>. Internal severity level: <int_severity>
Explanation	Event occured at IKE SA.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	side msg int_severity

2.33.204. ipsec_sa_selection_failed (ID: 01802717)

Default Severity	WARNING
Log Message	Selection of IPsec SA failed due to <reason>. Internal severity level: <int_severity>
Explanation	Failed to select a SA.
Firewall Action	no_ipsec_sa_selected
Recommended Action	None.
Revision	2
Parameters	reason int_severity

2.33.205. crl_search_failed (ID: 01802719)

Default Severity	WARNING
Log Message	Certificate manager search failure: <reason>. Internal severity level: <int_severity>
Explanation	Search for a CRL failed. Certificate validation will conintue as CRL checks are not enforced by the current configuration.
Firewall Action	continuing
Recommended Action	None.
Revision	1
Parameters	reason int_severity

2.33.206. outofmem_create_policy_manager (ID: 01802800)

Default Severity	CRITICAL
Log Message	Failed to create Policy Manger
Explanation	Could not allocate memory for policymanager object.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.207. ek_accelerator_disabled (ID: 01802801)

Default Severity	ERROR
Log Message	Failed to set external key accelerator
Explanation	Invalid type of external key accelerator defined.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.208. ek_accelerator_disabled (ID: 01802802)

Default Severity	ERROR
Log Message	Failed to set init info to external key accelerator
Explanation	Invalid init info to external key accelerator.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.209. outofmem_create_engine (ID: 01802901)

Default Severity	CRITICAL
Log Message	Failed to allocate memory for engine object
Explanation	Could not allocate memory for engine object.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.210. failed_init_fastpath (ID: 01802902)

Default Severity	CRITICAL
Log Message	Failed to initialize fastpath
Explanation	Failed to initialize fastpath.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.211. init_rulelooklup_failed (ID: 01802903)

Default Severity	CRITICAL
Log Message	Initialization of rule lookup failed
Explanation	Initialization of rule lookup failed.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.212. init_rule_looklup_failed (ID: 01802904)

Default Severity	CRITICAL
Log Message	Allocating default drop rule failed!
Explanation	Allocating default drop rule failed!.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.213. init_rule_looklup_failed (ID: 01802905)

Default Severity	CRITICAL
Log Message	allocating default pass rule failed!
Explanation	Allocating default pass rule failed!.
Firewall Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.33.214. maximum_nr_of_ipsec_sa_per_ike_sa_reached (ID: 01803000)

Default Severity	ERROR
Log Message	Maximum number (<max_ipsec>) of allowed IPsec SAs per IKE SA reached by peer <peerip>
Explanation	Maximum number of allowed IPsec SA per IKE SA reached by peer.

Firewall Action	Discarding request and sending No Additional SAs response
Recommended Action	Discarding request and sending No Additional SAs response.
Revision	1
Parameters	max_ipsec peerip

2.33.215. ipsec_sa_per_ike_sa_limit_violated to many times (ID: 01803001)

Default Severity	ERROR
Log Message	Maximum number of IPsec SAs limit has been violated too many times (<limit>)
Explanation	Maximum number of IPsec SAs limit has been violated too many times.
Firewall Action	Discarding request and deleting SA
Recommended Action	Discarding request and deleting SA.
Revision	1
Parameters	limit

2.33.216. certificate_validation_check_failed (ID: 01803100)

Default Severity	WARNING
Log Message	Warning: Host certificate <certname> has expired <not_valid_after>
Explanation	Host certificate has expired.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	certname not_valid_after

2.33.217. certificate_validation_check_warning (ID: 01803101)

Default Severity	WARNING
Log Message	Warning: Host certificate <certname> expires <not_valid_after>
Explanation	Host certificate expires within two days.

Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	certname not_valid_after

2.33.218. audit_event (ID: 01803200)

Default Severity	INFORMATIONAL
Log Message	An audit event occured: <msg>. Internal severity level: <int_severity>
Explanation	An audit event occured in the IPsec stack.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	msg int_severity

2.33.219. faild_to_link_ike_and_userauth (ID: 01803300)

Default Severity	WARNING
Log Message	Faild to link IKE SA with userauth object. No userauth object were found for peer <peer> with IMSI <imsi>. The imported SA will be destroyed.
Explanation	Failed to link an imported IKE SA with an userauthentication object.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	peer imsi

2.33.220. faild_to_find_userauthobject_for_ipsec_sa (ID: 01803302)

Default Severity	NOTICE
Log Message	No userauth object were found for IP <cfgmodeip> on iface <iface>. The IPsec SA will not be imported.

Explanation	Faild to find an userauth object when importing a IPsec SA. The IPsec SA will not be imported.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	cfgmodeip iface

2.33.221. modexp_accel_failed (ID: 01803400)

Default Severity	NOTICE
Log Message	Hardware acceleration of modexp calculation failed due to <msg>.
Explanation	The failed calculation will be made in software instead. Hardware acceleration can fail due to valid reasons like a full request queue. A lot of these logs during a short timeframe could indicate issues with hardware acceleration.
Firewall Action	None
Recommended Action	Verify that the firewall is not in a overloaded state. If it's not overloaded and a lot of these logs is generated, contact the support and report this issue.
Revision	2
Parameters	msg

2.33.222. eap_authentication_failed (ID: 01803500)

Default Severity	WARNING
Log Message	EAP Authentication failed (<errorcode>).
Explanation	Client failed EAP authentication.
Firewall Action	ike_negotiation_aborted
Recommended Action	None.
Revision	1
Parameters	errorcode

2.33.223. monitored_host_reachable (ID: 01803600)

Default Severity	INFORMATIONAL
Log Message	Monitored host <ip> is reachable over tunnel <tunnel>.

Explanation	Monitored host started to respond on ICMP ping.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	ip tunnel

2.33.224. monitored_host_unreachable (ID: 01803601)

Default Severity	WARNING
Log Message	Monitored host <ip> didn't respond. Deleting all IKE and IPsec SAs for tunnel <tunnel>
Explanation	Monitored host didn't respond on ICMP ping. All IKE and IPsec SAs for the tunnel interface will be deleted and traffic routed into the tunnel will trigger a new IKE negotiation against the remote peer.
Firewall Action	sas_deleted
Recommended Action	Check the connectivity of the monitored host.
Revision	1
Parameters	ip tunnel

2.33.225. failed_to_attach_radius (ID: 01803700)

Default Severity	WARNING
Log Message	Failed to attach RADIUS (<errorcode>) server in IKE negotiation for peer <peer_ip>:<peer_port>
Explanation	Failed to attach RADIUS server communication, IKE negotiation will fail.
Firewall Action	fail_ike_negotiation
Recommended Action	None.
Revision	1
Parameters	errorcode peer_ip peer_port

2.33.226. failed_to_attach_radius (ID: 01803701)

Default Severity	WARNING

Log Message	Failed to attach RADIUS (<errorcode>) server in IKE negotiation for peer <peer_ip>:<peer_port>
Explanation	Failed to attach RADIUS server communication, IKE negotiation will fail.
Firewall Action	fail_ike_negotiation
Recommended Action	None.
Revision	1
Parameters	errorcode peer_ip peer_port

2.34. IPV6_ND

These log messages refer to the **IPV6_ND (Neighbor Discovery events)** category.

2.34.1. neighbor_discovery_resolution_failed (ID: 06400009)

Default Severity	WARNING
Log Message	Neighbor Discovery resolution failed
Explanation	Neighbor Discovery query was not resolved before the cache entry expired.
Firewall Action	remove_entry
Recommended Action	None.
Revision	1
Parameters	ipaddr iface

2.34.2. nd_resolution_success (ID: 06400020)

Default Severity	NOTICE
Log Message	ND entry was added to the ND cache.
Explanation	ND entry was added to the ND cache.
Firewall Action	added_entry
Recommended Action	None.
Revision	1
Parameters	enetaddr ipaddr iface

2.34.3. nd_spoofed_option_address (ID: 06400028)

Default Severity	WARNING
Log Message	ND HW sender address matches our own address, but the option address does not. Dropping packet.
Explanation	The Neighbor Discovery packet Ethernet sender address appears to be our own, but the Link Layer option address does not. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.4. nd_spoofed_hw_sender (ID: 06400029)

Default Severity	WARNING
Log Message	ND HW sender address matches our own address. Dropping packet.
Explanation	The Neighbor Discovery packet Ethernet sender address appears to be our own. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.5. neighbor_discovery_cache_size_limit_reached (ID: 06400030)

Default Severity	NOTICE
Log Message	Neighbor Discovery cache size limit reached
Explanation	The Neighbor Discovery cache size limit has been reached. Current license limit is [limit].
Firewall Action	None
Recommended Action	Update your license to allow a greater amount of concurrent Neighbor Discovery entries.
Revision	1
Parameters	limit

2.34.6. nd_option_hw_address_multicast (ID: 06400031)

Default Severity	WARNING
Log Message	ND Link Layer option contains Enet multicast address. Dropping packet.
Explanation	The Neighbor Discovery packet Link Layer option contains an Ethernet multicast address. Dropping packet.
Firewall Action	drop

Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.7. nd_option_hw_address_mismatch (ID: 06400032)

Default Severity	WARNING
Log Message	ND Link Layer option Enet sender mismatch. Dropping packet.
Explanation	The Neighbor Discovery packet Link Layer option does not match HW sender. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.8. nd_option_hw_address_mismatch (ID: 06400033)

Default Severity	NOTICE
Log Message	ND Link Layer option Enet sender mismatch. Dropping packet.
Explanation	The Neighbor Discovery packet Link Layer option does not match HW sender. Allowing packet.
Firewall Action	allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.9. nd_duplicated_option (ID: 06400034)

Default Severity	WARNING
Log Message	The same ND option appears more than once in the same packet. Dropping
Explanation	The Neighbor Discovery packet Link Layer Address Source appears more than once in the same packet. Dropping packet.
Firewall Action	drop

Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.10. nd_duplicated_option (ID: 06400035)

Default Severity	WARNING
Log Message	The same ND option appears more than once in the same packet. Dropping packet.
Explanation	The Neighbor Discovery packet Link Layer Address Target appears more than once in the same packet. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.11. nd_illegal_lladdress_option_size (ID: 06400036)

Default Severity	WARNING
Log Message	Illegal option size. Dropping
Explanation	The Neighbor Discovery packet option size is illegal. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.12. nd_illegal_lladdress_option_size (ID: 06400037)

Default Severity	WARNING
Log Message	Illegal option size. Dropping
Explanation	The Neighbor Discovery packet option size is illegal. Dropping packet.
Firewall Action	drop

Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.13. nd_illegal_prefix_info_option_size (ID: 06400038)

Default Severity	WARNING
Log Message	Illegal option size. Dropping
Explanation	The Neighbor Discovery packet option size is illegal. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.14. nd_illegal_redirect_option_size (ID: 06400039)

Default Severity	WARNING
Log Message	Illegal option size. Dropping
Explanation	The Neighbor Discovery packet option size is illegal. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.15. nd_illegal_mtu_option_size (ID: 06400040)

Default Severity	WARNING
Log Message	Illegal option size. Dropping
Explanation	The Neighbor Discovery packet option size is illegal. Dropping packet.
Firewall Action	drop

Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.16. nd_zero_size_option (ID: 06400041)

Default Severity	WARNING
Log Message	Illegal option size. Dropping
Explanation	The Neighbor Discovery packet option size is zero. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.17. nd_option_truncated (ID: 06400042)

Default Severity	WARNING
Log Message	Neighbor Discovery packet truncated at ND option. Dropping
Explanation	The Neighbor Discovery packet is truncated at ND option. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.18. nd_packet_truncated (ID: 06400043)

Default Severity	WARNING
Log Message	Neighbor Discovery packet truncated at L4 header. Dropping
Explanation	The Neighbor Discovery packet is truncated at L4 header. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.19. nd_unknown_icmp_code (ID: 06400044)

Default Severity	WARNING
Log Message	Unsupported ICMP code. Dropping
Explanation	The Neighbor Discovery packet ICMP code is unknown. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.20. nd_spoofed_target (ID: 06400045)

Default Severity	WARNING
Log Message	Neighbor Advertisement Target IP <targetip> is my address, but Ethernet address <targetenet> is not. Dropping
Explanation	The Neighbor Advertisement packet target IP address matches that of the receiving interface, but the target link layer address does not. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	targetip targetenet
Context Parameters	Rule Name Packet Buffer

2.34.21. nd_spoofed_sender (ID: 06400046)

Default Severity	WARNING
Log Message	Sender IP <senderip> is my address. Dropping
Explanation	The Neighbor Discovery packet sender IP address matches that of the receiving interface. Dropping packet.

Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	senderip
Context Parameters	Rule Name Packet Buffer

2.34.22. nd_hoplimit_reached (ID: 06400047)

Default Severity	WARNING
Log Message	Neighbor Discovery packet from <senderip> appears to have been routed. Dropping
Explanation	The Neighbor Discovery packet IP header contains a Hop Limit smaller than 255. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	senderip
Context Parameters	Rule Name Packet Buffer

2.34.23. nd_multicast_target_address (ID: 06400048)

Default Severity	WARNING
Log Message	Neighbor Discovery target address <targetip> is multicast. Dropping
Explanation	The Neighbor Discovery target IP address is a multicast address, this is illegal according to RFC4861. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	targetip
Context Parameters	Rule Name Packet Buffer

2.34.24. invalid_nd_sender_ip_address (ID: 06400049)

Default Severity	WARNING
Log Message	Failed to verify Neighbor Discovery sender IP address. Dropping
Explanation	The Neighbor Discovery sender IP address could not be verified according to the "access" section, and the packet is dropped.
Firewall Action	drop
Recommended Action	If all Neighbor Discovery sender IP addresses should be accepted without validation, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.25. nd_access_allowed_expect (ID: 06400050)

Default Severity	NOTICE
Log Message	Allowed by expect rule in access section
Explanation	The Neighbor Discovery sender IP address is verified by an expect rule in the access section.
Firewall Action	access_allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.26. nd_na_send_failure (ID: 06400051)

Default Severity	WARNING
Log Message	Failed to send Neighbor Advertisement packet.
Explanation	The system received a Neighbor Solicitation for one of its addresses but failed to reply with a Neighbor Advertisement packet.
Firewall Action	none
Recommended Action	None.
Revision	1

2.34.27. nd_unknown_sender (ID: 06400052)

Default Severity	WARNING

Log Message	Sender IP <senderip> is the Unknown Address. Dropping packet.
Explanation	The Neighbor Advertisement packet sender IP address matches that of the Unknown Address (::). Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	senderip
Context Parameters	Rule Name Packet Buffer

2.34.28. nd_missing_tll_opt (ID: 06400053)

Default Severity	WARNING
Log Message	Neighbor Advertisement from <senderip> without target link-layer option. Dropping packet.
Explanation	The Neighbor Advertisement packet is missing the Target Link-Layer option. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	senderip
Context Parameters	Rule Name Packet Buffer

2.34.29. nd_spoofed_dpd_reply (ID: 06400054)

Default Severity	WARNING
Log Message	Dead peer probe reply HW address <targetenet> does not match the cached address <cachedenet>. Dropping packet.
Explanation	The dead peer probe reply packet target HW address does not match the cached address. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	cachedenet targetenet
Context Parameters	Rule Name

Packet Buffer

2.34.30. nd_mcast_dpd_reply (ID: 06400055)

Default Severity	WARNING
Log Message	Dead peer probe answered with multicast message. Dropping packet.
Explanation	The dead peer probe reply packet destination IP is a multicast address. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.31. nd_advert_for_static_entry (ID: 06400056)

Default Severity	WARNING
Log Message	Neighbor Advertisement for static entry hw address <cachedenet>, advertised as <targetenet>. Dropping packet.
Explanation	A Neighbor Advertisement for a configured static entry was received. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	cachedenet targetenet
Context Parameters	Rule Name Packet Buffer

2.34.32. nd_blatant_advertisement (ID: 06400057)

Default Severity	WARNING
Log Message	Forged Neighbor Advertisement claiming cached enet address <cachedenet> should be <targetenet>. Dropping packet.
Explanation	An unsolicited Neighbor Advertisement claiming to be solicited was received. Dropping packet.
Firewall Action	drop

Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	cachedenet targetenet
Context Parameters	Rule Name Packet Buffer

2.34.33. nd_updated_entry (ID: 06400058)

Default Severity	NOTICE
Log Message	ND cache entry <ipaddress> updated from <oldenet> to <newenet>.
Explanation	A Neighbor Advertisement updated an entry in the Neighbor Discovery cache.
Firewall Action	allow
Recommended Action	None.
Revision	1
Parameters	ipaddress oldenet newenet
Context Parameters	Rule Name Packet Buffer

2.34.34. nd_update_entry_request (ID: 06400059)

Default Severity	NOTICE
Log Message	ND cache entry <ipaddress> update from <oldenet> to <newenet> request. DPD old address.
Explanation	A Neighbor Advertisement requests updating an entry in the Neighbor Discovery cache. Performing Dead Peer Detection before allowing changes.
Firewall Action	dpd_old_entry
Recommended Action	None.
Revision	1
Parameters	ipaddress oldenet newenet
Context Parameters	Rule Name Packet Buffer

2.34.35. nd_update_entry_request (ID: 06400060)

Default Severity	NOTICE
Log Message	ND cache entry <ipaddress> update from <oldenet> to <newenet> request. Dropping packet.
Explanation	A Neighbor Advertisement requests updating an entry in the Neighbor Discovery cache. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipaddress oldenet newenet
Context Parameters	Rule Name Packet Buffer

2.34.36. nd_broadcast_enet (ID: 06400061)

Default Severity	WARNING
Log Message	Neighbor Discovery packet ethernet destination is broadcast. Dropping
Explanation	The Neighbor Discovery packet ethernet destination is broadcast. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.37. nd_dad_probe_unicast_dest (ID: 06400062)

Default Severity	WARNING
Log Message	Duplicate address probe with unicast destination address from <sendermac>. Dropping packet.
Explanation	The Neighbor Solicitation Duplicatge Address Probe packet destination IP address is not a multicast address. Dropping packet.
Firewall Action	drop

Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	sendermac
Context Parameters	Rule Name Packet Buffer

2.34.38. nd_rs_unicast_target (ID: 06400063)

Default Severity	WARNING
Log Message	Router Solicitation destination address <destip> isn't multicast. Dropping
Explanation	The Router Solicitation destination IP address isn't a multicast address, this is illegal according to RFC4861. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	destip
Context Parameters	Rule Name Packet Buffer

2.34.39. nd_rs_illegal_option (ID: 06400064)

Default Severity	WARNING
Log Message	Router Solicitation packet contains an illegal option. Dropping
Explanation	The Router Solicitation packet contains a source link layer adderss option, this is illegal according to RFC4861. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.40. nd_ns_illegal_option (ID: 06400065)

Default Severity	WARNING
Log Message	Neighbor Solicitation packet contains an illegal option. Dropping

Explanation	The Neighbor Solicitation packet contains a source link layer adderss option, this is illegal according to RFC4861. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.41. nd_updated_entry (ID: 06400066)

Default Severity	NOTICE
Log Message	ND cache entry <ipaddress> updated from <oldenet> to <newenet>.
Explanation	A Neighbor Solicitation updated an entry in the Neighbor Discovery cache.
Firewall Action	allow
Recommended Action	None.
Revision	1
Parameters	ipaddress oldenet newenet
Context Parameters	Rule Name Packet Buffer

2.34.42. nd_update_entry_request (ID: 06400067)

Default Severity	NOTICE
Log Message	ND cache entry <ipaddress> update from <oldenet> to <newenet> request. DPD old address.
Explanation	A Neighbor Solicitation requests updating an entry in the Neighbor Discovery cache. Performing Dead Peer Detection before allowing changes.
Firewall Action	dpd_old_entry
Recommended Action	None.
Revision	1
Parameters	ipaddress oldenet newenet
Context Parameters	Rule Name

Packet Buffer

2.34.43. nd_update_entry_request (ID: 06400068)

Default Severity	NOTICE
Log Message	ND cache entry <ipaddress> update from <oldenet> to <newenet> request. Dropping packet.
Explanation	A Neighbor Solicitation requests updating an entry in the Neighbor Discovery cache. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipaddress oldenet newenet
Context Parameters	Rule Name Packet Buffer

2.34.44. nd_sol_multicast_dest_address (ID: 06400069)

Default Severity	WARNING
Log Message	Neighbor Discovery destination address <destip> is multicast but the solicited flag is set. Dropping
Explanation	The Neighbor Discovery destination IP address is a multicast address but the solicited flag is set, this is illegal according to RFC4861. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	destip
Context Parameters	Rule Name Packet Buffer

2.34.45. nd_dad_probe_faulty_dest (ID: 06400070)

Default Severity	WARNING
Log Message	Duplicate address probe with faulty destination address from <sendermac>. Dropping packet.

Explanation	The Neighbor Solicitation Duplicatge Address Probe packet destination IP address is not a solicited node multicast address. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Parameters	sendermac
Context Parameters	Rule Name Packet Buffer

2.34.46. nd_dupe_addr_detected (ID: 06400071)

Default Severity	WARNING
Log Message	Conflicting duplicate address probe received on <iface>. IPv6 disabled.
Explanation	The link-local EUI64-generated [iface] address is already occupied by another host in the network. Resolve the address conflict by changing the ethernet address on the interface or on the conflicting host. IPv6 disabled.
Firewall Action	IPv6_Disabled
Recommended Action	Resolve the address conflict.
Revision	1
Parameters	iface
Context Parameters	Rule Name Packet Buffer

2.34.47. nd_dupe_addr_detected (ID: 06400072)

Default Severity	WARNING
Log Message	Duplicate address reply received on <iface>. IPv6 disabled.
Explanation	The link-local EUI64-generated [iface] address is already occupied by another host in the network. Resolve the address conflict by changing the ethernet address on the interface or on the conflicting host. IPv6 disabled.
Firewall Action	IPv6_Disabled
Recommended Action	Resolve the address conflict.
Revision	1
Parameters	iface

Context Parameters	Rule Name Packet Buffer

2.34.48. more_ndoptcount (ID: 06400073)

Default Severity	WARNING
Log Message	Number of options more than ICMP6MaxOptND - <optcount>
Explanation	Received a packet with number of options more than ICMP6MaxOptND.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	optcount
Context Parameters	Rule Name

2.34.49. more_ndoptcount (ID: 06400074)

Default Severity	WARNING
Log Message	Number of options more than ICMP6MaxOptND - <optcount>
Explanation	Received a packet with number of options more than ICMP6MaxOptND.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	optcount
Context Parameters	Rule Name

2.34.50. nd_rd_missing_pi_option (ID: 06400075)

Default Severity	WARNING
Log Message	Router Advertisement is missing Prefix Information option. Ignoring
Explanation	The Router Advertisement packet is missing a Prefix Information option, it is needed for the system to auto-configure interface network.
Firewall Action	drop
Recommended Action	Re-configure the advertising router.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.34.51. router_discovered (ID: 06400076)

Default Severity	NOTICE
Log Message	Interface <iface> have successfully processed a Router Advertisement
Explanation	An interface have successfully processed a Router Advertisement.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface router_ip
Context Parameters	Packet Buffer

2.34.52. ra_prefix (ID: 06400077)

Default Severity	NOTICE
Log Message	Interface <iface> have successfully processed a Router Advertisement Prefix Information option
Explanation	An interface have successfully processed a Router Advertisement Prefix Information option.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface prefix
Context Parameters	Packet Buffer

2.34.53. router_cease (ID: 06400078)

Default Severity	NOTICE
Log Message	Router <ip> on interface <iface> is ceasing to be a router
Explanation	A router on the local network is ceasing to be a router.

Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface ip
Context Parameters	Packet Buffer

2.34.54. router_not_found (ID: 06400079)

Default Severity	NOTICE
Log Message	Unable to find router on interface <iface>
Explanation	The gateway has solicited the local network for a router but have not received a reply.
Firewall Action	None
Recommended Action	Check connection and router reachability.
Revision	1
Parameters	iface

2.35. IP_ERROR

These log messages refer to the **IP_ERROR (Packet discarded due to IP header error(s))** category.

2.35.1. too_small_packet (ID: 01500001)

Default Severity	WARNING
Log Message	Packet is too small to contain IPv4 header
Explanation	The received packet is too small to contain an IPv4 header, and will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Context Parameters	Rule Name Packet Buffer

2.35.2. disallowed_ip_ver (ID: 01500002)

Default Severity	WARNING
Log Message	Disallowed IP version <ipver>
Explanation	The received packet has a disallowed IP version, and will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	ipver
Context Parameters	Rule Name Packet Buffer

2.35.3. invalid_ip_length (ID: 01500003)

Default Severity	WARNING
Log Message	Invalid IP header length - IPTotLen=<iptotlen>, IPHdrLen=<iphdrlen>
Explanation	The received packet IP header specifies an invalid length. The IP Header length can never be smaller than 20 bytes or longer than the total packet length. Dropping packet.

Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	iptotlen iphdrlen
Context Parameters	Rule Name Packet Buffer

2.35.4. invalid_ip_length (ID: 01500004)

Default Severity	WARNING
Log Message	Invalid IP header length, IPTotLen=<iptotlen>, RecvLen=<recvlen>
Explanation	The received packet IP total length is larger than the received transport data. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	iptotlen recvlen
Context Parameters	Rule Name Packet Buffer

2.35.5. invalid_ip_checksum (ID: 01500005)

Default Severity	WARNING
Log Message	Invalid IP header checksum - RecvChkSum=<recvchksum>, CompChkSum=<compchksum>
Explanation	The received packet IP header checksum is invalid, dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	recvchksum compchksum
Context Parameters	Rule Name Packet Buffer

2.35.6. Invalid_ip6_flow (ID: 01500020)

Default Severity	WARNING
Log Message	Invalid flow label value
Explanation	The received packet with flow label other than zero.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	flow_label
Context Parameters	Rule Name Packet Buffer

2.35.7. Invalid_ip6_flow (ID: 01500021)

Default Severity	WARNING
Log Message	Invalid flow label value
Explanation	The received packet with flow label other than zero.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	flow_label
Context Parameters	Rule Name Packet Buffer

2.35.8. Invalid_ip6_tc (ID: 01500022)

Default Severity	WARNING
Log Message	Invalid traffic class value
Explanation	The received packet with traffic class other than zero.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	traffic_class
Context Parameters	Rule Name Packet Buffer

2.35.9. Invalid_ip6_tc (ID: 01500023)

Default Severity	WARNING
Log Message	Invalid traffic class value
Explanation	The received packet with traffic class other than zero.
Firewall Action	strip
Recommended Action	None.
Revision	1
Parameters	traffic_class
Context Parameters	Rule Name Packet Buffer

2.35.10. Invalid_ip6_tc (ID: 01500024)

Default Severity	WARNING
Log Message	Invalid traffic class value
Explanation	The received packet with traffic class other than zero.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	traffic_class
Context Parameters	Rule Name Packet Buffer

2.35.11. faulty_payload (ID: 01500025)

Default Severity	WARNING
Log Message	Packet actual payload size <ipactpaylen> does not match IPv6 header payload size <ippaylen>.
Explanation	The received packet IPv6 header payload size is faulty, and will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ippaylen

	ipactpaylen
Context Parameters	Rule Name Packet Buffer

2.35.12. too_small_packet (ID: 01500026)

Default Severity	WARNING
Log Message	Packet is too small to contain IPv6 header
Explanation	The received packet is too small to contain an IPv6 header, and will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Context Parameters	Rule Name Packet Buffer

2.36. IP_FLAG

These log messages refer to the **IP_FLAG (Events concerning the IP header flags)** category.

2.36.1. ttl_low (ID: 01600001)

Default Severity	WARNING
Log Message	Received packet with too low TTL of <ttl>. Min TTL is <ttlmin>. Ignoring
Explanation	The received packet has a TTL (Time-To-Live) field which is too low. Ignoring and forwarding packet anyway.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	ttl ttlmin
Context Parameters	Rule Name Packet Buffer

2.36.2. ip_rsv_flag_set (ID: 01600002)

Default Severity	NOTICE
Log Message	The IP Reserved Flag was set. Ignoring
Explanation	The received packet has the IP Reserved Flag set. This is ignored.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.3. ip_rsv_flag_set (ID: 01600003)

Default Severity	WARNING
Log Message	The IP Reserved Flag was set, stripping
Explanation	The received packet has the IP Reserved Flag set. Removing it.
Firewall Action	strip_flag
Recommended Action	None.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.4. hop_limit_low (ID: 01600004)

Default Severity	WARNING
Log Message	Received packet with too low HopLimit of <hoplimit>. Min HopLimit is <hoplimitmin>. Ignoring
Explanation	The received packet has a HopLimit field which is too low. Ignoring and forwarding packet anyway.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	hoplimit hoplimitmin
Context Parameters	Rule Name Packet Buffer

2.37. IP_OPT

These log messages refer to the **IP_OPT (Events concerning the IP header options)** category.

2.37.1. source_route (ID: 01700001)

Default Severity	NOTICE
Log Message	Packet has a source route
Explanation	The packet has a source route. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.2. timestamp (ID: 01700002)

Default Severity	NOTICE
Log Message	Packet has a timestamp IP Option
Explanation	The packet contains a timestamp IP Option. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.3. router_alert (ID: 01700003)

Default Severity	NOTICE
Log Message	Packet has a router alert IP option
Explanation	The packet contains a router alert IP Option. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.4. ipopt_present (ID: 01700004)

Default Severity	NOTICE
Log Message	IP Option <ipopt>(<optname>) is present
Explanation	The packet contains an IP Option. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	ipopt optname
Context Parameters	Rule Name Packet Buffer

2.37.5. ipoptlen_too_small (ID: 01700010)

Default Severity	WARNING
Log Message	Type <ipopt> is multibyte, available <avail>. Dropping
Explanation	The IP Option type is multi byte which requires two bytes, and there is less than two bytes available. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt minoptlen avail
Context Parameters	Rule Name Packet Buffer

2.37.6. ipoptlen_invalid (ID: 01700011)

Default Severity	WARNING
Log Message	Type <ipopt> claims len=<optlen>, available=<avail>. Dropping
Explanation	The IP Option type does not fit in the option space. Dropping packet.
Firewall Action	drop
Recommended Action	None.

Revision	1
Parameters	ipopt optlen avail
Context Parameters	Rule Name Packet Buffer

2.37.7. multiple_ip_option_routes (ID: 01700012)

Default Severity	WARNING
Log Message	Multiple source/return routes in IP options. Dropping
Explanation	There are multiple source/return routes specified among the IP Options. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.8. bad_length (ID: 01700013)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad length <optlen> for <route> Route. Dropping
Explanation	An invalid length is specified for the IP Option type. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen route
Context Parameters	Rule Name Packet Buffer

2.37.9. bad_route_pointer (ID: 01700014)

Default Severity	WARNING

Log Message	IP Option Type <ipopt>: Bad Source Route Pointer <routeptr>. Dropping
Explanation	The packet has a Source Route Pointer, which is invalid. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt routeptr
Context Parameters	Rule Name Packet Buffer

2.37.10. source_route_disallowed (ID: 01700015)

Default Severity	WARNING
Log Message	Source route IP option disallowed. Dropping
Explanation	The packet has a source route, which is disallowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.11. multiple_ip_option_timestamps (ID: 01700016)

Default Severity	WARNING
Log Message	Multiple timestamps in IP options. Dropping
Explanation	The packet contains mutliple timestamps in IP Options. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.12. bad_timestamp_len (ID: 01700017)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad length <optlen>. Dropping
Explanation	The packet contains an IP Option, which has an invalid lengh. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen
Context Parameters	Rule Name Packet Buffer

2.37.13. bad_timestamp_pointer (ID: 01700018)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad Timestamp Pointer <tsptr>. Dropping
Explanation	The packet contains an invalid Timestamp Pointer. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt tsptr
Context Parameters	Rule Name Packet Buffer

2.37.14. bad_timestamp_pointer (ID: 01700019)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad Timestamp Pointer <tsptr> with overflow <oflo>. Dropping
Explanation	The packet contains an invalid Timestamp Pointer, with Overflow. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt

	tsptr oflo
Context Parameters	Rule Name Packet Buffer

2.37.15. timestamp_disallowed (ID: 01700020)

Default Severity	WARNING
Log Message	Timestamp IP option disallowed. Dropping
Explanation	The packet contains a timestamp IP Option, which is disallowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.16. router_alert_bad_len (ID: 01700021)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad length <optlen>. Dropping
Explanation	Packet contains a router alert IP Option, which has an invalid Length. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen
Context Parameters	Rule Name Packet Buffer

2.37.17. router_alert_disallowed (ID: 01700022)

Default Severity	WARNING
Log Message	Router Alert IP Option disallowed. Dropping
Explanation	The packet contains a timestamp IP Option, which is disallowed. Dropping packet.

Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.18. ipopt_present_disallowed (ID: 01700023)

Default Severity	WARNING
Log Message	IP Option <ipopt>(<optname>) is present. Dropping
Explanation	The packet contains an IP Option, which is disallowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optname
Context Parameters	Rule Name Packet Buffer

2.37.19. invalid_ip6payload_for_jumbo (ID: 01700039)

Default Severity	WARNING
Log Message	Non zero ip6 payload length for jumbo option
Explanation	Received a non zero ip6 payload length jumbo option packet.
Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.20. small_payload (ID: 01700040)

Default Severity	WARNING
Log Message	Jumbo option packet with a payload less than 65535
Explanation	Received a jumbo option packet with a payload less than 65535.

Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.21. small_payload (ID: 01700041)

Default Severity	WARNING
Log Message	Jumbo option packet with a payload less than 65535
Explanation	Received a jumbo option packet with a payload less than 65535.
Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.22. invalid_ip6payload_for_jumbo (ID: 01700042)

Default Severity	WARNING
Log Message	Non zero ip6 payload length for jumbo option
Explanation	Received a non zero ip6 payload length jumbo option packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.23. recvd_jumbo (ID: 01700043)

Default Severity	WARNING
Log Message	Received a jumbo option packet
Explanation	Received a jumbo option packet.
Firewall Action	none
Recommended Action	None.
Revision	1

Context Parameters	Rule Name

2.37.24. invalid_order (ID: 01700044)

Default Severity	WARNING
Log Message	Invalid Jumbogram packet option other than in hop by hop header
Explanation	Received a Jumbogram packet other than in hop by hop header.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.25. recvd_jumbo (ID: 01700045)

Default Severity	WARNING
Log Message	Received a jumbo option packet
Explanation	Received a jumbo option packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.26. recvd_jumbo (ID: 01700046)

Default Severity	WARNING
Log Message	Received a jumbo option packet
Explanation	Received a jumbo option packet.
Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.27. rcvd_router_alert (ID: 01700047)

Default Severity	WARNING
Log Message	Received Router Alert option Packet
Explanation	Received Router Alert option Packet.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.28. rcvd_router_alert (ID: 01700048)

Default Severity	WARNING
Log Message	Received Router Alert option Packet
Explanation	Received Router Alert option Packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.29. rcvd_router_alert (ID: 01700049)

Default Severity	WARNING
Log Message	Received Router Alert option Packet
Explanation	Received Router Alert option Packet.
Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.30. invalid_option (ID: 01700050)

Default Severity	WARNING
Log Message	Invalid IPv6 extension header option encountered.
Explanation	The packet contains an IPv6 extension header option of unknown

	type. The option will be ignored and the rest of the packet will be processed.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.31. invalid_option (ID: 01700051)

Default Severity	WARNING
Log Message	Invalid IPv6 extension header option encountered.
Explanation	The packet contains an IPv6 extension header option of unknown type. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.32. invalid_option (ID: 01700052)

Default Severity	WARNING
Log Message	Invalid IPv6 extension header option encountered.
Explanation	The packet contains an IPv6 extension header option of unknown type. Sending ICMPv6 Parameter Problem to the packet originator.
Firewall Action	send_param_problem
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37.33. rcvd_ha_Option (ID: 01700053)

Default Severity	WARNING
Log Message	Received Home address option Packet

Explanation	Received Home address option Packet.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.34. rcvd_ha_Option (ID: 01700054)

Default Severity	WARNING
Log Message	Received Home address option Packet
Explanation	Received Home address option Packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.35. rcvd_ha_Option (ID: 01700055)

Default Severity	WARNING
Log Message	Received Home address option Packet
Explanation	Received Home address option Packet.
Firewall Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.36. invalid_padN_data (ID: 01700056)

Default Severity	WARNING
Log Message	Option data containing non-zero value
Explanation	Option data containing non-zero value.
Firewall Action	none
Recommended Action	None.

Revision	1
Context Parameters	Rule Name

2.37.37. invalid_padN_data (ID: 01700057)

Default Severity	WARNING
Log Message	Option data containing non-zero value
Explanation	Option data containing non-zero value.
Firewall Action	strip
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.38. invalid_padN_data (ID: 01700058)

Default Severity	WARNING
Log Message	Option data containing non-zero value
Explanation	Option data containing non-zero value.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.39. invalid_optLen (ID: 01700059)

Default Severity	WARNING
Log Message	Option Length is more than the specified number of bytes 5
Explanation	Option Length is more than the specified number of bytes 5.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	OptLen
Context Parameters	Rule Name

2.37.40. mismatch_ip_eth (ID: 01700060)

Default Severity	WARNING
Log Message	IP and ethernet destination mismatch
Explanation	IP and ethernet destination mismatch.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.41. mismatch_ip_eth (ID: 01700061)

Default Severity	WARNING
Log Message	IP and ethernet destination mismatch
Explanation	IP and ethernet destination mismatch.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.42. invalid_optlen (ID: 01700062)

Default Severity	WARNING
Log Message	Option Length is more than the size of extension header
Explanation	Option Length is more than the size of extension header.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.43. invalid_order (ID: 01700064)

Default Severity	WARNING

Log Message	Invalid Router Alert option other than in hop by hop header
Explanation	Received a Router Alert packet other than in hop by hop header.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.44. invalid_order (ID: 01700065)

Default Severity	WARNING
Log Message	Invalid home address options other than in destination header
Explanation	Received a home address packet other than in destination header.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.45. excessive_padding (ID: 01700066)

Default Severity	WARNING
Log Message	Multiple occurance of Pad1/PadN option
Explanation	Multiple occurance of Pad1/PadN option.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.46. repeated_option (ID: 01700067)

Default Severity	WARNING
Log Message	Received a packet with a repetitive options
Explanation	Received a packet with a repetitive options.
Firewall Action	none

Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.47. more_optcount (ID: 01700068)

Default Severity	WARNING
Log Message	Number of options more than IP6MaxOPH - <optcount>
Explanation	Received a packet with number of options more than IP6MaxOPH.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	optcount
Context Parameters	Rule Name

2.37.48. more_optcount (ID: 01700069)

Default Severity	WARNING
Log Message	Number of options more than IP6MaxOPH - <optcount>
Explanation	Received a packet with number of options more than IP6MaxOPH.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	optcount
Context Parameters	Rule Name

2.37.49. ip6_rhother (ID: 01700070)

Default Severity	WARNING
Log Message	Routing packet with type other than 0 or 2
Explanation	Received Routing packet other than 0 or 2.
Firewall Action	none
Recommended Action	None.

Revision	1
Context Parameters	Rule Name

2.37.50. ip6_rhother (ID: 01700071)

Default Severity	WARNING
Log Message	Routing packet with type other than 0 or 2
Explanation	Received Routing packet other than 0 or 2.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.51. ip6_rh2 (ID: 01700072)

Default Severity	WARNING
Log Message	Routing header with type 2 packet
Explanation	Received Routing header type 2 packet.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.52. ip6_rh2 (ID: 01700073)

Default Severity	WARNING
Log Message	Routing header with type 2 packet
Explanation	Received Routing header type 2 packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.53. ip6_rh0 (ID: 01700074)

Default Severity	WARNING
Log Message	Routing header with type 0 packet
Explanation	Received Routing header type 0 packet.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.54. ip6_rh0 (ID: 01700075)

Default Severity	WARNING
Log Message	Routing header with type 0 packet
Explanation	Received Routing header type 0 packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.55. too_small_packet (ID: 01700076)

Default Severity	WARNING
Log Message	Packet is too small to process
Explanation	The received packet is too small to contain the next header, and will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Context Parameters	Rule Name Packet Buffer

2.37.56. invalid_extnhdr_order (ID: 01700077)

Default Severity	WARNING
Log Message	Invalid header order

Explanation	Received a packet with invalid header order.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.57. invalid_ip6_exthdr (ID: 01700078)

Default Severity	WARNING
Log Message	Extension header length is greater than IP6ExtHdr Setting
Explanation	The received packet with extension header length is greater than IP6ExtHdr Setting.
Firewall Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.58. invalid_ip6_exthdr (ID: 01700079)

Default Severity	WARNING
Log Message	Extension header length is greater than IP6ExtHdr Setting
Explanation	The received packet with extension header length is greater than IP6ExtHdr Setting.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.37.59. invalid_nextheader (ID: 01700080)

Default Severity	WARNING
Log Message	Unrecognized IPv6 next header.
Explanation	A packet with unrecognized IPv6 Next Header was received.
Firewall Action	drop

Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.38. IP_PROTO

These log messages refer to the **IP_PROTO (IP Protocol verification events)** category.

2.38.1. multicast_ethernet_ip_address_mismatch (ID: 07000011)

Default Severity	WARNING
Log Message	Received packet with a destination IP address <ip_multicast_addr> that does not match the Ethernet multicast address <eth_multicast_addr>
Explanation	A packet was received with an IP multicast Ethernet address as destination address. The IP address in the IP header does however not match it. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ip_multicast_addr eth_multicast_addr
Context Parameters	Rule Name Packet Buffer

2.38.2. invalid_ip4_header_length (ID: 07000012)

Default Severity	WARNING
Log Message	Invalid IP4 Header length - total length is <totlen> bytes. Dropping
Explanation	The packet contains an invalid IP4 Header Length. The total length is more than 64 Kb, which is not allowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	totlen
Context Parameters	Rule Name Packet Buffer

2.38.3. ttl_zero (ID: 07000013)

Default Severity	WARNING

Log Message	Received packet with zero TTL. Dropping
Explanation	A packet was received with a TTL (Time-To-Live) field set to zero, which is not allowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.38.4. ttl_low (ID: 07000014)

Default Severity	WARNING
Log Message	Received packet with too low TTL of <ttl>. Min TTL is <ttlmin>. Dropping
Explanation	The received packet has a TTL (Time-To-Live) field which is too low. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ttl ttlmin
Context Parameters	Rule Name Packet Buffer

2.38.5. ip_rsv_flag_set (ID: 07000015)

Default Severity	WARNING
Log Message	The IP Reserved Flag was set. Dropping
Explanation	The received packet has the IP Reserved Flag set. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.38.6. oversize_tcp (ID: 07000018)

Default Severity	WARNING
Log Message	Configured size limit for the TCP protocol exceeded. Dropping
Explanation	The configured size limit for the TCP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.7. invalid_tcp_header (ID: 07000019)

Default Severity	WARNING
Log Message	Invalid TCP header - IPDataLen=<ipdatalen>, TCPHdrLen=<tcphdrlen>. Dropping
Explanation	The TCP packet contains an invalid header. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen tcphdrlen
Context Parameters	Rule Name Packet Buffer

2.38.8. oversize_udp (ID: 07000021)

Default Severity	WARNING
Log Message	Configured size limit for the UDP protocol exceeded. Dropping
Explanation	The configured size limit for the UDP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto

Context Parameters	Rule Name Packet Buffer

2.38.9. invalid_udp_header (ID: 07000022)

Default Severity	WARNING
Log Message	Invalid UDP header - IPDataLen=<ipdatalen>, UDPTotLen=<udptotlen>. Dropping
Explanation	The UDP packet contains an invalid header. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen udptotlen
Context Parameters	Rule Name Packet Buffer

2.38.10. oversize_icmp (ID: 07000023)

Default Severity	WARNING
Log Message	Configured size limit for the ICMP protocol exceeded. Dropping
Explanation	The configured size limit for the ICMP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.11. invalid_icmp_header (ID: 07000024)

Default Severity	WARNING
Log Message	Invalid ICMP header - IPDataLen=<ipdatalen>, ICMPMinLen=<icmpminlen>. Dropping
Explanation	The ICMP packet contains an invalid header. Dropping packet.
Firewall Action	drop

Recommended Action	None.
Revision	1
Parameters	ipdatalen icmpminlen
Context Parameters	Rule Name Packet Buffer

2.38.12. multicast_ethernet_ip_address_mismatch (ID: 07000033)

Default Severity	WARNING
Log Message	Received packet with a destination IP address <ip_multicast_addr> that does not match the Ethernet multicast address <eth_multicast_addr>
Explanation	A packet was received with an IP multicast Ethernet address as destination address, but the IP address in the IP header does however not match it. This is a known exploit, though the gateway is currently configured to forward these packets.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	ip_multicast_addr eth_multicast_addr
Context Parameters	Rule Name Packet Buffer

2.38.13. oversize_gre (ID: 07000050)

Default Severity	WARNING
Log Message	Configured size limit for the GRE protocol exceeded. Dropping
Explanation	The configured size limit for the GRE protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.14. oversize_esp (ID: 07000051)

Default Severity	WARNING
Log Message	Configured size limit for the ESP protocol exceeded. Dropping
Explanation	The configured size limit for the ESP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.15. oversize_ah (ID: 07000052)

Default Severity	WARNING
Log Message	Configured size limit for the AH protocol exceeded. Dropping
Explanation	The configured size limit for the AH protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.16. oversize_skip (ID: 07000053)

Default Severity	WARNING
Log Message	Configured size limit for the SKIP protocol exceeded. Dropping
Explanation	The configured size limit for the SKIP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1

Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.17. oversize_ospf (ID: 07000054)

Default Severity	WARNING
Log Message	Configured size limit for the OSPF protocol exceeded. Dropping
Explanation	The configured size limit for the OSPF protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.18. oversize_ipip (ID: 07000055)

Default Severity	WARNING
Log Message	Configured size limit for the IPIP protocol exceeded. Dropping
Explanation	The configured size limit for the IPIP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.19. oversize_ipcomp (ID: 07000056)

Default Severity	WARNING
Log Message	Configured size limit for the IPComp protocol exceeded. Dropping
Explanation	The configured size limit for the IPComp protocol was exceeded. Dropping packet.

Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.20. oversize_l2tp (ID: 07000057)

Default Severity	WARNING
Log Message	Configured size limit for the L2TP protocol exceeded. Dropping
Explanation	The configured size limit for the L2TP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.21. oversize_ip (ID: 07000058)

Default Severity	WARNING
Log Message	Configured size limit for IP protocol exceeded. Dropping
Explanation	The configured size limit for the IP protocol was exceeded. Dropping packet.
Firewall Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.38.22. hop_limit_zero (ID: 07000059)

Default Severity	WARNING

Log Message	Forward IPv6 packet with zero HopLimit. Dropping
Explanation	Try to forward a IPv6 packet with the HopLimit field set to zero, which is not allowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	3
Context Parameters	Rule Name Packet Buffer

2.38.23. hop_limit_low (ID: 07000060)

Default Severity	WARNING
Log Message	Received packet with too low HopLimit of <hoplimit>. Min HopLimit is <hoplimitmin>. Dropping
Explanation	The received packet has a HopLimit field which is too low. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	hoplimit hoplimitmin
Context Parameters	Rule Name Packet Buffer

2.38.24. fragmented_icmp (ID: 07000070)

Default Severity	WARNING
Log Message	This ICMP type is not allowed to be fragmented. Dropping
Explanation	The ICMP type is not allowed to be framented. Only "Echo" and "EchoReply" are allowed to be fragmented. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.38.25. invalid_icmp_data_too_small (ID: 07000071)

Default Severity	WARNING
Log Message	Invalid ICMP data length. ICMPDataLen=<icmpdatalen> ICMPIPHdrMinLen=<icmpiphdrminlen>. Dropping
Explanation	The ICMP data is not large enough to contain an IPv4 Header. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpiphdrminlen
Context Parameters	Rule Name Packet Buffer

2.38.26. invalid_icmp_data_ip_ver (ID: 07000072)

Default Severity	WARNING
Log Message	Invalid ICMP data. ICMPDataLen=<icmpdatalen> ICMPIPVer=<icmpipver>. Dropping
Explanation	An invalid IP version is specified in the ICMP data. Version 4 expected. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipver
Context Parameters	Rule Name Packet Buffer

2.38.27. invalid_icmp_data_too_small (ID: 07000073)

Default Severity	WARNING
Log Message	Invalid ICMP data length. ICMPDataLen=<icmpdatalen> ICMPIPHdrLen=<icmphdrlen>. Dropping
Explanation	The ICMP data length is invalid. It must be large enough for the actual header, and the header must specify that it is atleast 20 bytes long. Dropping packet.
Firewall Action	drop
Recommended Action	None.

Revision	1
Parameters	icmpdatalen icmphdrlen
Context Parameters	Rule Name Packet Buffer

2.38.28. invalid_icmp_data_invalid_ip_length (ID: 07000074)

Default Severity	WARNING
Log Message	Invalid ICMP data length. ICMPDataLen=<icmpdatalen> ICMPIPDataLen=<icmpipdatalen> ICMPIPDataMinLen=<icmpipdataminlen>. Dropping
Explanation	The ICMP data length is invalid. The contained IP data must be atleast 8 bytes long. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipdatalen icmpipdataminlen
Context Parameters	Rule Name Packet Buffer

2.38.29. invalid_icmp_data_invalid_paramprob (ID: 07000075)

Default Severity	WARNING
Log Message	Invalid ICMP ProbPtr. ICMPDataLen=<icmpdatalen> ICMPIPDataLen=<icmpipdatalen> ParamProbPtr=<paramprobptr>. Dropping
Explanation	Invalid ICMP Parameter Problem pointer. Parameter Problem pointer is not within the allowed range. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipdatalen paramprobptr
Context Parameters	Rule Name Packet Buffer

2.38.30. illegal_sender_address (ID: 07000076)

Default Severity	WARNING
Log Message	Source address does not identify a single node uniquely. Dropping
Explanation	The source address is ending in zeroes. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.38.31. dest_beyond_scope (ID: 07000080)

Default Severity	WARNING
Log Message	Destination is beyond the scope of the source address. Dropping
Explanation	Link-local source address and a global-scope destination address. Dropping packet.
Firewall Action	drop
Recommended Action	Verify that no faulty network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.38.32. ttl_zero (ID: 07000111)

Default Severity	WARNING
Log Message	Forward IPv4 packet with zero TTL. Dropping
Explanation	Try to forward a IPv4 packet with the TTL field set to zero, which is not allowed. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	3
Context Parameters	Rule Name Packet Buffer

2.39. L2TP

These log messages refer to the **L2TP (L2TP tunnel events)** category.

2.39.1. l2tpclient_resolve_successful (ID: 02800001)

Default Severity	NOTICE
Log Message	L2TP client <iface> resolved <remotegwname> to <remotegw>
Explanation	The L2TP client successfully resolved the DNS name of the remote gateway.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.39.2. l2tpclient_resolve_failed (ID: 02800002)

Default Severity	WARNING
Log Message	L2TP client <iface> failed to resolve <remotegwname>
Explanation	The L2TP client failed to resolve the DNS name of the remote gateway.
Firewall Action	None
Recommended Action	Make sure you have configured the DNS name of the remote gateway and the DNS servers correctly.
Revision	1
Parameters	iface remotegwname

2.39.3. l2tpclient_init (ID: 02800003)

Default Severity	NOTICE
Log Message	L2TP client initialized, request sent to server on <remotegw>
Explanation	The L2TP client has been initialized and a request has been sent to the remote gateway.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	iface remotegw

2.39.4. l2tp_connection_disallowed (ID: 02800004)

Default Severity	NOTICE
Log Message	L2TP connection disallowed according to rule <rule>! Tunnel ID: <tunnelid>, Session ID: <sessionid>
Explanation	The L2TP connection is disallowed according to the specified userauth rule.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule tunnelid sessionid

2.39.5. unknown_l2tp_auth_source (ID: 02800005)

Default Severity	WARNING
Log Message	Unknown L2TP authentication source for <rule>! Tunnel ID: <tunnelid>, Session ID: <sessionid>
Explanation	The authentication source for the specified userauth rule is unknown to the L2TP server.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule tunnelid sessionid

2.39.6. only_routes_set_up_by_server_iface_allowed (ID: 02800006)

Default Severity	WARNING
Log Message	L2TP server <iface> received a packet routed by a route not set up by the interface itself. Dropping packet

Explanation	The L2TP server received a packet that was routed to the interface by a route that was either manually configured or set up by another subsystem.
Firewall Action	drop
Recommended Action	Make sure no manually configured routes to the L2TP server interface exists in the configuration.
Revision	1
Parameters	iface

2.39.7. l2tp_session_closed (ID: 02800007)

Default Severity	NOTICE
Log Message	Closed L2TP session. Session ID: <sessionid>, Tunnel ID: <tunnelid>
Explanation	The L2TP session with the specified session ID has been closed. The session was set up using the specified tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface sessionid tunnelid

2.39.8. l2tp_tunnel_closed (ID: 02800008)

Default Severity	NOTICE
Log Message	Closed L2TP tunnel. Tunnel ID: <tunnelid>, Interface: <iface>.
Explanation	The L2TP tunnel with the specified tunnel ID has been closed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface tunnelid

2.39.9. session_closed (ID: 02800009)

Default Severity	WARNING
Log Message	MPPE failed but is required, closing session <sessionid> to

	<remotegw> on <iface>
Explanation	MPPE is required by the configuration but the MPPE negotiation failed. Session will be closed.
Firewall Action	None
Recommended Action	Make sure the peer is capable of MPPE encryption, or disable the MPPE requirement.
Revision	1
Parameters	iface sessionid remotegw

2.39.10. l2tp_session_request (ID: 02800010)

Default Severity	NOTICE
Log Message	L2TP session request sent. Tunnel ID: <tunnelid>
Explanation	An L2TP session request has been sent over the specified L2TP tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid

2.39.11. l2tp_session_up (ID: 02800011)

Default Severity	NOTICE
Log Message	L2TP session up. Tunnel ID: <tunnelid>, Session ID: <sessionid>, Auth: <auth>, MPPE: <mppe>
Explanation	The L2TP session negotiation has completed successfully.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid sessionid auth mppe

2.39.12. l2tp_no_userauth_rule_found (ID: 02800014)

Default Severity	WARNING
Log Message	Did not find a matching userauth rule for this L2TP server! Tunnel ID: <tunnelid>, Session ID: <sessionid>
Explanation	The L2TP server was unsuccessful trying to find a matching userauth rule.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	tunnelid sessionid

2.39.13. l2tp_session_request (ID: 02800015)

Default Severity	NOTICE
Log Message	L2TP session request received. Tunnel ID: <tunnelid>
Explanation	A new session request was received on the specified tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid

2.39.14. l2tp_session_up (ID: 02800016)

Default Severity	NOTICE
Log Message	L2TP session up. Tunnel ID: <tunnelid>, Session ID: <sessionid>, User: <user>, Auth: <auth>, MPPE: <mppe>, Assigned IP: <assigned_ip>
Explanation	The L2TP session negotiation has completed successfully.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid sessionid user auth mppe assigned_ip

2.39.15. failure_init_radius_accounting (ID: 02800017)

Default Severity	WARNING
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accounting will be disabled
Explanation	Failed to send START message to RADIUS accounting server. RADIUS accounting will be disabled for this session.
Firewall Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.
Revision	1

2.39.16. l2tpclient_tunnel_up (ID: 02800018)

Default Severity	NOTICE
Log Message	L2TP tunnel to <remotegw> is up. Tunnel ID: <tunnelid>
Explanation	L2TP tunnel negotiated successfully.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid iface remotegw

2.39.17. malformed_packet (ID: 02800019)

Default Severity	WARNING
Log Message	Malformed packet received from <remotegw> on tunnel <iface>. Error code: <error_code>
Explanation	A malformed packet was received by the L2TP interface.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw error_code

2.39.18. unknown_ctrl_conn_id (ID: 02800020)

Default Severity	WARNING
Log Message	Unknown Control Connection ID <ctrlconnid> from <remotegw> on tunnel <iface>.
Explanation	A packet with an unknown Control Connection ID was received by the L2TP interface.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw ctrlconnid

2.39.19. l2tp_session_closed (ID: 02800037)

Default Severity	NOTICE
Log Message	Closed L2TP session. Session ID: <sessionid>, Tunnel ID: <ctrlconnid>
Explanation	The L2TP session with the specified session ID has been closed. The session was set up using the specified tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface sessionid ctrlconnid

2.39.20. l2tp_tunnel_closed (ID: 02800038)

Default Severity	NOTICE
Log Message	Closed L2TP tunnel. Tunnel ID: <ctrlconnid>, Interface: <iface>.
Explanation	The L2TP tunnel with the specified tunnel ID has been closed.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters	iface ctrlconnid

2.39.21. l2tp_session_request (ID: 02800045)

Default Severity	NOTICE
Log Message	L2TP session request received. Control Connection ID: <ctrlconnid>
Explanation	A new session request was received on the specified tunnel.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ctrlconnid

2.39.22. l2tp_session_up (ID: 02800046)

Default Severity	NOTICE
Log Message	L2TP session up. Control Connection ID: <ctrlconnid>, Session ID: <sessionid>
Explanation	The L2TP session negotiation has completed successfully.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ctrlconnid sessionid

2.39.23. l2tp_session_up (ID: 02800047)

Default Severity	NOTICE
Log Message	L2TP session up. Control Connection ID: <ctrlconnid>, Session ID: <sessionid>
Explanation	The L2TP session negotiation has completed successfully.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ctrlconnid sessionid

2.39.24. waiting_for_ip_to_listen_on (ID: 02800050)

Default Severity	NOTICE
Log Message	L2TP server <iface> cannot start until it has an IP address to listen on
Explanation	The L2TP server cannot start until the L2TP interface has a proper IP address to listen on.
Firewall Action	None
Recommended Action	Make sure that the IP address is configured correctly on the L2TP server interface, or that the DHCP server can hand out a proper IP address to the interface.
Revision	1
Parameters	iface

2.39.25. no_session_found (ID: 02800060)

Default Severity	WARNING
Log Message	No session found for message sent from <remotegw> on tunnel <iface>.
Explanation	No session found for message received by the L2TP interface.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.40. LACP

These log messages refer to the **LACP (Link Aggregation Control Protocol)** category.

2.40.1. lacp_up (ID: 07700001)

Default Severity	INFORMATIONAL
Log Message	Negotiation was successful and <physiface> was added to the <laiface> aggregation.
Explanation	LACP has successfully negotiated with a partner system and the specified Member interface is now fully operational. This event is generated independently for each Member interface.
Firewall Action	include_link
Recommended Action	None.
Revision	1
Parameters	physiface laiface

2.40.2. lacp_expired (ID: 07700002)

Default Severity	NOTICE
Log Message	The partner system on <physiface> has timed out due to no message being received in <timeout> seconds.
Explanation	LACP has not received a periodic message from the established partner system in some time and the link has been excluded from the aggregation.
Firewall Action	exclude_link
Recommended Action	If this occurs frequently, look for an unstable link or partner system.
Revision	1
Parameters	physiface laiface timeout

2.40.3. lacp_down (ID: 07700003)

Default Severity	WARNING
Log Message	No response has been received on <physiface>. The link will not be used in the <laiface> aggregation.
Explanation	No LACP message has been received on the link.

Firewall Action exclude_link

Recommended Action Verify that the link is operational and connected to a properly configured LACP system.

Revision 1

Parameters physiface
laiface

2.40.4. lacp_partner_mismatch (ID: 07700004)

Default Severity ERROR

Log Message The information exchanged with the partner system on <physiface> does not match that of other configured Members of the <laiface> aggregation.

Explanation LACP has successfully exchanged information on several links but the exchanged information is not identical on all of those links. LACP has selected the best set of those links for aggregation and the rest have been excluded. This event is generated for each of the excluded links.

Firewall Action exclude_link

Recommended Action Verify that all configured Member interfaces are physically connected to the same properly configured system.

Revision 1

Parameters physiface
laiface

2.40.5. lacp_link_speed_mismatch (ID: 07700005)

Default Severity ERROR

Log Message <physiface> is not compatible with other Members of the <laiface> aggregation because they are not operating at the same link speed.

Explanation All of the configured Member interfaces are not operating at the same link speed. LACP has selected the best set of those links for aggregation and the rest have been excluded. This event is generated for each of the excluded links.

Firewall Action exclude_link

Recommended Action Look for hardware or configuration limitations that may be preventing the affected link from operating at the same link speed as the other configured Members.

Revision 1

Parameters physiface
laiface

2.40.6. lacp_link_down (ID: 07700006)

Default Severity	ERROR
Log Message	<physiface> appears to be down.
Explanation	.
Firewall Action	exclude_link
Recommended Action	.
Revision	1
Parameters	physiface laiface

2.40.7. lacp_disabled_half_duplex (ID: 07700007)

Default Severity	ERROR
Log Message	<physiface> has been disabled because it is operating at Half Duplex which is unsupported by the Link Aggregation feature.
Explanation	The specified interface has been disabled because it is operating at Half Duplex which is not supported by the Link Aggregation feature.
Firewall Action	exclude_link
Recommended Action	Look for hardware or configuration limitations that may be preventing the affected link from operating in Full Duplex mode.
Revision	1
Parameters	physiface laiface

2.41. LICENSE

These log messages refer to the **LICENSE (License)** category.

2.41.1. myD-Link_connection_succeeded (ID: 08400001)

Default Severity	NOTICE
Log Message	MyD-Link connection succeeded.
Explanation	None.
Firewall Action	none
Recommended Action	Activate and commit to apply the changes.
Revision	1

2.41.2. myD-Link_connection_failed (ID: 08400002)

Default Severity	NOTICE
Log Message	MyD-Link connection failed.
Explanation	None.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	message

2.41.3. myD-Link_connection_cleared (ID: 08400003)

Default Severity	NOTICE
Log Message	MyD-Link connection has been cleared.
Explanation	MyD-Link connection has been removed from the configuration.
Firewall Action	none
Recommended Action	Activate and commit.
Revision	1

2.42. NATPOOL

These log messages refer to the **NATPOOL (Events related to NAT Pools)** category.

2.42.1. uninitialized_ippool (ID: 05600001)

Default Severity	ERROR
Log Message	NATPool <poolname> has not been initialized
Explanation	The NATPool is not initialized. This can happen if the NATPool contains no valid IP addresses. If the NATPool is configured to use an IPPool, no IP addresses have been received form the IPPool.
Firewall Action	drop
Recommended Action	If the NATPool is configured to use an IPPool, verify that addresses have been loaded from IPPool.
Revision	1
Parameters	poolname

2.42.2. removed_translation_address (ID: 05600002)

Default Severity	WARNING
Log Message	Translation IP address <address> does no longer exist in NATPool <poolname>
Explanation	The translation IP has been removed by a configuration change. The connection is no longer valid and will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	address poolname

2.42.3. reconf_state_violation (ID: 05600003)

Default Severity	NOTICE
Log Message	State violation during re-mapping to STATFUL NATPool <poolname>.
Explanation	The NATPool's configuration has changed to STATEFUL. This connection's translation IP violates the stateful NATPool. Connection will remain open but will no longer be attached to this NATPool.
Firewall Action	decouple

Recommended Action	None.
Revision	1
Parameters	address poolname
Context Parameters	Connection

2.42.4. out_of_memory (ID: 05600005)

Default Severity	ERROR
Log Message	Out of memory while allocating NATPool state for <poolname>
Explanation	A state could not be allocated since the unit is out of memory.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	poolname

2.42.5. dhcp_address_expired (ID: 05600006)

Default Severity	WARNING
Log Message	NATPool DHCP address <address> lease expired
Explanation	The IP Address used by this NATPool have expired and may not be used any more. The connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	address poolname
Context Parameters	Connection

2.42.6. out_of_memory (ID: 05600007)

Default Severity	ERROR
Log Message	Out of memory while allocating NATPool IP entry for <poolname>
Explanation	An IP entry could not be allocated since the unit is out of memory.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	poolname

2.42.7. proxyarp_failed (ID: 05600008)

Default Severity	ERROR
Log Message	Could not add dynamic ProxyARP route. NATPool <poolname>
Explanation	It was not possible to dynamically add a core route for the given IP address.
Firewall Action	None
Recommended Action	Try to configure a core route with ProxyARP manually.
Revision	1
Parameters	poolname ip

2.42.8. max_states_reached (ID: 05600009)

Default Severity	WARNING
Log Message	Maximum amount of states <num_states> have been reached for NATPool <poolname>. Replacing lingering state <replacedip>
Explanation	The maximum configured number of states for this NAT Pool have been reached. NATPool subsystem will try to replace the oldest lingering state.
Firewall Action	replace_lingering
Recommended Action	Increase the MAXSTATES variable for this NATPool if more concurrent states are wanted.
Revision	1
Parameters	poolname num_states replacedip

2.42.9. max_states_reached (ID: 05600010)

Default Severity	WARNING
Log Message	Maximum amount of states <num_states> have been reached for NATPool <poolname>. Replacing active state <replacedip>
Explanation	The maximum configured number of states for this NAT Pool have

	been reached. NATPool subsystem must replace an active state since no lingering states exist.
Firewall Action	replace_active
Recommended Action	Increase the MAXSTATES variable for this NATPool if more concurrent states are wanted.
Revision	1
Parameters	poolname num_states replacedip

2.42.10. registerip_failed (ID: 05600011)

Default Severity	WARNING
Log Message	Request to activate already active Translation IP address <ip> in pool <poolname>
Explanation	Attempt to activate an already active Translation IP.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	poolname ip

2.42.11. registerip_failed (ID: 05600012)

Default Severity	WARNING
Log Message	Too many Translation IP addresses requested for <poolname>
Explanation	To many Translation IP addresses was requested for NAT Pool. Dropping this address.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	poolname

2.42.12. dynamicip_failed (ID: 05600013)

Default Severity	ERROR
Log Message	Failed to fetch new Translation IP address from IP Pool <poolname>

Explanation	Failed to fetch new Translation IP address from IP Pool.
Firewall Action	None
Recommended Action	Check configuration for NAT Pool and IP Pool.
Revision	1
Parameters	poolname

2.42.13. synchronization_failed (ID: 05600014)

Default Severity	ERROR
Log Message	Failed to synchronize Translation IP address to peer
Explanation	Failed to synchronize Translation IP address to peer.
Firewall Action	None
Recommended Action	Check status of peer and verify High Availability configuration.
Revision	1

2.42.14. registerip_failed (ID: 05600015)

Default Severity	WARNING
Log Message	Invalid synchronized translated connection receivedRequest to activate already active Translation IP address <ip> in pool <poolname>
Explanation	Attempt to activate an already active Translation IP.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	poolname ip

2.43. OSPF

These log messages refer to the **OSPF (OSPF events)** category.

2.43.1. internal_error (ID: 02400001)

Default Severity	WARNING
Log Message	Internal Error. Iface <iface> got IEvent <ievent> in IState <istate>. Ignored
Explanation	Internal error in the OSPF interface state engine.
Firewall Action	ignore
Recommended Action	Contact support.
Revision	1
Parameters	iface ievent istate
Context Parameters	Rule Name

2.43.2. internal_error (ID: 02400002)

Default Severity	WARNING
Log Message	Internal Error. Iface <iface> got NEvent <nevent> in NState <nstate>. Ignored
Explanation	Internal error in the OSPF interface neighbor state engine.
Firewall Action	ignore
Recommended Action	Contact support.
Revision	1
Parameters	iface nevent nstate
Context Parameters	Rule Name

2.43.3. unable_to_map_ptp_neighbor (ID: 02400003)

Default Severity	WARNING
Log Message	Unable to map PTP neighbor <neighborid> to my ip <myifaceip> at HA failover
Explanation	Unable to map a configured PTP neighbor to the local IP at HA

	failover.
Firewall Action	None
Recommended Action	Check OSPF interface configuration.
Revision	1
Parameters	iface neighborid myifaceip
Context Parameters	Rule Name

2.43.4. bad_packet_len (ID: 02400004)

Default Severity	WARNING
Log Message	Received OSPF packet with bad length
Explanation	Received OSPF packet with a bad length.
Firewall Action	drop
Recommended Action	Check the configuration on the neighboring router.
Revision	1
Parameters	ospflen iplen type
Context Parameters	Rule Name Packet Buffer

2.43.5. bad_ospf_version (ID: 02400005)

Default Severity	WARNING
Log Message	Packet OSPF version is not 2
Explanation	Received OSPF packet with other version then 2.
Firewall Action	drop
Recommended Action	Make sure that all routers are using version 2.
Revision	1
Parameters	ver
Context Parameters	Rule Name Packet Buffer

2.43.6. sender_not_in_iface_range (ID: 02400006)

Default Severity	WARNING
Log Message	Sender source <srcip> not within interface range (<ifacerange>)
Explanation	Received OSPF data from a neighboring router not within the receive interface range.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routes are on the same network.
Revision	1
Parameters	srcip ifacerange
Context Parameters	Rule Name Packet Buffer

2.43.7. area_mismatch (ID: 02400007)

Default Severity	WARNING
Log Message	Bad area <area>
Explanation	Received OSPF data from a neighboring router not within the same area as the receive interface.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routers are in the same area as the attaching interfaces.
Revision	1
Parameters	area
Context Parameters	Rule Name Packet Buffer

2.43.8. hello_netmask_mismatch (ID: 02400008)

Default Severity	WARNING
Log Message	Hello netmask mismatch. Received was <recv_netmask>, mine is <my_netmask>. Dropping
Explanation	Received OSPF data from a neighboring router with different network netmask then the receive interface.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routers have the same netmask as the attaching interfaces.
Revision	1

Parameters	recv_netmask my_netmask
Context Parameters	Rule Name Packet Buffer

2.43.9. hello_interval_mismatch (ID: 02400009)

Default Severity	WARNING
Log Message	Hello interval mismatch. Received was <recv_interval>, mine is <my_interval>. Dropping
Explanation	Received OSPF data from a neighboring router with a mismatching hello interval.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same hello interval.
Revision	1
Parameters	recv_interval my_interval
Context Parameters	Rule Name Packet Buffer

2.43.10. hello_rtr_dead_mismatch (ID: 02400010)

Default Severity	WARNING
Log Message	Hello router dead interval mismatch. Received was <recv_rtrdead>, mine is <my_rtrdead>. Dropping
Explanation	Received OSPF data from a neighboring router with a mismatching router dead interval.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same router dead interval.
Revision	1
Parameters	recv_rtrdead my_rtrdead
Context Parameters	Rule Name Packet Buffer

2.43.11. hello_e_flag_mismatch (ID: 02400011)

Default Severity	WARNING
Log Message	Hello E-flag mismatch. Received was <recv_e_flag>, mine is <my_e_flag>. Dropping
Explanation	Received OSPF data from a neighboring router with mismatching E-flag (describes how AS-external-LSAs are flooded) configuration.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same E-flag configuration.
Revision	1
Parameters	recv_e_flag my_e_flag
Context Parameters	Rule Name Packet Buffer

2.43.12. hello_n_flag_mismatch (ID: 02400012)

Default Severity	WARNING
Log Message	Hello N-flag mismatch. Received was <recv_n_flag>, mine is <my_n_flag>. Dropping
Explanation	Received OSPF data from a neighboring router with mismatching N-flag (NSSA details) configuration.
Firewall Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same N-flag configuration.
Revision	1
Parameters	recv_n_flag my_n_flag
Context Parameters	Rule Name Packet Buffer

2.43.13. both_np_and_e_flag_set (ID: 02400013)

Default Severity	WARNING
Log Message	Hello N-flag and E-flag set. This is a illegal combination. Dropping
Explanation	Received OSPF data from a neighboring router which illegally have both the N and E-flag set.
Firewall Action	drop
Recommended Action	Check the configuration on the neighboring router.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.43.14. unknown_lsa_type (ID: 02400014)

Default Severity	WARNING
Log Message	Unknown LSA type <lsatype>. Dropping
Explanation	Received OSPF data from a neighbor which contained a unknown LSA.
Firewall Action	drop
Recommended Action	Check the configuration on the neighboring router.
Revision	1
Parameters	lsatype
Context Parameters	Rule Name Packet Buffer

2.43.15. auth_mismatch (ID: 02400050)

Default Severity	WARNING
Log Message	Authentication mismatch. Received was <recv_auth>, mine is <my_auth>
Explanation	Authentication mismatch with neighboring OSPF router.
Firewall Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same authentication.
Revision	1
Parameters	recv_auth my_auth
Context Parameters	Rule Name

2.43.16. bad_auth_password (ID: 02400051)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad password
Explanation	Authentication failed due to a bad password.

Firewall Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same password.
Revision	1
Context Parameters	Rule Name

2.43.17. bad_auth_crypto_key_id (ID: 02400052)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad crypto key id. Received was <recv_id>, mine is <my_id>
Explanation	Authentication failed due to a bad crypto key id.
Firewall Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same crypto key id.
Revision	1
Parameters	recv_id my_id
Context Parameters	Rule Name

2.43.18. bad_auth_crypto_seq_number (ID: 02400053)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad crypto sequence number. Received was <recv_seq>, expected atleast <my_seq>
Explanation	Authentication failed due to mismatching crypto sequence number.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	recv_seq my_seq
Context Parameters	Rule Name

2.43.19. bad_auth_crypto_digest (ID: 02400054)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad crypto digest

Explanation	Authentication failed due to bad crypto digest.
Firewall Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same crypto digest.
Revision	1
Context Parameters	Rule Name

2.43.20. checksum_mismatch (ID: 02400055)

Default Severity	WARNING
Log Message	Checksum mismatch. Received was <recv_chksum>, mine is <my_chksum>
Explanation	Received OSPF data from neighbor with mismatching checksum.
Firewall Action	drop
Recommended Action	Check network equipment for problems.
Revision	1
Parameters	recv_chksum my_chksum
Context Parameters	Rule Name

2.43.21. dd_mtu_exceeds_interface_mtu (ID: 02400100)

Default Severity	WARNING
Log Message	Neighbor <neighbor> MTU is too high. Received DD has MTU <dd_mtu>. Interface MTU is <iface_mtu>
Explanation	Received database description from neighbor with too high MTU.
Firewall Action	drop
Recommended Action	Lower the MTU on the neighboring OSPF router.
Revision	1
Parameters	neighbor dd_mtu iface_mtu
Context Parameters	Rule Name

2.43.22. m_ms_mismatch (ID: 02400101)

Default Severity	WARNING
Log Message	Neighbor <neighbor> M/MS mismatch. Restarting exchange
Explanation	Received indication that a neighbor got the M/MS (master/slave) role wrong.
Firewall Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.43.23. i_flag_misuse (ID: 02400102)

Default Severity	WARNING
Log Message	Neighbor <neighbor> misused the I-flag. Restarting exchange
Explanation	Neighbor misused the I-flag.
Firewall Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.43.24. opt_change (ID: 02400103)

Default Severity	WARNING
Log Message	Neighbor <neighbor> changed options during exchange. Restarting exchange
Explanation	Neighbor illegally changed options during the exchange phase.
Firewall Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.43.25. bad_seq_num (ID: 02400104)

Default Severity	WARNING
Log Message	Neighbor <neighbor> replied with a unexpected sequence number. Restarting exchange
Explanation	Received neighbor reply with a unexpected sequence number.
Firewall Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.43.26. non_dup_dd (ID: 02400105)

Default Severity	WARNING
Log Message	Neighbor <neighbor> sent a non dup DD from a higher state then exchange. Restarting exchange
Explanation	Received a non dup database descriptor from a neighbor in a higher state then exchange.
Firewall Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.43.27. as_ext_on_stub (ID: 02400106)

Default Severity	WARNING
Log Message	Neighbor <neighbor> implied AS-EXT on a stub area. Restarting exchange
Explanation	A neighbor illegally implied AS-EXT on a stub area.
Firewall Action	restart
Recommended Action	Check neighboring OSPF router configuration.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.43.28. unknown_lsa (ID: 02400107)

Default Severity	WARNING
Log Message	Neighbor <neighbor> implied unknown LSA (<lsa_type>). Restarting exchange
Explanation	A neighbor described an unknown LSA type.
Firewall Action	restart
Recommended Action	Check neighboring OSPF router configuration.
Revision	1
Parameters	neighbor lsa_type
Context Parameters	Rule Name

2.43.29. bad_lsa_sequencenumber (ID: 02400108)

Default Severity	WARNING
Log Message	Got LSA with bad sequence number <seqnum>. Restarting exchange
Explanation	Received a LSA with a bad sequence number.
Firewall Action	restart
Recommended Action	None.
Revision	1
Parameters	seqnum
Context Parameters	Rule Name

2.43.30. bad_lsa_maxage (ID: 02400109)

Default Severity	WARNING
Log Message	Got LSA with bad maxage (<maxage> > <def_maxage>). Restarting exchange
Explanation	Received a LSA with a bad maxage value.
Firewall Action	restart
Recommended Action	Check orginating router configuration.
Revision	1
Parameters	maxage

	def_maxage
Context Parameters	Rule Name

2.43.31. lsa_checksum_mismatch (ID: 02400150)

Default Severity	WARNING
Log Message	LSA checksum mismatch. LSA is discarded
Explanation	Received LSA with mismatching checksum.
Firewall Action	discard
Recommended Action	Check network equipment for problems.
Revision	1
Context Parameters	Rule Name

2.43.32. unknown_lsa_type (ID: 02400151)

Default Severity	WARNING
Log Message	Unknown LSA type (<lsa_type>). LSA is discarded
Explanation	Received LSA of unknown type.
Firewall Action	discard
Recommended Action	Check originating router configuration.
Revision	1
Parameters	lsa_type
Context Parameters	Rule Name

2.43.33. bad_lsa_sequencenumber (ID: 02400152)

Default Severity	WARNING
Log Message	Bad LSA sequence number (<seqnum>). LSA is discarded
Explanation	Received LSA with a bad sequence number.
Firewall Action	discard
Recommended Action	None.
Revision	1
Parameters	seqnum

Context Parameters	Rule Name

2.43.34. bad_lsa_maxage (ID: 02400153)

Default Severity	WARNING
Log Message	Bad LSA maxage (<maxage>). LSA is discarded
Explanation	Received LSA with a bad max age.
Firewall Action	discard
Recommended Action	None.
Revision	1
Parameters	maxage
Context Parameters	Rule Name

2.43.35. received_as_ext_on_stub (ID: 02400154)

Default Severity	WARNING
Log Message	Received AS-EXT LSA on stub. LSA is discarded
Explanation	Received AS external LSA which is illegal on a stub area.
Firewall Action	discard
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.43.36. received_selforg_for_unknown_lsa_type (ID: 02400155)

Default Severity	WARNING
Log Message	Received selforiginated LSA for unknown LSA <lsatype> type? Flushing
Explanation	Received selforiginated LSA of unknown type.
Firewall Action	flush
Recommended Action	None.
Revision	1
Parameters	lsatype

Context Parameters	Rule Name

2.43.37. db_copy_more_recent_then_received (ID: 02400156)

Default Severity	WARNING
Log Message	Received LSA(LSA-<lsa> ID:<lsaid> AdvRtr:<lsartr>) is older then DB copy. Discarding received LSA
Explanation	Received LSA which is older then the copy in the database.
Firewall Action	discard
Recommended Action	None.
Revision	1
Parameters	lsa lsaid lsartr
Context Parameters	Rule Name

2.43.38. got_ack_mismatched_lsa (ID: 02400157)

Default Severity	WARNING
Log Message	Got ACK for mismatched LSA (LSA-<lsa> ID:<lsaid> AdvRtr:<lsartr>). ACK ingored
Explanation	Received acknowledge for mismatched LSA.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	lsa lsaid lsartr
Context Parameters	Rule Name

2.43.39. upd_packet_lsa_size_mismatch (ID: 02400158)

Default Severity	WARNING
Log Message	UPD packet LSA size mismatch. Parsing aborted
Explanation	Received OSPF UPD packet with a mismatching LSA size.
Firewall Action	abort

Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.43.40. req_packet_lsa_size_mismatch (ID: 02400159)

Default Severity	WARNING
Log Message	REQ packet LSA size mismatch. Parsing aborted
Explanation	Received OSPF REQ packet with a mismatching LSA size.
Firewall Action	abort
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.43.41. ack_packet_lsa_size_mismatch (ID: 02400160)

Default Severity	WARNING
Log Message	ACK packet LSA size mismatch. Parsing aborted
Explanation	Received OSPF ACK packet with a mismatching LSA size.
Firewall Action	abort
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.43.42. failed_to_create_replacement_lsa (ID: 02400161)

Default Severity	CRITICAL
Log Message	Failed to prepare replacement LSA (LSA- <lsa> ID:<lsaid> AdvRtr:<lsartr>)
Explanation	Failed to create LSA.
Firewall Action	alert
Recommended Action	Check memory consumption.

Revision	1
Parameters	lsa lsaid lsartr
Context Parameters	Rule Name

2.43.43. unable_to_send_ack (ID: 02400162)

Default Severity	CRITICAL
Log Message	Unable to send ACK
Explanation	Unable to send acknowledgement.
Firewall Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Rule Name

2.43.44. got_router_lsa_mismatched_fields (ID: 02400163)

Default Severity	WARNING
Log Message	Received Router LSA which contains mismatched Link State ID:(<lsaid>) and Advertising Router:(<lsartr>). LSA is discarded
Explanation	Received LSA of incompatible Link State ID and Advertising Router.
Firewall Action	discard
Recommended Action	None.
Revision	2
Parameters	lsaid lsartr
Context Parameters	Rule Name

2.43.45. unknown_neighbor (ID: 02400200)

Default Severity	WARNING
Log Message	Unknown neighbor(IP:<neighbor> ID:<neighborid>) seen on <iface>. Ignoring
Explanation	Unknown neighbor seen on PTP based interface.
Firewall Action	None

Recommended Action	Check for incorrectly configured neighbors.
Revision	1
Parameters	neighbor neighborid iface
Context Parameters	Rule Name

2.43.46. too_many_neighbors (ID: 02400201)

Default Severity	WARNING
Log Message	Too many neighbors on <iface>. Unable to maintain 2-way with all of them(hello packet)
Explanation	There are too many OSPF routers on a directly connected network.
Firewall Action	None
Recommended Action	Reduce the number of OSPF routers on the network.
Revision	1
Parameters	iface
Context Parameters	Rule Name

2.43.47. neighbor_died (ID: 02400202)

Default Severity	WARNING
Log Message	Neighbor <neighbor> on <neighboriface> died
Explanation	Lost connectivity with neighbor router.
Firewall Action	None
Recommended Action	Check neighbor status and connectivity.
Revision	1
Parameters	neighbor neighboriface
Context Parameters	Rule Name

2.43.48. unable_to_find_transport_area (ID: 02400300)

Default Severity	WARNING
Log Message	Unable to find transport area <area> for VLINK <vlink> when building router LSA. Iface skipped

Explanation	Unable to find transport area for a vlink.
Firewall Action	skip_iface
Recommended Action	Check OSPF area configuration.
Revision	1
Parameters	area vlink
Context Parameters	Rule Name

2.43.49. internal_error_unable_to_map_identifier (ID: 02400301)

Default Severity	WARNING
Log Message	Internal error: Unable to map a identifier for LSA Type:<lsatype> ID:<lsaid> AdvRouter:<lsaadvrtr>
Explanation	Unable to map an identifier for a LSA.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	lsatype lsaid lsaadvrtr
Context Parameters	Rule Name

2.43.50. lsa_size_too_big (ID: 02400302)

Default Severity	WARNING
Log Message	Requested LSA size(<lsasize>) too big. Unable to create LSA
Explanation	Unable to create LSA since the size is too big.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	lsasize
Context Parameters	Rule Name

2.43.51. memory_usage_exceeded_70_percent_of_max_allowed

(ID: 02400303)

Default Severity	WARNING
Log Message	Memory usage for OSPF process <ospfproc> have now exceeded 70 percent of the maximum allowed
Explanation	The memory usage for a OSPF process have exceeded 70 percent of the maximum allowed.
Firewall Action	None
Recommended Action	Check memory consumption.
Revision	1
Parameters	ospfproc
Context Parameters	Rule Name

2.43.52. memory_usage_exceeded_90_percent_of_max_allowed (ID: 02400304)

Default Severity	WARNING
Log Message	Memory usage for OSPF process <ospfproc> have now exceeded 90 percent of the maximum allowed
Explanation	The memory usage for a OSPF process have exceeded 70 percent of the maximum allowed.
Firewall Action	None
Recommended Action	Check memory consumption.
Revision	1
Parameters	ospfproc
Context Parameters	Rule Name

2.43.53. as_disabled_due_to_mem_alloc_fail (ID: 02400305)

Default Severity	CRITICAL
Log Message	AS disabled due to memory allocation failure
Explanation	An OSPF AS have been disabled due to memory allocation failure.
Firewall Action	alert
Recommended Action	Check memory consumption.
Revision	1

Context Parameters	Rule Name

2.43.54. internal_lsa_chksum_error (ID: 02400306)

Default Severity	CRITICAL
Log Message	LSA internal checksum error
Explanation	Internal LSA checksum error.
Firewall Action	alert
Recommended Action	Check hardware for defects.
Revision	1
Context Parameters	Rule Name

2.43.55. unable_to_find_iface_to_stub_net (ID: 02400400)

Default Severity	WARNING
Log Message	Internal error: Unable to find my interface attached to stub network <stub>
Explanation	Unable to find local interface attached to stub network.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	stub
Context Parameters	Rule Name

2.43.56. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400401)

Default Severity	WARNING
Log Message	Internal error: Unable to find my link connecting to described LSA (NetVtxId: <netvtxid>)
Explanation	Unable to find local link to described LSA.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1

Parameters	netvtxid
Context Parameters	Rule Name

2.43.57. internal_error_unable_to_find_iface_connecting_to_lsa (ID: 02400402)

Default Severity	WARNING
Log Message	Internal error: Unable to find my interface connecting to described LSA (NetVtxId: <netvtxid>)
Explanation	Unable to find local interface connecting to described LSA.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	netvtxid
Context Parameters	Rule Name

2.43.58. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400403)

Default Severity	WARNING
Log Message	Internal error: Unable to find my link connecting to described LSA (RtrVtxId: <rtrvtxid>)
Explanation	Unable to find local link connecting to described LSA.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	rtrvtxid
Context Parameters	Rule Name

2.43.59. internal_error_unable_to_find_iface_connecting_to_lsa (ID: 02400404)

Default Severity	WARNING
Log Message	Internal error: Unable to find my interface connecting to described LSA (RtrVtxId: <rtrvtxid>)

Explanation	Unable to find local interface connecting to descried LSA.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	rtrvtxid
Context Parameters	Rule Name

2.43.60. internal_error_unable_neighbor_iface_attached_back_to_me (ID: 02400405)

Default Severity	WARNING
Log Message	Internal error: Unable to find neighbor (RtrVtxId: <rtrvtxid>) interface attached back to me
Explanation	Unable to find neighbor interface attached back.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	rtrvtxid
Context Parameters	Rule Name

2.43.61. bad_iface_type_mapping_rtr_to_rtr_link (ID: 02400406)

Default Severity	WARNING
Log Message	Internal error: Bad interface type (<ifacetype>) when mapping rtr-to-rtr (RtrVtxId:<rtrvtxid>)
Explanation	Bad interface type found when doing router-to-router mapping.
Firewall Action	None
Recommended Action	Check OSPF interface configuration.
Revision	1
Parameters	ifacetype rtrvtxid
Context Parameters	Rule Name

2.43.62. internal_error_unable_to_find_lnk_connecting_to_lsa

(ID: 02400407)

Default Severity	WARNING
Log Message	Internal error: Unable to find my link connecting to described LSA (NetVtxId:<netvtxid>)
Explanation	Unable to find local link connected to described LSA.
Firewall Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	netvtxid
Context Parameters	Rule Name

2.43.63. memory_allocation_failure (ID: 02400500)

Default Severity	CRITICAL
Log Message	Internal Error: Memory allocation failure! OSPF process now considered inconsistent
Explanation	Memory allocation failure.
Firewall Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Rule Name

2.43.64. unable_to_send (ID: 02400501)

Default Severity	CRITICAL
Log Message	Internal Error: Unable to send (No sendbuffer?)
Explanation	Unable to get buffer for sending.
Firewall Action	alert
Recommended Action	Check buffer consumption.
Revision	1
Context Parameters	Rule Name

2.43.65. failed_to_add_route (ID: 02400502)

Default Severity	CRITICAL
Log Message	Failed to add route <route>! OSPF process should now be considered inconsistent
Explanation	Unable to add route.
Firewall Action	alert
Recommended Action	Check memory consumption.
Revision	1
Parameters	route
Context Parameters	Rule Name

2.44. PPP

These log messages refer to the **PPP (PPP tunnel events)** category.

2.44.1. ip_pool_empty (ID: 02500001)

Default Severity	WARNING
Log Message	IPCP can not assign IP address to peer because the IP address pool is empty
Explanation	IPCP can not assign an IP address to the peer because there are no free IP addresses in IP address pool.
Firewall Action	failed_ipcp_address_assignment
Recommended Action	Increase the number of IP addresses in the IP address pool to allow all connecting clients to be assigned a unique IP address.
Revision	1
Parameters	tunnel_type

2.44.2. ip_address_required_but_not_received (ID: 02500002)

Default Severity	WARNING
Log Message	IP address required but not received. PPP terminated
Explanation	Peer refuses to give out an IP address. Since an IP address lease is required, PPP is terminated.
Firewall Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.3. primary_dns_address_required_but_not_received (ID: 02500003)

Default Severity	WARNING
Log Message	Primary DNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a primary DNS address. Since reception of a primary DNS address is required, PPP is terminated.
Firewall Action	ppp_terminated
Recommended Action	None.

Revision	1
Parameters	tunnel_type

2.44.4. seconday_dns_address_required_but_not_received (ID: 02500004)

Default Severity	WARNING
Log Message	Secondary DNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a secondary DNS address. Since reception of a secondary DNS address is required, PPP is terminated.
Firewall Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.5. primary_nbns_address_required_but_not_received (ID: 02500005)

Default Severity	WARNING
Log Message	Primary NBNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a primary NBNS address. Since reception of a primary NBNS address is required, PPP is terminated.
Firewall Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.6. seconday_nbns_address_required_but_not_received (ID: 02500006)

Default Severity	WARNING
Log Message	Secondary NBNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a secondary NBNS address. Since reception of a secondary NBNS address is required, PPP is terminated.
Firewall Action	ppp_terminated

Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.7. failed_to_agree_on_authentication_protocol (ID: 02500050)

Default Severity	ERROR
Log Message	Failed to agree on authentication protocol. PPP terminated
Explanation	Failed to agree on PPP authentication protocol. PPP is terminated.
Firewall Action	ppp_terminated
Recommended Action	Review the allowed authentication protocols configured. The client and server must be configured to have at least one authentication protocol in common.
Revision	1
Parameters	tunnel_type

2.44.8. peer_refuses_to_use_authentication (ID: 02500051)

Default Severity	ERROR
Log Message	Peer refuses to use authentication. PPP terminated
Explanation	Peer refuses to use any authentication at all. PPP is terminated since we demand authentication.
Firewall Action	ppp_terminated
Recommended Action	Review the allowed authentication types configured. The client and server must be configured to have at least one authentication type in common.
Revision	1
Parameters	tunnel_type

2.44.9. lcp_negotiation_stalled (ID: 02500052)

Default Severity	ERROR
Log Message	LCP negotiation stalled. PPP terminated
Explanation	PPP LCP negotiation stalled. Terminating PPP since the peer persistently demands the use of an LCP option that is unsupported.

Firewall Action	ppp_terminated
Recommended Action	Try to reconfigure the peer so it does not demand the use of this LCP option.
Revision	1
Parameters	tunnel_type unsupported_lcp_option

2.44.10. ppp_tunnel_limit_exceeded (ID: 02500100)

Default Severity	ALERT
Log Message	PPP Tunnel license limit exceeded. PPP terminated
Explanation	PPP is terminated because the license restrictions do not allow any more PPP tunnels. No new PPP tunnels can be established until an existing one is closed.
Firewall Action	ppp_terminated
Recommended Action	Upgrade your license to allow more simultaneous PPP tunnels.
Revision	1
Parameters	tunnel_type limit

2.44.11. authentication_failed (ID: 02500101)

Default Severity	WARNING
Log Message	Authentication failed. PPP terminated
Explanation	Authentication failed. PPP terminated.
Firewall Action	ppp_terminated
Recommended Action	Make sure that the right username and password is used.
Revision	1
Parameters	tunnel_type user

2.44.12. response_value_too_long (ID: 02500150)

Default Severity	WARNING
Log Message	PPP CHAP response value was truncated because it was too long
Explanation	PPP CHAP response value was truncated because it was too long.

Firewall Action	chap_response_value_truncated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.13. username_too_long (ID: 02500151)

Default Severity	WARNING
Log Message	PPP CHAP username was truncated because it was too long
Explanation	PPP CHAP username was truncated because it was too long.
Firewall Action	chap_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.44.14. username_too_long (ID: 02500201)

Default Severity	WARNING
Log Message	PPP MSCHAPv1 username was truncated because it was too long
Explanation	PPP MSCHAPv1 username was truncated because it was too long.
Firewall Action	mschapv1_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.44.15. username_too_long (ID: 02500301)

Default Severity	WARNING
Log Message	PPP MSCHAPv2 username was truncated because it was too long
Explanation	PPP MSCHAPv2 username was truncated because it was too long.
Firewall Action	mschapv2_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1

Parameters	tunnel_type

2.44.16. username_too_long (ID: 02500350)

Default Severity	WARNING
Log Message	PPP PAP username was truncated because it was too long
Explanation	PPP PAP username was truncated because it was too long.
Firewall Action	pap_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.44.17. password_too_long (ID: 02500351)

Default Severity	WARNING
Log Message	PPP PAP password was truncated because it was too long
Explanation	PPP PAP password was truncated because it was too long.
Firewall Action	pap_password_truncated
Recommended Action	Reconfigure the endpoints to use a shorter password.
Revision	1
Parameters	tunnel_type

2.44.18. one_time_password_too_long (ID: 02500352)

Default Severity	WARNING
Log Message	PPP PAP one time password was truncated because it was too long
Explanation	PPP PAP one time password was truncated because it was too long.
Firewall Action	pap_one_time_password_truncated
Recommended Action	Reconfigure the endpoints to use a shorter one time password.
Revision	1
Parameters	tunnel_type

2.44.19. radius_state_id_too_long (ID: 02500353)

Default Severity	WARNING
Log Message	PPP PAP Radius state ID was truncated because it was too long
Explanation	PPP PAP Radius state ID was truncated because it was too long.
Firewall Action	pap_radius_state_id_truncated
Recommended Action	Reconfigure the endpoints to use a shorter Radius state ID.
Revision	1
Parameters	tunnel_type

2.44.20. unsupported_auth_server (ID: 02500500)

Default Severity	ERROR
Log Message	Unsupported authentication server. PPP Authentication terminated
Explanation	Unsupported authentication server. PPP Authentication terminated.
Firewall Action	authentication_terminated
Recommended Action	Review the authentication server configuration.
Revision	1
Parameters	tunnel_type

2.44.21. radius_error (ID: 02500501)

Default Severity	ERROR
Log Message	Radius server authentication error. PPP Authentication terminated
Explanation	There was an error while authenticating using a radius server. PPP Authentication terminated.
Firewall Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.22. authdb_error (ID: 02500502)

Default Severity	ERROR
Log Message	Local database authentication error. PPP Authentication terminated

Explanation	There was an error while authenticating using a local user database. PPP Authentication terminated.
Firewall Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.23. ldap_error (ID: 02500503)

Default Severity	ERROR
Log Message	LDAP server authentication error. PPP Authentication terminated
Explanation	There was an error while authenticating using a LDAP server. PPP Authentication terminated.
Firewall Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.44.24. MPPE_decrypt_fail (ID: 02500600)

Default Severity	ERROR
Log Message	MPPE decryption resulted in the unsupported protocol <protocol>. Terminating PPP
Explanation	MPPE decryption resulted in an unsupported protocol. IP is the only protocol supported. This either means that the decryption failed or that the peer actually sent data using an unsupported protocol. PPP is terminated.
Firewall Action	ppp_terminated
Recommended Action	Reconnect the tunnel. If the peer keeps sending the same unsupported protocol, try to reconfigure the peer to only send IP packets through the tunnel.
Revision	1
Parameters	protocol

2.45. PPPOE

These log messages refer to the **PPPOE (PPPoE tunnel events)** category.

2.45.1. pppoe_tunnel_up (ID: 02600001)

Default Severity	NOTICE
Log Message	PPPoE tunnel on <iface> established to <pppoeserver>. Auth: <auth>, IfaceIP: <ifaceip>, Downtime: <downtime>
Explanation	The PPPoE tunnel for the interface have been established. .
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface pppoeserver auth ifaceip downtime

2.45.2. pppoe_tunnel_closed (ID: 02600002)

Default Severity	NOTICE
Log Message	PPPoE tunnel on <iface> to <pppoeserver> closed. Uptime: <uptime>
Explanation	The PPPoE tunnel for the interface have been closed. .
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface pppoeserver uptime

2.46. PPTP

These log messages refer to the **PPTP (PPTP tunnel events)** category.

2.46.1. pptpclient_resolve_successful (ID: 02700001)

Default Severity	NOTICE
Log Message	PPTP client <iface> resolved <remotegwname> to <remotegw>
Explanation	The PPTP client succesfully resolved the DNS name of remote gateway.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.46.2. pptpclient_resolve_failed (ID: 02700002)

Default Severity	WARNING
Log Message	PPTP client <iface> failed to resolve <remotegwname>
Explanation	The PPTP client failed to resolve the DNS name of the remote gateway.
Firewall Action	None
Recommended Action	Make sure you have configured the DNS name of the remote gateway and the DNS servers correctly.
Revision	1
Parameters	iface remotegwname

2.46.3. pptp_connection_disallowed (ID: 02700003)

Default Severity	WARNING
Log Message	PPTP connection from <remotegw> disallowed according to rule <rule>! Call ID: <callid>
Explanation	The PPTP connection is disallowed by the new configuration according to the specified userauth rule. Closing down the PPTP connection.
Firewall Action	pptp_connection_closed

Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule remotegw callid

2.46.4. unknown_pptp_auth_source (ID: 02700004)

Default Severity	WARNING
Log Message	Unknown PPTP authentication source for <rule>! Remote gateway: <remotegw>, Call ID: <callid>
Explanation	The authentication source for the specified userauth rule found in the new configuration is unknown to the PPTP server. Closing down the PPTP connection.
Firewall Action	pptp_connection_closed
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule remotegw callid

2.46.5. user_disconnected (ID: 02700005)

Default Severity	WARNING
Log Message	User <user> is forcibly disconnected. Call ID: <callid> Remote gateway: <remotegw>
Explanation	The connected client is forcibly disconnected by the userauth system.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	user callid remotegw

2.46.6. only_routes_set_up_by_server_iface_allowed (ID: 02700006)

Default Severity	WARNING

Log Message	PPTP server <iface> received a packet routed by a route not set up by the interface itself. Dropping packet.
Explanation	The PPTP server interface received a packet that was routed to the interface by a route that was either manually configured or set up by another subsystem. Traffic can only be sent out on the PPTP server using the dynamic routes set up by the interface itself.
Firewall Action	drop
Recommended Action	Make sure there are no manually configured routes pointing to the PPTP server interface in the configuration.
Revision	1
Parameters	iface

2.46.7. mppe_required (ID: 02700007)

Default Severity	WARNING
Log Message	MPPE failed but is required, closing session <callid> to <remotegw> on <iface>.
Explanation	MPPE is required by the configuration but the MPPE negotiation failed. Session will be closed.
Firewall Action	close_session
Recommended Action	Make sure the peer is capable of MPPE encryption, or disable the MPPE requirement.
Revision	1
Parameters	iface remotegw callid

2.46.8. pptp_session_closed (ID: 02700008)

Default Severity	NOTICE
Log Message	PPTP session <callid> to <remotegw> on <iface> closed.
Explanation	A PPTP session has been closed. The specified interface, remote gateway and call ID identify the specific session.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw callid

2.46.9. pptp_session_request (ID: 02700009)

Default Severity	NOTICE
Log Message	PPTP session request sent on control connection to <remotegw>
Explanation	An PPTP session request has been sent on the control connection to the specified remote gateway.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	remotegw

2.46.10. unsupported_message (ID: 02700010)

Default Severity	WARNING
Log Message	Unsupported message type <type> received on session <callid> from <remotegw>. Ignoring message.
Explanation	A message with unsupported type received. Ignoring it. The specified interface, remote gateway and call ID identify the specific session.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	iface type callid remotegw

2.46.11. failure_init_radius_accounting (ID: 02700011)

Default Severity	WARNING
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accouting will be disabled. Interface: <iface>, Remote gateway: <remotegw>, Call ID: <callid>
Explanation	Failed to send START message to RADIUS accounting server. RADIUS accounting will be disabled for this session. The specified interface, remote gateway and call ID identify the specific session.
Firewall Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.

Revision	1
Parameters	callid remotegw iface

2.46.12. pptp_session_up (ID: 02700012)

Default Severity	WARNING
Log Message	PPP negotiation completed for session <callid> to <remotegw> on <iface>. User: <user>, Auth: <auth>, MPPE: <mppe>, Assigned IP: <assigned_ip>
Explanation	The PPP negotiation has completed successfully for this session. The specified interface, remote gateway and call ID identify the specific session.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	callid iface remotegw user auth mppe assigned_ip

2.46.13. pptp_session_up (ID: 02700013)

Default Severity	WARNING
Log Message	PPP negotiation completed for session <callid> on <iface> connected to <remotegw>. Auth: <auth>, MPPE: <mppe>
Explanation	The PPP negotiation has completed successfully for this session. The specified interface, remote gateway and call ID identify the specific session.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	callid iface remotegw auth mppe

2.46.14. tunnel_idle_timeout (ID: 02700014)

Default Severity	WARNING
Log Message	PPTP tunnel to <remotegw> on <iface> has been idle for too long. Closing it.
Explanation	A PPTP tunnel has been idle for too long. Tunnel will be closed.
Firewall Action	close_tunnel
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.46.15. session_idle_timeout (ID: 02700015)

Default Severity	WARNING
Log Message	PPTP session <callid> to <remotegw> on <iface> has been idle for too long. Closing it.
Explanation	A PPTP session has been idle for too long. Session will be closed.
Firewall Action	close_session
Recommended Action	None.
Revision	1
Parameters	iface remotegw callid

2.46.16. pptpclient_start (ID: 02700017)

Default Severity	NOTICE
Log Message	PPTP client <iface> started, connecting to server on <remotegw>
Explanation	A PPTP client has initiated the connection to its remote gateway.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.46.17. pptpclient_connected (ID: 02700018)

Default Severity	NOTICE
Log Message	PPTP client <iface> connected to <remotegw>, requesting control connection
Explanation	A PPTP client has established a connection to its remote gateway and is sending a control connection request message.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.46.18. pptp_tunnel_up (ID: 02700019)

Default Severity	NOTICE
Log Message	PPTP tunnel up, client <remotegw> connected to <iface>
Explanation	A remote PPTP client has established a connection to this PPTP server.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.46.19. ctrlconn_refused (ID: 02700020)

Default Severity	WARNING
Log Message	The remote PPTP server on <remotegw> refused to establish PPTP control connection. Reason: <reason>
Explanation	A remote PPTP server refused to establish PPTP control connection.
Firewall Action	None
Recommended Action	Read the reason specified by the PPTP server. This might give a clue why the PPTP server refused the PPTP control connection.
Revision	1
Parameters	reason

iface
remotegw

2.46.20. pptp_tunnel_up (ID: 02700021)

Default Severity	NOTICE
Log Message	PPTP tunnel on <iface> is up. Connected to server on <remotegw>.
Explanation	This PPTP client has established a control connection to the remote PPTP server.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.46.21. pptp_tunnel_closed (ID: 02700022)

Default Severity	NOTICE
Log Message	PPTP tunnel to <remotegw> on <iface> closed.
Explanation	The PPTP tunnel to has been closed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.46.22. pptp_connection_disallowed (ID: 02700024)

Default Severity	WARNING
Log Message	PPTP connection from <remotegw> disallowed according to rule <rule>. Interface: <iface>.
Explanation	The PPTP connection is disallowed according to the specified userauth rule.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1

Parameters rule
iface
remotegw

2.46.23. unknown_pptp_auth_source (ID: 02700025)

Default Severity WARNING

Log Message Unknown PPTP authentication source for <rule>!. Interface: <iface>, Remote gateway: <remotegw>.

Explanation The authentication source for the specified userauth rule is unknown to the PPTP server.

Firewall Action None

Recommended Action Make sure the userauth rules are configured correctly.

Revision 1

Parameters rule
iface
remotegw

2.46.24. pptp_no_userauth_rule_found (ID: 02700026)

Default Severity WARNING

Log Message Did not find a matching userauth rule for the incoming PPTP connection. Interface: <iface>, Remote gateway: <remotegw>.

Explanation The PPTP server was unsuccessful trying to find a userauth rule matching the incoming PPTP connection.

Firewall Action None

Recommended Action Make sure the userauth rules are configured correctly.

Revision 1

Parameters iface
remotegw

2.46.25. malformed_packet (ID: 02700027)

Default Severity WARNING

Log Message Malformed packet received from <remotegw> on <iface>. Error code: <error_code>

Explanation A malformed packet was received by the PPTP interface.

Firewall Action None

Recommended Action	None.
Revision	1
Parameters	iface remotegw error_code

2.46.26. waiting_for_ip_to_listen_on (ID: 02700050)

Default Severity	WARNING
Log Message	PPTP server <iface> cannot start until it has an IP address to listen on.
Explanation	The PPTP server cannot start until it has a proper IP address to listen on.
Firewall Action	None
Recommended Action	Make sure that the IP address is configured correctly on the PPTP server interface. If the PPTP server is supposed to listen on an IP assigned by a DHCP server, make sure that the DHCP server is working properly.
Revision	1
Parameters	iface

2.47. RADIUSRELAY

These log messages refer to the **RADIUSRELAY (RADIUS relay)** category.

2.47.1. malformed_packet (ID: 07500001)

Default Severity	WARNING
Log Message	Malformed packet received.
Explanation	A malformed packet was received.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	username imsi mac iface

2.47.2. user_reauthenticated (ID: 07500002)

Default Severity	NOTICE
Log Message	User <username> was reauthenticated.
Explanation	A user was re-authenticated.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	username imsi mac iface ip

2.47.3. user_authenticated (ID: 07500003)

Default Severity	NOTICE
Log Message	User <username> was authenticated.
Explanation	A user was authenticated.
Firewall Action	None
Recommended Action	None.

Revision 1

Parameters username
imsi
mac
iface
ip
calledstationid

2.47.4. user_removed_timeout (ID: 07500004)

Default Severity NOTICE

Log Message User <username> was removed due to timeout.

Explanation A user was removed because a timeout was reached.

Firewall Action None

Recommended Action None.

Revision 1

Parameters username
imsi
mac
iface
ip

2.47.5. user_authentication_rejected (ID: 07500005)

Default Severity NOTICE

Log Message User <username> authentication was rejected

Explanation A user authentication was rejected.

Firewall Action None

Recommended Action None.

Revision 1

Parameters username
imsi
mac
iface
calledstationid

2.47.6. user_logged_out (ID: 07500006)

Default Severity NOTICE

Log Message	User <username> was logged out.
Explanation	A user was logged out.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	username imsi mac iface ip

2.47.7. login_from_same_mac (ID: 07500007)

Default Severity	NOTICE
Log Message	User <newusername> is logging from in the same MAC address as <username>, logging out current user.
Explanation	A user is logging in from the same MAC address as an already authenticated user. The current user will be logged out.
Firewall Action	logout_current_user
Recommended Action	None.
Revision	1
Parameters	username imsi mac iface ip newusername

2.47.8. create_server_session_failed (ID: 07500009)

Default Severity	CRITICAL
Log Message	Failed to create server session for <name> on <ip>:<port> on interface <iface>.
Explanation	It was not possible to start a session for listening for RADIUS traffic.
Firewall Action	none
Recommended Action	Check configuration.
Revision	1
Parameters	name iface

ip
port

2.47.9. login_from_new_mac (ID: 07500010)

Default Severity	NOTICE
Log Message	User <username> is logging in from another MAC address, logging out current user.
Explanation	An already authenticated user is logging in from a new MAC address than before. The current user instance will be logged out.
Firewall Action	logout_current_user
Recommended Action	None.
Revision	1
Parameters	username imsi mac iface ip newmac

2.48. REALTIMEMONITOR

These log messages refer to the **REALTIMEMONITOR (Real-time monitor events)** category.

Note

The log message IDs in this category are assigned dynamically based on the realtime monitor configuration. The variable part of the ID (indicated by x below) corresponds to the assigned ID of the realtime monitor rule that triggered, e.g. assigned ID 1 results in log message ID 05400001 and assigned ID 12 becomes log message ID 05400012.

2.48.1. value_above_high_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Firewall Monitoring. Current uptime: <uptime>. The value of: <name> is above the high threshold High threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	High threshold passed.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	uptime name threshold numbersamples currentvalue

2.48.2. value_below_low_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Firewall Monitoring. Current uptime: <uptime>. The value of: <name> is below the low threshold Low threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	Low threshold passed.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	uptime name threshold numbersamples currentvalue

2.48.3. value_below_high_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Firewall Monitoring. Current uptime: <uptime>. The value of: <name> is now bellow the high threshold Low threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	Low threshold passed.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	uptime name threshold numbersamples currentvalue

2.48.4. value_above_low_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Firewall Monitoring. Current uptime: <uptime>. The value of: <name> is above the low threshold Low threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	Low threshold passed.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	uptime name threshold numbersamples currentvalue

2.49. REASSEMBLY

These log messages refer to the **REASSEMBLY (Events concerning data reassembly)** category.

2.49.1. ack_of_not_transmitted_data (ID: 04800002)

Default Severity	INFORMATIONAL
Log Message	TCP segment acknowledges data not yet transmitted
Explanation	A TCP segment that acknowledges data not yet transmitted was received. The segment will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Connection

2.49.2. invalid_tcp_checksum (ID: 04800003)

Default Severity	NOTICE
Log Message	TCP segment with invalid checksum
Explanation	A TCP segment with an invalid checksum was received. The segment will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Connection

2.49.3. mismatching_data_in_overlapping_tcp_segment (ID: 04800004)

Default Severity	ERROR
Log Message	Overlapping TCP segment containing different data
Explanation	A TCP segment that partly overlaps segments that has been received earlier was received. The data in the overlapping part is however different from the data in the segments received earlier. The segment's data will be replaced so that it is consistent with the earlier received segments.
Firewall Action	correct the data

Recommended Action	Research the source of this errornous traffic.
Revision	1
Context Parameters	Connection

2.49.4. memory_allocation_failure (ID: 04800005)

Default Severity	ERROR
Log Message	Can't allocate memory to keep track of a packet
Explanation	The firewall is unable to allocate memory to keep track of packet that was received. The packet will be dropped.
Firewall Action	drop
Recommended Action	Review configuration to reduce memory consumption.
Revision	2

2.49.5. drop_due_to_buffer_starvation (ID: 04800007)

Default Severity	ERROR
Log Message	Can't allocate resources to process a packet
Explanation	The firewall ran out of resources when trying to allocate resources to send a packet. The packet that triggered the need to send a packet will be dropped.
Firewall Action	drop
Recommended Action	Check buffer consumption.
Revision	2

2.49.6. failed_to_send_ack (ID: 04800008)

Default Severity	ERROR
Log Message	Failed to send TCP ACK in response to a segment
Explanation	The firewall responds to some segments by sending an acknowledgement segment to the sender. An example is when it receives a segment that is outside of the receiver's receive window. This log message indicates that the firewall failed to allocate resources to send such an acknoledgement segment.
Firewall Action	none
Recommended Action	Check buffer consumption.
Revision	2

2.49.7. processing_memory_limit_reached (ID: 04800009)

Default Severity	NOTICE
Log Message	Maximum processing memory limit reached
Explanation	The reassembly subsystem has reached the maximum limit set on its processing memory. This will decrease the performance of connections that are processed by the reassembly subsystem.
Firewall Action	drop
Recommended Action	Consider increasing the setting Reassembly_MaxProcessingMem.
Revision	1

2.49.8. maximum_connections_limit_reached (ID: 04800010)

Default Severity	NOTICE
Log Message	Maximum connections limit reached
Explanation	The reassembly subsystem has reached the maximum number of concurrent connections.
Firewall Action	none
Recommended Action	Consider increasing the setting Reassembly_MaxConnections.
Revision	1
Context Parameters	Connection

2.49.9. state_memory_allocation_failed (ID: 04800011)

Default Severity	ERROR
Log Message	Failed to allocate the memory needed to activate reassembly on a connection
Explanation	The reassembly subsystem has failed to allocate the memory needed to activate reassembly on a connection.
Firewall Action	none
Recommended Action	Review configuration to reduce memory consumption.
Revision	1
Context Parameters	Connection

2.50. RFO

These log messages refer to the **RFO (Route fail over events)** category.

2.50.1. has_ping (ID: 04100001)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route enabled, got PING reply from GW <gateway>
Explanation	Route is available. Received PING reply from the gateway.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	iface table net gateway

2.50.2. no_ping (ID: 04100002)

Default Severity	WARNING
Log Message	Interface <iface>, Table <table>, Net <net>: Unable to open conn for PING trying again later
Explanation	Unable to open a connection to verify the status of the route. Will try again later.
Firewall Action	try_again_later
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.50.3. no_ping (ID: 04100003)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route disabled, no PING reply from Gateway <gateway>
Explanation	Route is not available, and has been disabled. Did not receive a PING

reply from the gateway.

Firewall Action route_disabled

Recommended Action None.

Revision 1

Parameters iface
table
net
gateway

2.50.4. unable_to_register_pingmon (ID: 04100004)

Default Severity WARNING

Log Message Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register PING monitor

Explanation Internal Error: The route is no longer monitored. Failed to register PING Route Monitor.

Firewall Action route_not_monitored

Recommended Action None.

Revision 1

Parameters iface
table
net
gateway

2.50.5. unable_to_register_pingmon (ID: 04100005)

Default Severity ERROR

Log Message Interface <iface>, Table <table>, Net <net>: Route no longer monitored via PING, unable to register PING monitor

Explanation Internal Error: The route is no longer monitored. Failed to register PING Route Monitor.

Firewall Action disabled_monitor

Recommended Action None.

Revision 1

Parameters iface
table
net
gateway

2.50.6. has_arp (ID: 04100006)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route enabled, got ARP reply from Gateway <gateway>
Explanation	Route is available. Received ARP reply from the gateway.
Firewall Action	route_enabled
Recommended Action	None.
Revision	2
Parameters	iface table net gateway

2.50.7. no_arp (ID: 04100007)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route disabled, no ARP reply from Gateway <gateway>
Explanation	Route is not available, and has been disabled. Did not receive a ARP reply from the gateway.
Firewall Action	route_disabled
Recommended Action	None.
Revision	2
Parameters	iface table net gateway

2.50.8. unable_to_register_arp_monitor (ID: 04100008)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register ARP monitor
Explanation	Internal Error: The route is no longer monitored. Failed to register ARP Route Monitor.
Firewall Action	no_monitoring
Recommended Action	None.

Revision 1

Parameters iface
table
net
gateway

2.50.9. unable_to_register_arp_monitor (ID: 04100009)

Default Severity WARNING

Log Message Interface <iface>, Table <table>, Net <net>: Route no longer monitored via ARP, unable to register ARP monitor

Explanation Internal Error: The route is no longer monitored. Failed to register ARP Route Monitor.

Firewall Action disabled_monitor

Recommended Action None.

Revision 1

Parameters iface
table
net
gateway

2.50.10. no_link (ID: 04100010)

Default Severity ERROR

Log Message Interface <iface> has no link (reason: <reason>), all associated routes disabled.

Explanation The interface has no link, and all associated routes has been disabled.

Firewall Action associated_routes_disabled

Recommended Action None.

Revision 2

Parameters iface
reason

2.50.11. has_link (ID: 04100011)

Default Severity NOTICE

Log Message Interface <iface> has link. Some associated routes may require ARP to be enabled

Explanation	The interface has a link. Some associated routes may require ARP to be enabled.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	iface

2.50.12. unable_to_register_interface_monitor (ID: 04100012)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register interface monitor
Explanation	Internal Error: Route is no longer monitored. Unable to register Interface Monitor.
Firewall Action	no_monitoring
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.50.13. unable_to_register_interface_monitor (ID: 04100013)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register interface monitor
Explanation	Internal Error: Route is no longer monitored. Unable to register Interface Monitor.
Firewall Action	disabled_monitor
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.50.14. hostmon_failed (ID: 04100014)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route disabled, host monitoring failed
Explanation	Route is disabled. Host monitoring failed.
Firewall Action	route_disabled
Recommended Action	None.
Revision	1
Parameters	iface table net

2.50.15. hostmon_successful (ID: 04100015)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route enabled, host monitoring successful
Explanation	Route is available. Host monitoring successful.
Firewall Action	route_enabled
Recommended Action	None.
Revision	1
Parameters	iface table net

2.51. RULE

These log messages refer to the **RULE (Events triggered by rules)** category.

2.51.1. ruleset_fwdfast (ID: 06000003)

Default Severity	NOTICE
Log Message	Packet statelessly forwarded (fwdfast)
Explanation	The packet matches a rule with a "fwdfast" action, and is statelessly forwarded.
Firewall Action	fwdfast
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.51.2. ip_verified_access (ID: 06000005)

Default Severity	NOTICE
Log Message	IP address verified according to ACCESS section
Explanation	The IP address was verified according to the ACCESS section.
Firewall Action	access_allow
Recommended Action	None.
Revision	2
Context Parameters	Rule Name Packet Buffer

2.51.3. rule_match (ID: 06000006)

Default Severity	DEBUG
Log Message	GOTO action trigged
Explanation	A rule with a special GOTO action was trigged by an IP-rule lookup. This log message only appears if you explicitly requested it for the rule in question, and it is considered of DEBUG severity.
Firewall Action	GOTO
Recommended Action	None.
Revision	1

Context Parameters	Rule Name Rule Information Packet Buffer

2.51.4. rule_match (ID: 06000007)

Default Severity	DEBUG
Log Message	RETURN action trigged
Explanation	A rule with a special RETURN action was trigged by an IP-rule lookup. This log message only appears if you explicitly requested it for the rule in question, and it is considered of DEBUG severity.
Firewall Action	RETURN
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Rule Information Packet Buffer

2.51.5. block0net (ID: 06000010)

Default Severity	WARNING
Log Message	Destination address is the 0.* net. Dropping
Explanation	The destination address was the 0.* net, which is not allowed according to the configuration. The packet is dropped.
Firewall Action	drop
Recommended Action	Investigate why this traffic had the 0.* net as the destination.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.6. block0net (ID: 06000011)

Default Severity	WARNING
Log Message	Destination address is the 0.* net. Accepting
Explanation	The destination address was the 0.* net, which is allowed according to the configuration. The packet is accepted.
Firewall Action	accept
Recommended Action	If this type of traffic should be dropped, modify the "Settings"

section in the configuration.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.51.7. block127net (ID: 06000012)

Default Severity WARNING

Log Message Destination address is the 127.* net. Dropping

Explanation The destination address was the 127.* net, which is not allowed according to the configuration. The packet is dropped.

Firewall Action drop

Recommended Action Investigate why this traffic had the 127.* net as the destination.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.51.8. block127net (ID: 06000013)

Default Severity WARNING

Log Message Destination address is the 127.* net. Accepting

Explanation The destination address was the 127.* net, which is allowed according to the configuration. The packet is accepted.

Firewall Action accept

Recommended Action If this type of traffic should be dropped, modify the "Settings" section in the configuration.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.51.9. broadcast_nat (ID: 06000014)

Default Severity NOTICE

Log Message \nat" action does not forward broadcast traffic.

Explanation Broadcast traffic can be only forwarded by "allow" or "fwdfast" actions.

Firewall Action drop

Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.10. allow_broadcast (ID: 06000016)

Default Severity	NOTICE
Log Message	Broadcast packet statelessly forwarded
Explanation	The broadcast packet matches a rule with a "allow" action, and is statelessly forwarded.
Firewall Action	stateless_fwd
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.51.11. block0net (ID: 06000020)

Default Severity	WARNING
Log Message	Destination address is the 0::/8 net. Dropping
Explanation	The destination address was the 0::/8 net, which is not allowed according to the configuration. The packet is dropped.
Firewall Action	drop
Recommended Action	Investigate why this traffic had the 0::/8 net as the destination.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.12. block0net (ID: 06000021)

Default Severity	WARNING
Log Message	Destination address is the 0::/8 net. Accepting
Explanation	The destination address was the 0::/8 net, which is allowed according to the configuration. The packet is accepted.
Firewall Action	accept

Recommended Action	If this type of traffic should be dropped, modify the "Settings" section in the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.13. directed_broadcasts (ID: 06000030)

Default Severity	NOTICE
Log Message	Packet directed to the broadcast address of the destination network. Forwarding
Explanation	The packet was directed to the broadcast address of the destination network, and the unit is configured to allow this.
Firewall Action	forward
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.14. directed_broadcasts (ID: 06000031)

Default Severity	NOTICE
Log Message	Packet directed to the broadcast address of the destination network. Dropping
Explanation	The packet was directed to the broadcast address of the destination network, and the unit is configured to disallow this.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.15. unknown_vlantag (ID: 06000040)

Default Severity	WARNING
Log Message	Received VLAN packet with unknown type<type> and VLAN ID <vlanid>. Dropping
Explanation	The unit received a VLAN packet with an unknown tag, and the

	packet is dropped.
Firewall Action	drop
Recommended Action	None.
Revision	3
Parameters	type vlanid
Context Parameters	Rule Name Packet Buffer

2.51.16. ruleset_reject_packet (ID: 06000050)

Default Severity	WARNING
Log Message	Packet rejected by rule-set. Rejecting
Explanation	The rule-set is configured to rejected this packet.
Firewall Action	reject
Recommended Action	If this is not the indended behaviour, modify the rule-set.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.51.17. ruleset_drop_packet (ID: 06000051)

Default Severity	WARNING
Log Message	Packet dropped by rule-set. Dropping
Explanation	The rule-set is configured to drop this packet.
Firewall Action	drop
Recommended Action	If this is not the indended behaviour, modify the rule-set.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.51.18. unhandled_local (ID: 06000060)

Default Severity	NOTICE
Log Message	Allowed but unhandled packet to the firewall. Dropping

Explanation	A packet directed to the unit itself was received. The packet is allowed, but there is no matching state information for this packet. It is not part of any open connections, and will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.51.19. ip4_address_added (ID: 06000070)

Default Severity	INFORMATIONAL
Log Message	IP address <ip> added to FQDN address <fqdn_name> used in IPPolicy <dir> filter.
Explanation	The IPPolicy address filter was updated by the DNS Cache.
Firewall Action	policy_updated
Recommended Action	None.
Revision	1
Parameters	fqdn_name dir ip
Context Parameters	Rule Name

2.51.20. ip6_address_added (ID: 06000071)

Default Severity	INFORMATIONAL
Log Message	IP address <ip> added to FQDN address <fqdn_name> used in IPPolicy <dir> filter.
Explanation	The IPPolicy address filter was updated by the DNS Cache.
Firewall Action	policy_updated
Recommended Action	None.
Revision	1
Parameters	fqdn_name dir ip
Context Parameters	Rule Name

2.51.21. ip4_address_removed (ID: 06000072)

Default Severity	INFORMATIONAL
Log Message	IP address <ip> removed from FQDN address <fqdn_name> used in IPPolicy <dir> filter.
Explanation	The IPPolicy address filter was updated by the DNS Cache.
Firewall Action	policy_updated
Recommended Action	None.
Revision	1
Parameters	fqdn_name dir ip
Context Parameters	Rule Name

2.51.22. ip6_address_removed (ID: 06000073)

Default Severity	INFORMATIONAL
Log Message	IP address <ip> removed from FQDN address <fqdn_name> used in IPPolicy <dir> filter.
Explanation	The IPPolicy address filter was updated by the DNS Cache.
Firewall Action	policy_updated
Recommended Action	None.
Revision	1
Parameters	fqdn_name dir ip
Context Parameters	Rule Name

2.51.23. dns_no_record (ID: 06000074)

Default Severity	ERROR
Log Message	DNS reports no record of FQDN address <fqdn_name> used in IPPolicy <dir> filter.
Explanation	The DNS server reports that there is no record of the configured FQDN address.
Firewall Action	None

Recommended Action	Verify that the FQDN address was entered correctly.
Revision	1
Parameters	fqdn_name dir
Context Parameters	Rule Name

2.51.24. dns_timeout (ID: 06000075)

Default Severity	ERROR
Log Message	DNS query of FQDN address <fqdn_name> in IPPolicy <dir> filter timed out.
Explanation	The DNS Cache did not receive a response from the DNS server.
Firewall Action	None
Recommended Action	Verify that the configured DNS server is reachable.
Revision	1
Parameters	fqdn_name dir
Context Parameters	Rule Name

2.51.25. dns_error (ID: 06000076)

Default Severity	ERROR
Log Message	DNS query of FQDN address <fqdn_name> in IPPolicy <dir> filter failed.
Explanation	The system was unable to resolve the FQDN address due to an internal error.
Firewall Action	None
Recommended Action	If the problem persists, please contact the support and report this issue.
Revision	1
Parameters	fqdn_name dir
Context Parameters	Rule Name

2.52. SERVICES

These log messages refer to the **SERVICES (System services events)** category.

2.52.1. httpposter_success (ID: 06600100)

Default Severity	NOTICE
Log Message	Success updating <host> using HTTP Poster, next update in <update_delay> seconds
Explanation	The HTTP Poster update failed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	host update_delay
Context Parameters	Connection

2.52.2. httpposter_failure (ID: 06600101)

Default Severity	WARNING
Log Message	Failed to update <host> using HTTP Poster, retry in <retry_delay> seconds
Explanation	The HTTP Poster update failed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	host retry_delay reason
Context Parameters	Connection

2.52.3. httpposter_failure (ID: 06600102)

Default Severity	WARNING
Log Message	Failed to update <host> using HTTP Poster, retry in <retry_delay> seconds
Explanation	The HTTP Poster update failed.

Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	host retry_delay reason

2.53. SESMGR

These log messages refer to the **SESMGR (Session Manager events)** category.

2.53.1. sesmgr_session_created (ID: 04900001)

Default Severity	NOTICE
Log Message	Session connected for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	New session created in Session Manager.
Firewall Action	none
Recommended Action	None.
Revision	2
Parameters	user database ip type

2.53.2. sesmgr_session_denied (ID: 04900002)

Default Severity	WARNING
Log Message	New session denied for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	New session denied in Session Manager.
Firewall Action	remove_session
Recommended Action	Check settings for users.
Revision	2
Parameters	user database ip type

2.53.3. sesmgr_session_removed (ID: 04900003)

Default Severity	NOTICE
Log Message	Session disconnected for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Session disconnected in Session Manager.
Firewall Action	none

Recommended Action None.

Revision 2

Parameters user
database
ip
type

2.53.4. sesmgr_access_set (ID: 04900004)

Default Severity NOTICE

Log Message Access level changed to <access> for User: <user>. Database: <database>. IP: <ip>. Type: <type>.

Explanation Access level has been changed for session.

Firewall Action none

Recommended Action None.

Revision 2

Parameters user
access
database
ip
type

2.53.5. sesmgr_session_timeout (ID: 04900005)

Default Severity NOTICE

Log Message Session has timed out for User: <user>. Database: <database>. IP: <ip>. Type: <type>.

Explanation Session has timed out and will be removed.

Firewall Action remove_session

Recommended Action None.

Revision 2

Parameters user
database
ip
type

2.53.6. sesmgr_upload_denied (ID: 04900006)

Default Severity NOTICE

Log Message	File upload connection denied for User: <user>. IP: <ip>. Type: <type>.
Explanation	Administrator session already active, file upload session denied.
Firewall Action	deny_upload
Recommended Action	Terminate administrator session and try again.
Revision	2
Parameters	user ip type

2.53.7. sesmgr_console_denied (ID: 04900007)

Default Severity	WARNING
Log Message	Could not create new console for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Could not create new console, new session will be removed.
Firewall Action	remove_session
Recommended Action	Check maximum number of sessions and consoles.
Revision	2
Parameters	user database ip type

2.53.8. sesmgr_session_maximum_reached (ID: 04900008)

Default Severity	WARNING
Log Message	Maximum number of sessions reached
Explanation	Maximum number of sessions reached.
Firewall Action	deny_new_session
Recommended Action	Remove inactive sessions or increase maximum number of allowed sessions.
Revision	1

2.53.9. sesmgr_allocate_error (ID: 04900009)

Default Severity	EMERGENCY

Log Message	Could not allocate memory for new session
Explanation	Could not allocate memory for new session.
Firewall Action	none
Recommended Action	Check memory.
Revision	1

2.53.10. sesmgr_session_activate (ID: 04900010)

Default Severity	NOTICE
Log Message	Session has been activated for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Disabled session has been activated.
Firewall Action	none
Recommended Action	None.
Revision	2
Parameters	user database ip type

2.53.11. sesmgr_session_disabled (ID: 04900011)

Default Severity	NOTICE
Log Message	Session has been disabled for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Session has been disabled.
Firewall Action	none
Recommended Action	None.
Revision	2
Parameters	user database ip type

2.53.12. sesmgr_console_denied_init (ID: 04900012)

Default Severity	ALERT

Log Message	Could not create new console at initialization of firewall for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Could not create new console at initialization of firewall.
Firewall Action	remove_session
Recommended Action	Check maximum number of sessions and consoles.
Revision	2
Parameters	user database ip type

2.53.13. sesmgr_session_access_missing (ID: 04900015)

Default Severity	WARNING
Log Message	No access level set for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	No access level set for user, new session denied.
Firewall Action	deny_session
Recommended Action	Check user settings.
Revision	2
Parameters	user database ip type

2.53.14. sesmgr_session_old_removed (ID: 04900016)

Default Severity	NOTICE
Log Message	Old session disconnected to be replaced for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Old session disconnected and is being replaced by a new session for the user.
Firewall Action	none
Recommended Action	None.
Revision	2
Parameters	user database ip type

2.53.15. sesmgr_file_error (ID: 04900017)

Default Severity	ALERT
Log Message	Error accessing files.
Explanation	Error occured when accessing files for reading/writing.
Firewall Action	file_error
Recommended Action	Check available memory.
Revision	1

2.53.16. sesmgr_techsupport (ID: 04900018)

Default Severity	NOTICE
Log Message	Sending technical support file.
Explanation	Technical support file created and is being sent to user.
Firewall Action	techsupport_created
Recommended Action	None.
Revision	1

2.54. SLB

These log messages refer to the **SLB (SLB events)** category.

2.54.1. server_online (ID: 02900001)

Default Severity	NOTICE
Log Message	SLB Server <server_ip> is online according to monitor
Explanation	A disabled server has been determined to be alive again.
Firewall Action	Adding this server to the active servers list.
Recommended Action	None.
Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.54.2. server_offline (ID: 02900002)

Default Severity	WARNING
Log Message	SLB Server <server_ip> is offline according to monitor
Explanation	The server is determined to be offline according to monitor.
Firewall Action	Removing this server from the active servers list.
Recommended Action	Determine why the server is not responding.
Revision	2
Parameters	server_ip monitor [monitor_port] [url]
Context Parameters	Rule Name

2.54.3. maintenance_start (ID: 02900003)

Default Severity	NOTICE
Log Message	SLB Server <server_ip> is entering maintenance mode
Explanation	A server has entered maintenance mode.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.54.4. maintenance_end (ID: 02900004)

Default Severity	NOTICE
Log Message	SLB Server <server_ip> is leaving maintenance mode
Explanation	A server has left maintenance mode.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.54.5. server_load_unknown (ID: 02900005)

Default Severity	WARNING
Log Message	SLB Server <server_ip> is not reporting load
Explanation	A server has not reported its load within the minimum timeframe.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.54.6. malformed_post (ID: 02900006)

Default Severity	WARNING
Log Message	Malformed request sent to the SLB handler in REST API
Explanation	The request was not formatted correctly.
Firewall Action	None
Recommended Action	None.

Revision	1

2.54.7. no_such_server (ID: 02900007)

Default Severity	WARNING
Log Message	The specified SLB server identifier and IP not configured
Explanation	The request supplied incorrect information.
Firewall Action	None
Recommended Action	None.
Revision	1

2.55. SMTPLOG

These log messages refer to the **SMTPLOG (SMTPLOG events)** category.

2.55.1. unable_to_establish_connection (ID: 03000001)

Default Severity	WARNING
Log Message	Unable to establish connection to SMTP server <smtp_server>. Send aborted
Explanation	The unit failed to establish a connection to the SMTP server. No SMTP Log will be sent.
Firewall Action	abort_sending
Recommended Action	Verify that a SMTP server is running at the address specified.
Revision	1
Parameters	smtp_server

2.55.2. connect_timeout (ID: 03000002)

Default Severity	WARNING
Log Message	Timeout connecting to SMTP server <smtp_server>. Send aborted
Explanation	The unit timed out while trying to establish a connection to the SMTP server. No SMTP Log will be sent.
Firewall Action	abort_sending
Recommended Action	Verify that a SMTP server is running at the address specified.
Revision	1
Parameters	smtp_server

2.55.3. send_failure (ID: 03000004)

Default Severity	WARNING
Log Message	Unable to send data to SMTP server <smtp_server>. Send aborted
Explanation	The unit failed to send data to the SMTP server. No SMTP Log will be sent.
Firewall Action	abort_sending
Recommended Action	None.
Revision	1

Parameters	smtp_server

2.55.4. receive_timeout (ID: 03000005)

Default Severity	WARNING
Log Message	Receive timeout from SMTP server <smtp_server>. Send aborted
Explanation	The unit timed out while receiving data from the SMTP server. No SMTP Log will be sent.
Firewall Action	abort_sending
Recommended Action	None.
Revision	1
Parameters	smtp_server

2.55.5. rejected_connect (ID: 03000006)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected connection. Send aborted
Explanation	The SMTP server reject the connection attempt. No SMTP Log will be sent.
Firewall Action	abort_sending
Recommended Action	Verify that a SMTP Server is configured to accept connections from the unit.
Revision	1
Parameters	smtp_server

2.55.6. rejected_ehlo_helo (ID: 03000007)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected both EHLO/HELO. Trying to continue anyway
Explanation	The SMTP server rejected the normal handshake process. The unit will try to continue anyway.
Firewall Action	None
Recommended Action	If problems arise, verify that the SMTP server is properly configured.
Revision	1
Parameters	smtp_server

2.55.7. rejected_sender (ID: 03000008)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected sender <sender>. Send aborted
Explanation	The SMTP server rejected the sender. No SMTP Log will be sent.
Firewall Action	abort_sending
Recommended Action	Verify that the SMTP server is configured to accept this sender.
Revision	1
Parameters	smtp_server sender

2.55.8. rejected_recipient (ID: 03000009)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected recipient <recipient>
Explanation	The SMTP server rejected the recipient. No SMTP Log will be sent.
Firewall Action	None
Recommended Action	Verify that the SMTP server is configured to accept this recipient.
Revision	1
Parameters	smtp_server recipient

2.55.9. rejected_all_recipients (ID: 03000010)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected all recipients. Send aborted
Explanation	The SMTP server rejected all recipients. No SMTP Log will be sent.
Firewall Action	None
Recommended Action	Verify that the SMTP server is configured to accept these recipients.
Revision	1
Parameters	smtp_server

2.55.10. rejected_data (ID: 03000011)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected DATA request. Send aborted
Explanation	The SMTP server rejected the DATA request. No SMTP Log will be sent.
Firewall Action	None
Recommended Action	Verify that the SMTP server is properly configured.
Revision	1
Parameters	smtp_server

2.55.11. rejected_message_text (ID: 03000012)

Default Severity	WARNING
Log Message	SMTP server <smtp_server> rejected message text. Send aborted
Explanation	The SMTP server rejected the message text. No SMTP Log will be sent.
Firewall Action	None
Recommended Action	Verify that the SMTP server is properly configured.
Revision	1
Parameters	smtp_server

2.55.12. dns_subscription_failed (ID: 03000020)

Default Severity	ERROR
Log Message	Subscription <fqdn> for DNS CACHE failed for <logger>.
Explanation	The FQDN provided as .
Firewall Action	Verify that at least one DNS server is properly configured.
Recommended Action	Verify that at least one DNS server is properly configured.
Revision	1
Parameters	fqdn logger

2.55.13. ip4_address_removed (ID: 03000021)

Default Severity	WARNING

Log Message	IP address <ip> removed from FQDN address <fqdn_name> used in SMTP logger <logger>.
Explanation	The IP address used by [logger] has been deleted by the DNS module.
Firewall Action	smtplogger_updated
Recommended Action	None.
Revision	1
Parameters	ip fqdn_name logger

2.55.14. dns_no_record (ID: 03000022)

Default Severity	ERROR
Log Message	DNS reports no record of FQDN address <fqdn_name> used in SMTP logger <logger>.
Explanation	The DNS server reports that there is no record of the configured FQDN address.
Firewall Action	None
Recommended Action	Verify that the FQDN address was entered correctly.
Revision	1
Parameters	fqdn_name logger

2.55.15. dns_timeout (ID: 03000023)

Default Severity	ERROR
Log Message	DNS query of FQDN address <fqdn_name> in SMTP logger <logger> timed out.
Explanation	The DNS Cache did not receive a response from the DNS server.
Firewall Action	None
Recommended Action	Verify that the configured DNS server is reachable.
Revision	1
Parameters	fqdn_name logger

2.55.16. dns_error (ID: 03000024)

Default Severity	ERROR
Log Message	DNS query of FQDN address <fqdn_name> in SMTP logger <logger> failed.
Explanation	The system was unable to resolve the FQDN address due to an internal error.
Firewall Action	None
Recommended Action	If the problem persists, please contact the support and report this issue.
Revision	1
Parameters	fqdn_name logger

2.55.17. ip4_address_not_added (ID: 03000025)

Default Severity	ERROR
Log Message	Failed to update IP address <ip> added to FQDN address <fqdn_name> used in SMTP logger <logger>.
Explanation	The IP address for the SMTP server used by logger [logger] could not be updated.
Firewall Action	smtplogger_fail
Recommended Action	None.
Revision	1
Parameters	fqdn_name ip logger

2.55.18. ip4_address_added (ID: 03000026)

Default Severity	INFORMATIONAL
Log Message	IP address <ip> added to FQDN address <fqdn_name> used in SMTP logger <logger>.
Explanation	The IP address for the SMTP server used by logger [logger] was updated by the DNS Cache.
Firewall Action	smtplogger_updated
Recommended Action	None.
Revision	1
Parameters	fqdn_name ip

logger

2.56. SNMP

These log messages refer to the **SNMP (Allowed and disallowed SNMP accesses)** category.

2.56.1. disallowed_sender (ID: 03100001)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, disallowed sender IP
Explanation	The sender IP address is not allowed to send SNMP data to the unit. Dropping packet.
Firewall Action	drop
Recommended Action	If this sender IP address should have SNMP access to the unit, this should be configured in the ACCESS section.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.2. invalid_snmp_community (ID: 03100002)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, invalid community string
Explanation	The SNMP community string is invalid.
Firewall Action	drop
Recommended Action	Make sure the entered SNMP community string is correct.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.3. snmp3_received_unautherized_message (ID: 03100100)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, authentication failed
Explanation	Calculated message digest is not the same as received digest.
Firewall Action	drop
Recommended Action	Investigate client that send unauthorized messages.

Revision	1
Parameters	peer
Context Parameters	Connection

2.56.4. snmp3_local_password_too_short (ID: 03100101)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, local password is too short
Explanation	SNMPv3 specification RFC3414 ch. 11.2 demands that the passowrd is at least 8 characters. System will not allow SNMPv3 requests as long as the local password is too short.
Firewall Action	drop
Recommended Action	Make sure the password string in local user database is at least 8 characters.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.5. snmp3_authentication_failed (ID: 03100102)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, authentication failed
Explanation	The SNMP authentication failed.
Firewall Action	drop
Recommended Action	Make sure the entered SNMP username and password strings are correct.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.6. snmp3_unsupported_securitylevel (ID: 03100103)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, wrong security level
Explanation	System received a SNMP message with a security level that does not match the configured security level.

Firewall Action	drop
Recommended Action	Make sure the security level of the SNMP client match the security level of the system.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.7. snmp3_message_intended_for_other_system (ID: 03100104)

Default Severity	WARNING
Log Message	Disallowed SNMP from <peer>, message was intended for another system
Explanation	System received a SNMP message with an Engine ID that this system does not have.
Firewall Action	drop
Recommended Action	Find out what is sending these SNMP messages and take appropriate action to stop these messages.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.8. snmp3_rebooted_2147483647_times (ID: 03100105)

Default Severity	ERROR
Log Message	Disallowed SNMP from <peer>, system has rebooted 2147483647 times
Explanation	System has rebooted 2147483647 times. The reboot counter has reached its maximum value.
Firewall Action	drop
Recommended Action	The engine ID of the system must be changed manually.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.9. snmp3_outside_of_time_window (ID: 03100106)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, message is outside of the Time Window +/-150 seconds
Explanation	According to SNMPv3 specification RFC3414 a message containing engine time that differs more than +/-150 seconds from current time is to be dropped to prevent replay attacks.
Firewall Action	drop
Recommended Action	Investigate the peer that sends SNMP messages that are ouside the Time Window.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.10. snmp3_bad_version (ID: 03100107)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, wrong SNMP version
Explanation	The SNMP request did not have the correct SNMP version.
Firewall Action	drop
Recommended Action	Make sure the selected SNMP version is correct.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.11. snmp3_decryption_failed (ID: 03100108)

Default Severity	WARNING
Log Message	Disallowed SNMP from <peer>, decryption failed
Explanation	The SNMP decryption failed because peer did not send an appropriate privParameter.
Firewall Action	drop
Recommended Action	Investigate the device that send invalid privParameter.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.12. snmp3_decryption_failed (ID: 03100109)

Default Severity	WARNING
Log Message	Disallowed SNMP from <peer>, decryption failed
Explanation	The SNMP decryption failed.
Firewall Action	drop
Recommended Action	Check that peer uses correct cipher.
Revision	1
Parameters	peer
Context Parameters	Connection

2.56.13. snmp3_message_not_in_time_window (ID: 03100110)

Default Severity	ERROR
Log Message	Disallowed SNMP from <peer>, received message not in time window
Explanation	Received message did not have the same number of engine boots as system. Someone may be trying to resend old messages to system.
Firewall Action	drop
Recommended Action	Investigate peer that sends malformed message.
Revision	1
Parameters	peer
Context Parameters	Connection

2.57. SSHD

These log messages refer to the **SSHD (SSH Server events)** category.

2.57.1. out_of_mem (ID: 04700001)

Default Severity	ERROR
Log Message	Out of memory
Explanation	Memory Allocation Failure. System is running low on RAM memory.
Firewall Action	close
Recommended Action	Try to free some of the RAM used, or upgrade the amount of RAM memory.
Revision	1

2.57.2. dh_key_exchange_failure (ID: 04700002)

Default Severity	ERROR
Log Message	DH Key Exchange parse error when exchanging keys with client <client>
Explanation	A Diffie-Hellman Key Exchange Failure occured when keys were exchanged with the client. Connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	2
Parameters	client reason

2.57.3. illegal_version_string (ID: 04700004)

Default Severity	ERROR
Log Message	Version string is invalid.
Explanation	An invalid version string was received from the client. The connection will be closed.
Firewall Action	close
Recommended Action	Investigate why the SSH client is sending a malformed version string.
Revision	1

2.57.4. error_occurred (ID: 04700005)

Default Severity	ERROR
Log Message	<error> occurred with the connection from client <client>.
Explanation	An error occurred, and the connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	error client

2.57.5. invalid_mac (ID: 04700007)

Default Severity	WARNING
Log Message	MAC comparison failure.
Explanation	The MAC received from the client is invalid. The connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1

2.57.6. invalid_service_request (ID: 04700015)

Default Severity	WARNING
Log Message	Error processing service request from client <client>
Explanation	Failed to process service request sent from the client, closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	client

2.57.7. invalid_username_change (ID: 04700020)

Default Severity	WARNING

Log Message	Username change is not allowed. From name <fromname> to <toname> client. Client: <client>
Explanation	User changed the username between two authentication phases, which is not allowed. Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	fromname toname client

2.57.8. invalid_username_change (ID: 04700025)

Default Severity	WARNING
Log Message	Service change is not allowed. From serivce <fromservice> to <toservice>. Client: <client>
Explanation	User changed the service between two authentication phases, which is not allowed. Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	fromservice toservice client

2.57.9. max_auth_tries_reached (ID: 04700030)

Default Severity	ERROR
Log Message	Maximum authentication re-tries reached for client <client>
Explanation	User failed to authenticate within the maximum allowed number of tries. Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	client

2.57.10. ssh_login_timeout_expired (ID: 04700035)

Default Severity	WARNING
Log Message	SSH Login grace timeout (<gracetime> seconds) expired, closing connection. Client: <client>
Explanation	The client failed to login within the given login grace time. Closing connection.
Firewall Action	close
Recommended Action	Increase the grace timeout value if it is set too low.
Revision	1
Parameters	gracetime client

2.57.11. ssh_inactive_timeout_expired (ID: 04700036)

Default Severity	WARNING
Log Message	SSH session inactivity limit (<inactivetime>) has been reached. Closing connection. Client: <client>
Explanation	The connect client has been inactive for too long, and is forcibly logged out. Closing connection.
Firewall Action	close
Recommended Action	Increase the inactive session timeout value if it is set too low.
Revision	1
Parameters	inactivetime client

2.57.12. rsa_sign_verification_failed (ID: 04700050)

Default Severity	ERROR
Log Message	RSA signature verification for client <client> failed.
Explanation	The client RSA signuature could not be verified. Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	client

2.57.13. key_algo_not_supported. (ID: 04700055)

Default Severity	ERROR
Log Message	The authentication algorithm type <keytype> is not supported. Client <client>
Explanation	The authentication algorithm that the client uses is not supported. Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	keytype client

2.57.14. unsupported_pubkey_algo (ID: 04700057)

Default Severity	NOTICE
Log Message	Public Key Authentication Algorithm <authalgo> from client <client> not supported/enabled.
Explanation	The client is trying to authenticate using a Public Key Algorithm which is either not supported or not enabled.
Firewall Action	close
Recommended Action	If the algorithm is supported by unit, configure the unit to make use of it.
Revision	1
Parameters	authalgo client

2.57.15. unknown_ssh_public_key (ID: 04700058)

Default Severity	ERROR
Log Message	<client> provided an unknown key for SSH authentication.
Explanation	The client provided an unknown SSH public key for authentication. Closing connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	client

2.57.16. max_ssh_clients_reached (ID: 04700060)

Default Severity	WARNING
Log Message	Maximum number of connected SSH clients (<maxclients>) has been reached. Denying acces for client: <client>.
Explanation	The maximum number of simultaneously connected SSH clients has been reached. Denying access for this attempt, and closing the connection.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	maxclients client

2.57.17. client_disallowed (ID: 04700061)

Default Severity	WARNING
Log Message	Client <client> not allowed access according to the "remotes" section.
Explanation	The client is not allowed access to the SSH server. Closing connection.
Firewall Action	close
Recommended Action	If this client should be granted SSH access, add it in the "remotes" section.
Revision	1
Parameters	client

2.57.18. ssh_force_conn_close (ID: 04700105)

Default Severity	NOTICE
Log Message	SSH connection is no longer valid. Client: <client>, closing connection
Explanation	The SSH connection is no longer valid. The might be a result of a "remotes" object being changed to no longer allow the SSH connection. Closing connection.
Firewall Action	close
Recommended Action	None.

Revision	1
Parameters	client

2.57.19. scp_failed_not_admin (ID: 04704000)

Default Severity	NOTICE
Log Message	Administrator access could not set for session from this ip: <ip>
Explanation	SCP transfers can only be used if sessions has administrator access. Closing connection.
Firewall Action	close
Recommended Action	If there are other active administrator session, they might preventing this session from gaining administrator access.
Revision	1
Parameters	ip

2.58. SSLVPN

These log messages refer to the **SSLVPN (SSLVPN events.)** category.

2.58.1. sslvpn_session_created (ID: 06300010)

Default Severity	INFORMATIONAL
Log Message	SSL VPN Session created at <ssliface>
Explanation	SSL VPN Session created at [ssliface].
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	ssliface username ipaddr
Context Parameters	Connection

2.58.2. sslvpn_session_closed (ID: 06300011)

Default Severity	INFORMATIONAL
Log Message	SSLVPN session closed at <ssliface>
Explanation	SSLVPN session closed at [ssliface].
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	ssliface username ipaddr
Context Parameters	Connection

2.58.3. sslvpn_max_sessions_reached (ID: 06300012)

Default Severity	ERROR
Log Message	SSL VPN can not create session. Maximun allowed SSLVPN tunnels reached.
Explanation	SSL VPN can not create session. Maximun allowed SSLVPN tunnels reached.

Firewall Action	None
Recommended Action	None.
Revision	3

2.58.4. failure_init_radius_accounting (ID: 06300013)

Default Severity	WARNING
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accouting will be disabled. Interface: <iface>
Explanation	Failed to send START message to RADIUS accounting server. RADIUS accounting will be disabled for this session. The specified interface, client IP and call ID identify the specific session.
Firewall Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.
Revision	1
Parameters	iface

2.58.5. sslvpn_connection_disallowed (ID: 06300203)

Default Severity	WARNING
Log Message	SSL VPN connection from <client_ip> disallowed according to rule <rule>!
Explanation	The SSL VPN connection is disallowed by the new configuration according to the specified userauth rule. Closing down the SSL VPN connection.
Firewall Action	sslvpn_connection_closed
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	2
Parameters	rule client_ip

2.58.6. unknown_sslvpn_auth_source (ID: 06300204)

Default Severity	WARNING
Log Message	Unknown SSL VPN authentication source for <rule>! Client: <client_ip>
Explanation	The authentication source for the specified userauth rule found in the new configuration is unknown to the SSL VPN server. Closing

	down the SSL VPN connection.
Firewall Action	sslvpn_connection_closed
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	2
Parameters	rule client_ip

2.58.7. user_disconnected (ID: 06300205)

Default Severity	INFORMATIONAL
Log Message	User <username> is forcibly disconnected. Client: <client_ip>
Explanation	The connected client is forcibly disconnected by the userauth system.
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	username client_ip

2.58.8. sslvpn_connection_disallowed (ID: 06300224)

Default Severity	WARNING
Log Message	SSL VPN connection from <client_ip> disallowed according to rule <rule>. Interface: <iface>.
Explanation	The SSL VPN connection is disallowed according to the specified userauth rule.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	2
Parameters	rule iface client_ip

2.58.9. unknown_sslvpn_auth_source (ID: 06300225)

Default Severity	WARNING
Log Message	Unknown SSL VPN authentication source for <rule>!. Interface:

	<iface>, Client: <client_ip>.
Explanation	The authentication source for the specified userauth rule is unknown to the SSL VPN server.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	2
Parameters	rule iface client_ip

2.58.10. sslvpn_no_userauth_rule_found (ID: 06300226)

Default Severity	CRITICAL
Log Message	Did not find a matching userauth rule for the incoming SSL VPN connection. Interface: <iface>, Client: <client_ip>.
Explanation	The SSL VPN server was unsuccessful trying to find a userauth rule matching the incoming SSL VPN connection.
Firewall Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	3
Parameters	iface client_ip

2.59. SYSTEM

These log messages refer to the **SYSTEM (System-wide events: startup, shutdown, etc..)** category.

2.59.1. demo_mode (ID: 03200021)

Default Severity	ALERT
Log Message	The unit is running in DEMO mode, and will eventually expire. Install a license in order to avoid this
Explanation	None.
Firewall Action	lockdown_soon
Recommended Action	Install a license.
Revision	2
Parameters	lockdown time

2.59.2. demo_mode (ID: 03200022)

Default Severity	ALERT
Log Message	DEMO mode halted at the count of <time> seconds. Reason: <reason>.
Explanation	DEMO mode halted at the count of [time] seconds. Reason: [reason].
Firewall Action	shutdown_soon
Recommended Action	Install a license.
Revision	1
Parameters	reason time

2.59.3. demo_mode (ID: 03200023)

Default Severity	ALERT
Log Message	DEMO mode resumed at the count of <time> seconds. Reason: <reason>.
Explanation	DEMO mode resumed at the count of [time] seconds. Reason: [reason].
Firewall Action	shutdown_soon
Recommended Action	Install a license.

Revision	1
Parameters	reason time

2.59.4. demo_mode (ID: 03200024)

Default Severity	ALERT
Log Message	The unit is now running in License Lockdown Mode. Install a license in order to avoid this
Explanation	None.
Firewall Action	license_lockdown
Recommended Action	Install a license.
Revision	2

2.59.5. normal_mode (ID: 03200025)

Default Severity	NOTICE
Log Message	License file successfully loaded.
Explanation	The system is now running in normal operation mode.
Firewall Action	normal_operation
Recommended Action	None.
Revision	1

2.59.6. new_firmware_available (ID: 03200030)

Default Severity	NOTICE
Log Message	New firmware available.
Explanation	A new firmware release is available for download.
Firewall Action	None
Recommended Action	Upgrade_firmware.
Revision	1

2.59.7. reset_clock (ID: 03200100)

Default Severity	NOTICE

Log Message	The clock at <oldtime> was manually reset by <user> to <newtime>
Explanation	The clock has manually been reset.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	oldtime newtime user

2.59.8. invalid_ip_match_access_section (ID: 03200110)

Default Severity	WARNING
Log Message	Failed to verify IP address as per ACCESS section. Dropping
Explanation	The IP address was not verified according to the ACCESS section.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.59.9. nitrox2_watchdog_triggered (ID: 03200207)

Default Severity	ERROR
Log Message	Nitrox II watchdog triggered.
Explanation	Nitrox II watchdog triggered.
Firewall Action	Reboot
Recommended Action	None.
Revision	1

2.59.10. nitrox2_restarted (ID: 03200208)

Default Severity	ERROR
Log Message	NITROX II interfaces restarted.
Explanation	NITROX II interfaces restarted.
Firewall Action	None

Recommended Action	None.
Revision	1

2.59.11. hardware_watchdog_initialized (ID: 03200260)

Default Severity	NOTICE
Log Message	Hardware Watchdog <hardware_watchdog_chip> found and initialized with a timeout of <watchdog_timeout> minutes.
Explanation	The system has identified a Hardware Watchdog and initialized it.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	hardware_watchdog_chip watchdog_timeout

2.59.12. port_bind_failed (ID: 03200300)

Default Severity	ALERT
Log Message	Out of memory while tying to allocate dynamic port for local IP <localip> to destination IP <destip>
Explanation	The unit failed to allocate a dynamic port, as it is out of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason localip destip

2.59.13. port_bind_failed (ID: 03200301)

Default Severity	WARNING
Log Message	Out of dynamic assigned ports. All ports <port_base>-<port_end> for Local IP <localip> to Destination IP <destip> are in use
Explanation	Failed to allocate a dynamic port, as all ports are in use.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	reason localip destip port_base port_end

2.59.14. port_hlm_conversion (ID: 03200302)

Default Severity	NOTICE
Log Message	Using High Load Mode for Local IP <localip> Destination IP <destip> pair
Explanation	Mode for Local IP - Destination IP pair has changed to High Load because of heavy traffic.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	localip destip

2.59.15. port_llm_conversion (ID: 03200303)

Default Severity	NOTICE
Log Message	Using Low Load Mode for Local IP <localip> Destination IP <destip> pair
Explanation	Mode for Local IP - Destination IP pair has changed to Low Load because of low traffic.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	localip destip

2.59.16. log_messages_lost_due_to_throttling (ID: 03200400)

Default Severity	WARNING
Log Message	<logcnt> messages lost due to throttling
Explanation	Due to extensive logging, a number of log messages was not sent.

Firewall Action	None
Recommended Action	Examine why the unit sent such a large amount of log messages. If this is normal activity, the "LogSendPerSec" setting might be set too low.
Revision	1
Parameters	logcnt

2.59.17. log_messages_lost_due_to_log_buffer_exhaust (ID: 03200401)

Default Severity	WARNING
Log Message	<logcnt> log messages lost due to log buffer exhaustion
Explanation	Due to extensive logging, a number of log messages was not sent.
Firewall Action	None
Recommended Action	Examine why the unit sent such a large amount of log messages. If this is normal activity, the "LogSendPerSec" setting might be set too low.
Revision	1
Parameters	logcnt

2.59.18. ssl_encryption_failed (ID: 03200450)

Default Severity	ERROR
Log Message	Encryption failed.
Explanation	Encryption failed due to error. Connection closed.
Firewall Action	None
Recommended Action	None.
Revision	1

2.59.19. bidir_fail (ID: 03200600)

Default Severity	CRITICAL
Log Message	Failed to establish bi-directional communication with peer in <timeout> seconds
Explanation	The unit failed to establish a connection back to peer, using the new configuration. It will try to revert to the previous configuration file.

Firewall Action	None
Recommended Action	Verify that the new configuration file does not contain errors that would cause bi-directional communication failure.
Revision	2
Parameters	localcfgver remotecfgver timeout

2.59.20. file_open_failed (ID: 03200602)

Default Severity	ERROR
Log Message	Failed to open newly uploaded configuration file <new_cfg>
Explanation	The unit failed to open the uploaded configuration file.
Firewall Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	new_cfg

2.59.21. disk_cannot_remove (ID: 03200603)

Default Severity	ERROR
Log Message	Failed to remove <old_cfg>
Explanation	The unit failed to remove the old configuration file.
Firewall Action	None
Recommended Action	Verify that the disk media is intact, and that the file is not write protected.
Revision	2
Parameters	old_cfg

2.59.22. disk_cannot_rename (ID: 03200604)

Default Severity	ERROR
Log Message	Failed to rename <cfg_new> to <cfg_real>
Explanation	The unit failed to rename the new configuration file to the real configuration file name.
Firewall Action	None

Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	cfg_new cfg_real

2.59.23. cfg_switch_fail (ID: 03200605)

Default Severity	CRITICAL
Log Message	Failed to switch to new configuration
Explanation	For reasons specified in earlier log events, the unit failed to switch to the new configuration and will continue to use the present configuration.
Firewall Action	None
Recommended Action	Consult the recommended action in the previous log message, which contained a more detailed error description.
Revision	1

2.59.24. core_switch_fail (ID: 03200606)

Default Severity	CRITICAL
Log Message	Failed to switch to new core
Explanation	For reasons specified in earlier log events, the unit failed to switch to the new core executable and will continue to use the present core executable.
Firewall Action	None
Recommended Action	Consult the recommended action in the previous log message, which contained a more detailed error description.
Revision	1

2.59.25. bidir_ok (ID: 03200607)

Default Severity	NOTICE
Log Message	Configuration <localcfgver><remotecfgver> verified for bi-directional communication
Explanation	The new configuration has been verified for communication back to peer, and will now be used as the active configuration.
Firewall Action	None
Recommended Action	None.

Revision	2
Parameters	localcfgver remotecfgver

2.59.26. rules_configuration_changed (ID: 03200641)

Default Severity	INFORMATIONAL
Log Message	IP Rules or Policies were altered by configuration changes made <date>
Explanation	IP Rules or Policies have been altered due to changes in the configuration.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	date

2.59.27. user_blocked (ID: 03200802)

Default Severity	NOTICE
Log Message	Login for user <database>:<username> has failed: currently in blocked state for the next <blockedremaining> seconds. Blocked since: <blockedsince>.
Explanation	Too many failed login attempt for the user.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	database username blockedremaining blockedsince

2.59.28. shutdown (ID: 03201000)

Default Severity	NOTICE
Log Message	Shutdown <shutdown>. Active in <time> seconds. Reason: <reason>
Explanation	The unit is shutting down.
Firewall Action	shutdown

Recommended Action	None.
Revision	1
Parameters	shutdown time reason

2.59.29. reconfiguration (ID: 03201001)

Default Severity	NOTICE
Log Message	Initiating reconfiguration. Active in <time> seconds. Reason: <reason>
Explanation	The unit is reconfiguring.
Firewall Action	reconfiguration
Recommended Action	None.
Revision	1
Parameters	time reason

2.59.30. shutdown (ID: 03201011)

Default Severity	NOTICE
Log Message	Shutdown aborted. Core file <core> missing
Explanation	The unit was issued a shutdown command, but no core executable file is seen. The shutdown process is aborted.
Firewall Action	shutdown_gateway_aborted
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	shutdown reason core

2.59.31. config_activation (ID: 03201020)

Default Severity	NOTICE
Log Message	Reconfiguration requested by <username> from <config_system> <client_ip>.
Explanation	Reconfiguration requested.

Firewall Action	reconfiguration
Recommended Action	None.
Revision	2
Parameters	username userdb" client_ip config_system

2.59.32. reconfiguration (ID: 03201021)

Default Severity	NOTICE
Log Message	Reconfiguration will change <change_count> access control rule(s).
Explanation	Number of access control rules changed during the reconfiguration.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	change_count

2.59.33. startup_normal (ID: 03202000)

Default Severity	NOTICE
Log Message	Firewall starting. Core: <corever>. Build: <build>. Current uptime: <uptime>. Using configuration file <cfgfile>, version <localcfgver> <remotecfgver>. Previous event: <previous_event>
Explanation	The firewall is starting up.
Firewall Action	None
Recommended Action	None.
Revision	4
Parameters	corever build uptime cfgfile localcfgver remotecfgver previous_event

2.59.34. startup_echo (ID: 03202001)

Default Severity	NOTICE

Log Message	Firewall starting echo (<delay> seconds). Core: <corever>. Build: <build>. Current uptime: <uptime>. Using configuration file <cfgfile>, localcfgver <localcfgver>, remotecfgver <remotecfgver>. Previous event: <previous_event>
Explanation	The firewall is starting up, echo.
Firewall Action	None
Recommended Action	None.
Revision	4
Parameters	delay corever build uptime cfgfile localcfgver remotecfgver previous_event

2.59.35. shutdown (ID: 03202500)

Default Severity	NOTICE
Log Message	Event <event>
Explanation	The firewall is shutting down.
Firewall Action	shutdown
Recommended Action	None.
Revision	2
Parameters	event

2.59.36. reconfiguration (ID: 03202501)

Default Severity	NOTICE
Log Message	Event <event>
Explanation	The firewall is reconfiguring.
Firewall Action	reconfiguration
Recommended Action	None.
Revision	2
Parameters	event

2.59.37. admin_login (ID: 03203000)

Default Severity	NOTICE
Log Message	Administrative user <username> logged in via <authsystem>. Access level: <access_level>
Explanation	An administrative user has logged in to the configuration system.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	authsystem username access_level [interface] [usergroups] [authsource] [userdb] [server_ip] [server_port] [client_ip] [client_port]

2.59.38. admin_logout (ID: 03203001)

Default Severity	NOTICE
Log Message	Administrative user <username> logged out, via <authsystem>. Access level: <access_level>
Explanation	An administrative user has logged out from the configuration system.
Firewall Action	None
Recommended Action	None.
Revision	3
Parameters	authsystem username access_level [userdb] [client_ip]

2.59.39. admin_login_failed (ID: 03203002)

Default Severity	WARNING
Log Message	Administrative user <username> failed to log in via <authsystem>, because of bad credentials
Explanation	An administrative user failed to log in to configuration system. This

	is most likely due to an invalid entered username or password.
Firewall Action	disallow_admin_access
Recommended Action	None.
Revision	3
Parameters	authsystem username [interface] [server_ip] [server_port] [client_ip] [client_port]

2.59.40. admin_authorization_failed (ID: 03203003)

Default Severity	WARNING
Log Message	Administrative user <username> successfully logged in via <authsystem>, but is not authorized to access the system.
Explanation	An administrative user successfully authenticated but is not authorized to access the system.
Firewall Action	disallow_admin_access
Recommended Action	If the user should have access to the system, increase the access level of the user or one the user's groups.
Revision	1
Parameters	authsystem interface username usergroups authsource userdb server_ip server_port client_ip client_port

2.59.41. sslvpnuser_login (ID: 03203004)

Default Severity	NOTICE
Log Message	SSL VPN user <username> logged in via <authsystem>.
Explanation	An SSL VPN user has logged in to the SSL VPN user page.
Firewall Action	None
Recommended Action	None.

Revision	2
Parameters	authsystem username userdb server_ip server_port client_ip client_port

2.59.42. activate_changes_failed (ID: 03204000)

Default Severity	NOTICE
Log Message	Bidirectional confirmation of the new configuration failed, previous configuration will be used
Explanation	The unit failed to establish a connection back to peer, using the new configuration. The previous configuration will still be used.
Firewall Action	using_prev_config
Recommended Action	Make sure that the new configuration allows the unit to establish a connection with the administration interface.
Revision	1
Parameters	authsystem

2.59.43. accept_configuration (ID: 03204001)

Default Severity	NOTICE
Log Message	New configuration activated by user <username> from <config_system> <client_ip>.
Explanation	The new configuration has been successfully activated.
Firewall Action	using_new_config
Recommended Action	None.
Revision	2
Parameters	username userdb" client_ip config_system

2.59.44. reject_configuration (ID: 03204002)

Default Severity	NOTICE

Log Message	New configuration rejected by user <username> from <config_system> <client_ip>.
Explanation	The new configuration has been rejected.
Firewall Action	reconfiguration_using_old_config
Recommended Action	None.
Revision	1
Parameters	username userdb" client_ip config_system

2.59.45. date_time_modified (ID: 03205000)

Default Severity	NOTICE
Log Message	The local Date and Time has been modified by <user>. Time and Date before change: <pre_change_date_time>. Time and Date after change: <post_change_date_time>
Explanation	The local Date and Time of the unit has been changed.
Firewall Action	using_new_date_time
Recommended Action	None.
Revision	2
Parameters	authsystem user pre_change_date_time post_change_date_time

2.59.46. admin_timeout (ID: 03206000)

Default Severity	NOTICE
Log Message	Administrative user <username> timed out from <authsystem>
Explanation	The administrative user has been inactive for too long, and has been automatically logged out.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	authsystem username userdb client_ip

access_level

2.59.47. admin_login_group_mismatch (ID: 03206001)

Default Severity WARNING

Log Message Administrative user <username> not allowed access via <authsystem>

Explanation The user does not have proper administration access to the configuration system.

Firewall Action disallow_admin_access

Recommended Action None.

Revision 2

Parameters authsystem
username
server_ip
server_port
client_ip
client_port

2.59.48. admin_login_internal_error (ID: 03206002)

Default Severity WARNING

Log Message Internal error occured when administrative user <username> tried to login, not allowed access via <authsystem>

Explanation An internal error occured when the user tried to log in, and as a result has not been given administration access.

Firewall Action disallow_admin_access

Recommended Action Please contact the support and report this issue.

Revision 2

Parameters authsystem
username
server_ip
server_port
client_ip
client_port

2.59.49. admin_authsource_timeout (ID: 03206003)

Default Severity ERROR

Log Message Remote <authsource> server(s) could not be reached when

attempting to authenticate administrative user <username>.

Explanation The unit did not receive a response from the authentication servers, and the authentication process failed.

Firewall Action None

Recommended Action Investigate why the configured servers are not responding to authentication requests.

Revision 1

Parameters authsystem
interface
username
authsource
server_ip
server_port
client_ip
client_port

2.59.50. user_post_token_invalid (ID: 03206004)

Default Severity WARNING

Log Message <username> has provided an invalid token when attempting a POST request.

Explanation All POST requests are required to provide a valid token for authentication.

Firewall Action refused_post_request

Recommended Action Please contact the support and report this issue.

Revision 1

Parameters client_ip
username
client_port

2.59.51. valid_rest_api_call (ID: 03207000)

Default Severity NOTICE

Log Message REST API call

Explanation .

Firewall Action None

Recommended Action None.

Revision 1

Parameters URI

	Method
Context Parameters	User Authentication

2.59.52. bad_user_credentials (ID: 03207010)

Default Severity	NOTICE
Log Message	Unknown user or invalid password
Explanation	REST API call failed. The entered username or password was invalid.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	URI Method
Context Parameters	User Authentication

2.59.53. bad_user_credentials (ID: 03207011)

Default Severity	NOTICE
Log Message	Unable to decode authentication
Explanation	REST API call failed. Unable to decode authentication.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	URI Method
Context Parameters	User Authentication

2.59.54. method_not_allowed (ID: 03207012)

Default Severity	NOTICE
Log Message	Method not allowed
Explanation	REST API call failed. Method not allowed.
Firewall Action	None
Recommended Action	None.

Revision	1
Parameters	URI Method
Context Parameters	User Authentication

2.59.55. unknown_api_call (ID: 03207013)

Default Severity	NOTICE
Log Message	No such API PATH
Explanation	REST API call failed. No such path.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	URI Method
Context Parameters	User Authentication

2.60. TCP_FLAG

These log messages refer to the **TCP_FLAG (Events concerning the TCP header flags)** category.

2.60.1. tcp_flags_set (ID: 03300001)

Default Severity	NOTICE
Log Message	The TCP <good_flag> and <bad_flag> flags are set. Allowing
Explanation	The possible combinations for these flags are: SYN URG, SYN PSH, SYN RST, SYN FIN and FIN URG.
Firewall Action	allow
Recommended Action	If any of these combinations should either be dropped or having the bad flag stripped, specify this in configuration, in the "Settings" sub system.
Revision	1
Parameters	good_flag bad_flag
Context Parameters	Rule Name Packet Buffer

2.60.2. tcp_flags_set (ID: 03300002)

Default Severity	WARNING
Log Message	The TCP <good_flag> and <bad_flag> flags are set. Stripping <bad_flag> flag
Explanation	The possible combinations for these flags are: SYN URG, SYN PSH, SYN RST, SYN FIN and FIN URG. Removing the "bad" flag.
Firewall Action	strip_bad_flag
Recommended Action	If any of these combinations should either be dropped or ignored, specify this in configuration, in the "Settings" sub system.
Revision	1
Parameters	good_flag bad_flag
Context Parameters	Rule Name Packet Buffer

2.60.3. tcp_flag_set (ID: 03300003)

Default Severity	NOTICE
Log Message	The TCP <bad_flag> flag is set. Ignoring
Explanation	The TCP flag is set. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.60.4. tcp_flag_set (ID: 03300004)

Default Severity	NOTICE
Log Message	The TCP <bad_flag> flag is set. Stripping
Explanation	A "bad" TCP flag is set. Removing it.
Firewall Action	strip_flag
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.60.5. tcp_null_flags (ID: 03300005)

Default Severity	NOTICE
Log Message	Packet has no SYN, ACK, FIN or RST flag set
Explanation	The packet has no SYN, ACK, FIN or RST flag set. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.60.6. tcp_flags_set (ID: 03300008)

Default Severity	WARNING
Log Message	The TCP <good_flag> and <bad_flag> flags are set. Dropping
Explanation	The possible combinations for these flags are: SYN URG, SYN PSH, SYN RST, SYN FIN and FIN URG.
Firewall Action	drop
Recommended Action	If any of these combinations should either be ignored or having the bad flag stripped, specify this in configuration, in the "Settings" sub system.
Revision	1
Parameters	good_flag bad_flag
Context Parameters	Rule Name Packet Buffer

2.60.7. tcp_flag_set (ID: 03300009)

Default Severity	WARNING
Log Message	The TCP <bad_flag> flag is set. Dropping
Explanation	The TCP flag is set. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.60.8. unexpected_tcp_flags (ID: 03300010)

Default Severity	WARNING
Log Message	Unexpected tcp flags <flags> from <endpoint> during state <state>. Dropping
Explanation	Received unexpected tcp flags during a specific state. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1

Parameters	flags endpoint state
Context Parameters	Rule Name Connection Packet Buffer

2.60.9. mismatched_syn_resent (ID: 03300011)

Default Severity	WARNING
Log Message	Mismatched syn "resent" with seq <seqno>, expected <origseqno>. Dropping
Explanation	Mismatching sequence number in re-sent SYN. Re-sent SYN packet must have identical sequence number as the original SYN. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno origseqno
Context Parameters	Rule Name Connection Packet Buffer

2.60.10. mismatched_first_ack_seqno (ID: 03300012)

Default Severity	WARNING
Log Message	ACK packet with seq <seqno>. Expected <expectseqno>. Dropping
Explanation	Mismatching sequence numbers. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno expectseqno
Context Parameters	Rule Name Connection Packet Buffer

2.60.11. mismatched_first_ack_seqno (ID: 03300013)

Default Severity	WARNING
Log Message	SYNACK packet with seq <seqno>. Expected <expectseqno>. Dropping
Explanation	Mismatching sequence numbers. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno expectseqno
Context Parameters	Rule Name Connection Packet Buffer

2.60.12. rst_out_of_bounds (ID: 03300015)

Default Severity	WARNING
Log Message	Originator RST seq <seqno> is not in window <winstart>...<winend>. Dropping
Explanation	The RST flag sequence number is not within the receiver window. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno winstart winend
Context Parameters	Rule Name Connection Packet Buffer

2.60.13. tcp_seqno_too_low (ID: 03300016)

Default Severity	DEBUG
Log Message	TCP sequence number <seqno> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable sequence number was received. The packet will be dropped.
Firewall Action	drop

Recommended Action	None.
Revision	2
Parameters	seqno accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.60.14. unacceptable_ack (ID: 03300017)

Default Severity	NOTICE
Log Message	TCP acknowledgement <ack> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable acknowledgement number was received during state SYN_SENT. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	ack accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.60.15. rst_without_ack (ID: 03300018)

Default Severity	NOTICE
Log Message	TCP RST segment without ACK during state SYN_SENT. Dropping
Explanation	A TCP segment with the RST flag but not the ACK flag was received during state SYN_SENT. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.60.16. tcp_seqno_too_high (ID: 03300019)

Default Severity	WARNING
Log Message	TCP sequence number <seqno> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable sequence number was received. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.60.17. tcp_recv_windows_drained (ID: 03300022)

Default Severity	CRITICAL
Log Message	Out of large TCP receive windows. Maximum windows: <max_windows>. Triggered <num_events> times last 10 seconds.
Explanation	The TCP stack could not accept incomming data since it has run out of large TCP receive windows. This event was triggered [num_events] times during the last 10 seconds.
Firewall Action	close
Recommended Action	If the system is configured to use TCP based ALGs, increase the amount of maximum sessions parameter on the associated service.
Revision	1
Parameters	max_windows [num_events]

2.60.18. tcp_snd_windows_drained (ID: 03300023)

Default Severity	CRITICAL
Log Message	Out of large TCP send windows. Maximum windows: <max_windows>. Triggered <num_events> times last 10 seconds.
Explanation	The TCP stack could not send data since it has run out of large TCP send windows. This event was triggered [num_events] times during

	the last 10 seconds.
Firewall Action	close
Recommended Action	If the system is configured to use TCP based ALGs, increase the amount of maximum sessions parameter on the associated service.
Revision	1
Parameters	max_windows [num_events]

2.60.19. tcp_get_freesocket_failed (ID: 03300024)

Default Severity	WARNING
Log Message	System was not able to get a free socket. Triggered <num_events> times last 10 seconds.
Explanation	The TCP stack could not get a free socket. This event was triggered [num_events] times during the last 10 seconds.
Firewall Action	None
Recommended Action	None.
Revision	1

2.60.20. tcp_seqno_too_low_with_syn (ID: 03300025)

Default Severity	DEBUG
Log Message	TCP sequence number <seqno> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable sequence number was received. The packet will be dropped.
Firewall Action	drop
Recommended Action	None.
Revision	2
Parameters	seqno accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.60.21. tcp_syn_fragmented (ID: 03300026)

Default Severity	NOTICE
Log Message	SYN packet is fragmented
Explanation	The SYN packet is fragmented. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.60.22. tcp_syn_fragmented (ID: 03300027)

Default Severity	NOTICE
Log Message	SYN packet is fragmented. Dropping
Explanation	The SYN packet is fragmented. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.60.23. tcp_syn_data (ID: 03300028)

Default Severity	NOTICE
Log Message	SYN packet contains data
Explanation	The SYN packet contains payload data. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.60.24. tcp_syn_data (ID: 03300029)

Default Severity	NOTICE
Log Message	SYN packet contains data. Dropping

Explanation	The SYN packet contains payload data. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.60.25. tcp_null_flags (ID: 03300030)

Default Severity	WARNING
Log Message	Packet has no SYN, ACK, FIN or RST flag set. Dropping
Explanation	The packet has no SYN, ACK, FIN or RST flag set. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.61. TCP_OPT

These log messages refer to the **TCP_OPT (Events concerning the TCP header options)** category.

2.61.1. tcp_mss_too_low (ID: 03400001)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too low. TCPMSSMin=<minmss>
Explanation	The TCP MSS is too low. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.61.2. tcp_mss_too_low (ID: 03400002)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too low. TCPMSSMin=<minmss>. Adjusting
Explanation	The TCP MSS is too low. Adjusting to use the configured minimum MSS.
Firewall Action	adjust
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.61.3. tcp_mss_too_high (ID: 03400003)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too high. TCPMSSMax=<maxmss>

Explanation	The TCP MSS is too high. Ignoring.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.61.4. tcp_mss_too_high (ID: 03400004)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too high. TCPMSSMax=<maxmss>. Adjusting
Explanation	The TCP MSS is too high. Adjusting to use the configured maximum MSS.
Firewall Action	adjust
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.61.5. tcp_mss_above_log_level (ID: 03400005)

Default Severity	NOTICE
Log Message	TCP MSS <mss> higher than log level. TCPMSSLogLevel=<mssloglevel>
Explanation	The TCP MSS is higher than the log level.
Firewall Action	log
Recommended Action	None.
Revision	1
Parameters	tcpopt mss mssloglevel
Context Parameters	Rule Name

Packet Buffer

2.61.6. tcp_option (ID: 03400006)

Default Severity	NOTICE
Log Message	Packet has a type <tcpopt> TCP option
Explanation	The packet has a TCP Option of the specified type. Ignoring.
Firewall Action	ignore
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.61.7. tcp_option_strip (ID: 03400007)

Default Severity	NOTICE
Log Message	Packet has a type <tcpopt> TCP option. Stripping it
Explanation	The packet has a TCP Option of the specified type. Removing it.
Firewall Action	strip
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.61.8. bad_tcpopt_length (ID: 03400010)

Default Severity	WARNING
Log Message	Type <tcpopt> is multibyte, available=<avail>. Dropping
Explanation	The TCP Option type is multi byte which requires two bytes, and there is less than two bytes available. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1

Parameters	tcpopt minoptlen avail
Context Parameters	Rule Name Packet Buffer

2.61.9. bad_tcpopt_length (ID: 03400011)

Default Severity	WARNING
Log Message	Type <tcpopt> claims length=<len> bytes, avail=<avail> bytes. Dropping
Explanation	The TCP Option type does not fit in the option space. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt len avail
Context Parameters	Rule Name Packet Buffer

2.61.10. bad_tcpopt_length (ID: 03400012)

Default Severity	WARNING
Log Message	Type <tcpopt>: bad length <optlen>. Expected <expectlen> bytes. Dropping
Explanation	The TCP Option type has an invalid length. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt optlen expectlen
Context Parameters	Rule Name Packet Buffer

2.61.11. tcp_mss_too_low (ID: 03400013)

Default Severity	WARNING
Log Message	TCP MSS <mss> too low. TCPMSSMin=<minmss>. Dropping
Explanation	The TCP MSS is too low. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.61.12. tcp_mss_too_high (ID: 03400014)

Default Severity	WARNING
Log Message	TCP MSS <mss> too high. TCPMSSMax=<maxmss>. Dropping
Explanation	The TCP MSS is too high. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.61.13. tcp_option_disallowed (ID: 03400015)

Default Severity	WARNING
Log Message	Packet has a <tcpopt> TCP option, which is disallowed. Dropping
Explanation	The packet has a TCP Option of the specified type. Dropping packet.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name

Packet Buffer

2.61.14. multiple_tcp_ws_options (ID: 03400017)

Default Severity	WARNING
Log Message	Multiple window scale options present in a single TCP segment
Explanation	Multiple TCP window scale options present in a single TCP segment.
Firewall Action	strip
Recommended Action	None.
Revision	1
Context Parameters	Connection Packet Buffer

2.61.15. too_large_tcp_window_scale (ID: 03400018)

Default Severity	WARNING
Log Message	TCP window scale option with shift count <shift_cnt> was received. The shift count will be lowered to 14.
Explanation	A TCP segment with a window scale option specifying a shift count that is larger than 14 was received. The shift count will be lowered to 14.
Firewall Action	adjust
Recommended Action	None.
Revision	1
Parameters	shift_cnt
Context Parameters	Connection Packet Buffer

2.61.16. mismatching_tcp_window_scale (ID: 03400019)

Default Severity	WARNING
Log Message	Mismatching TCP window scale shift count. Expected <old> got <new> will use <effective>
Explanation	TCP segment with a window scale option specifying a different shift count than previous segments was received. The lower of the two values will be used.
Firewall Action	adjust

Recommended Action	None.
Revision	1
Parameters	old new effective
Context Parameters	Connection Packet Buffer

2.62. TELEMETRY

These log messages refer to the **TELEMETRY (Telemetry)** category.

2.62.1. current_usage (ID: 08500001)

Default Severity	INFORMATIONAL
Log Message Explanation	This is telemetry data from a Core device.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	cpu conns memory volume

2.63. THRESHOLD

These log messages refer to the **THRESHOLD (Threshold rule events)** category.

2.63.1. conn_threshold_exceeded (ID: 05300100)

Default Severity	WARNING
Log Message	Connection threshold <description> exceeded <threshold>. Source IP: <srcip>. Closing connection
Explanation	The source ip is opening up new connections too fast.
Firewall Action	closing_connection
Recommended Action	Investigate worms and DoS attacks.
Revision	1
Parameters	description threshold srcip
Context Parameters	Rule Name

2.63.2. reminder_conn_threshold (ID: 05300101)

Default Severity	INFORMATIONAL
Log Message	Reminder: Connection threshold <description> exceeded <threshold>. Source IP: <srcip>.
Explanation	The source ip is still opening up new connections too fast.
Firewall Action	None
Recommended Action	Look through logs to see if the source ip has misbehaved in the past.
Revision	1
Parameters	description threshold srcip
Context Parameters	Rule Name

2.63.3. conn_threshold_exceeded (ID: 05300102)

Default Severity	NOTICE
Log Message	Connection threshold <description> exceeded <threshold>. Source IP: <srcip>
Explanation	The source ip is opening up new connections too fast.

Firewall Action	None
Recommended Action	Investigate worms and DoS attacks.
Revision	1
Parameters	description threshold srcip
Context Parameters	Rule Name

2.63.4. failed_to_keep_connection_count (ID: 05300200)

Default Severity	ERROR
Log Message	Failed to keep connection count. Reason: Out of memory
Explanation	The device was unable to allocate resources needed to include the connection in the connection count kept by threshold rules. The connection will not be included in the connection count.
Firewall Action	none
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Connection

2.63.5. failed_to_keep_connection_count (ID: 05300201)

Default Severity	ERROR
Log Message	Failed to keep connection count. Reason: Out of memory
Explanation	The device was unable to allocate resources needed to include the connection in the connection count kept by threshold rules. Since there exist protect actions that are triggered by thresholds on the number of connections, the connection will be closed.
Firewall Action	close
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Connection

2.63.6. threshold_conns_from_srcip_exceeded (ID: 05300210)

Default Severity	NOTICE
Log Message	The number of connections matching the rule and originating from

	<srcip> exceeds <threshold>.
Explanation	The number of connections matching the threshold rule and originating from a single host exceeds the configured threshold. Note: This log message is rate limited via an exponential back-off procedure.
Firewall Action	none
Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.63.7. threshold_conns_from_srcip_exceeded (ID: 05300211)

Default Severity	NOTICE
Log Message	The number of connections matching the rule and originating from <srcip> exceeds <threshold>.
Explanation	The number of connections matching the threshold rule and originating from a single host exceeds the configured threshold. The configured protective measures will be triggered. Note: This log message is rate limited via an exponential back-off procedure.
Firewall Action	protect
Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.63.8. threshold_conns_from_filter_exceeded (ID: 05300212)

Default Severity	NOTICE
Log Message	The number of connections matching the rule exceeds <threshold>. The Offending host is <srcip>.
Explanation	The number of connections matching the threshold rule exceeds the configured threshold. Note: This log message is rate limited via an exponential back-off procedure.
Firewall Action	none

Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.63.9. threshold_conns_from_filter_exceeded (ID: 05300213)

Default Severity	NOTICE
Log Message	The number of connections matching the rule exceeds <threshold>. The Offending host is <srcip>.
Explanation	The number of connections matching the threshold rule exceeds the configured threshold. The configured protective measures will be triggered. Note: This log message is rate limited via an exponential back-off procedure.
Firewall Action	protect
Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.64. TIMESYNC

These log messages refer to the **TIMESYNC (Firewall time synchronization events)** category.

2.64.1. synced_clock (ID: 03500001)

Default Severity	NOTICE
Log Message	The clock at <oldtime>, was off by <clockdrift> second(s) and synchronized with <timeserver> to <newtime>
Explanation	The clock has been synchronized with the time server.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	oldtime newtime clockdrift timeserver

2.64.2. failure_communicate_with_timeservers (ID: 03500002)

Default Severity	WARNING
Log Message	Communication with the timeserver(s) failed. Clock not updated.
Explanation	The unit failed to establish a connection with the time sync server. The clock has not been updated.
Firewall Action	clock_not_synced
Recommended Action	Verify that the time sync server is running.
Revision	1

2.64.3. clockdrift_too_high (ID: 03500003)

Default Severity	WARNING
Log Message	According to the timeserver the clock has drifted <clockdrift> seconds(s) which is NOT in the allowed correction interval (+/-<interval> seconds)
Explanation	The clock has drifted so much that it is not within the allowed +/- correction interval. The clock will not be updated.
Firewall Action	clock_not_synced
Recommended Action	If the correction interval is too narrow, it can be changed in the DateTime section.

Revision	2
Parameters	clockdrift timeserver interval

2.64.4. leaving_daylight_saving (ID: 03500010)

Default Severity	NOTICE
Log Message	Leaving Daylight saving time and switching to non-DST time zone.
Explanation	Automatic DST is activated and time is adjusted by the system.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	dstoffset nondstoffset

2.64.5. entering_daylight_saving (ID: 03500011)

Default Severity	NOTICE
Log Message	Leaving standart time zone and switching to Daylight saving time.
Explanation	Automatic DST is activated and time is adjusted by the system.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	dstoffset nondstoffset

2.64.6. dst_location_not_found (ID: 03500012)

Default Severity	ERROR
Log Message	Timezone could not be loaded from database.
Explanation	Required data for the chosen location could not be found in time zone database.
Firewall Action	None
Recommended Action	None.
Revision	1

Parameters location

2.65. TRANSPARENCY

These log messages refer to the **TRANSPARENCY (Events concerning the Transparent Mode feature)** category.

2.65.1. impossible_hw_sender_address (ID: 04400410)

Default Severity	WARNING
Log Message	Impossible hardware sender address 0000:0000:0000. Dropping.
Explanation	Some equipment on the network is sending packets with a source MAC address of 0000:0000:0000. These packets will be dropped.
Firewall Action	drop
Recommended Action	Investigate if there are equipment sending packets using 0000:0000:0000 as source MAC address. If there are, try to change the behaviour of that equipment.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.65.2. enet_hw_sender_broadcast (ID: 04400411)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a broadcast address. Accepting.
Explanation	The Ethernet hardware sender address is a broadcast address. The packet will be accepted.
Firewall Action	accept
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.65.3. enet_hw_sender_broadcast (ID: 04400412)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a broadcast address. Rewriting to the address of the forwarding interface.
Explanation	The Ethernet hardware sender address is a broadcast address. The packet will be rewritten with the hardware sender address of the forwarding interface.

Firewall Action	rewrite
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.65.4. enet_hw_sender_broadcast (ID: 04400413)

Default Severity	WARNING
Log Message	Ethernet hardware sender is a broadcast address. Dropping.
Explanation	The Ethernet hardware sender address is a broadcast address. The packet will be dropped.
Firewall Action	drop
Recommended Action	Investigate if there are equipment sending packets using a broadcast address as sender MAC address. If there are, try to change the behaviour of that equipment.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.65.5. enet_hw_sender_multicast (ID: 04400414)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a multicast address. Accepting.
Explanation	The Ethernet hardware sender address is a multicast address. The packet will be accepted.
Firewall Action	accept
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.65.6. enet_hw_sender_multicast (ID: 04400415)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a multicast address. Rewriting to the address of the forwarding interface.

Explanation The Ethernet hardware sender address is a multicast address. The packet will be rewritten with the hardware sender address of the forwarding interface.

Firewall Action rewrite

Recommended Action None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.65.7. enet_hw_sender_multicast (ID: 04400416)

Default Severity WARNING

Log Message Ethernet hardware sender is a multicast address. Dropping.

Explanation The Ethernet hardware sender address is a multicast address. The packet will be dropped.

Firewall Action drop

Recommended Action Investigate if there are equipment sending packets using a multicast address as sender MAC address. If there are, try to change the behaviour of that equipment.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.65.8. relay_stp_frame (ID: 04400417)

Default Severity INFORMATIONAL

Log Message Relaying STP frame from <recvif> to switched interfaces

Explanation An incoming STP frame has been relayed to all switched interfaces in the same switch route as [recif].

Firewall Action allow

Recommended Action None.

Revision 1

Parameters recvif

2.65.9. dropped_stp_frame (ID: 04400418)

Default Severity INFORMATIONAL

Log Message	Dropping STP frame from <recvif>
Explanation	An incoming STP frame has been dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	recvif

2.65.10. invalid_stp_frame (ID: 04400419)

Default Severity	WARNING
Log Message	Incoming STP frame from <recvif> dropped. Reason: <reason>
Explanation	An incoming Spanning-Tree frame has been dropped since it is either malformed or its type is unknown. Supported Spanning-Tree versions are STP, RSTP, MSTP and PVST+.
Firewall Action	drop
Recommended Action	If the frame format is invalid, locate the unit which is sending the malformed frame.
Revision	1
Parameters	recvif reason

2.65.11. relay_mpls_frame (ID: 04400420)

Default Severity	INFORMATIONAL
Log Message	Forwarding MPLS packet from <recvif>.
Explanation	An incoming MPLS packet has been forwarded through the firewall. [destif] indicates if it was forwarded to an ultimate destination or if it was broadcasted to over all interfaces in the switch group.
Firewall Action	allow
Recommended Action	None.
Revision	2
Parameters	recvif destif

2.65.12. dropped_mpls_packet (ID: 04400421)

Default Severity	INFORMATIONAL

Log Message	Dropping MPLS packet from <recvif>
Explanation	An incoming MPLS packet has been dropped.
Firewall Action	drop
Recommended Action	None.
Revision	1
Parameters	recvif

2.65.13. invalid_mpls_packet (ID: 04400422)

Default Severity	WARNING
Log Message	Incoming MPLS packet on <recvif> dropped. Reason: <reason>
Explanation	An incoming MPLS packet has been dropped since it was malformed.
Firewall Action	drop
Recommended Action	If the packet format is invalid, locate the unit which is sending the malformed packet.
Revision	1
Parameters	recvif reason

2.66. USERAUTH

These log messages refer to the **USERAUTH (User authentication (e.g. RADIUS) events)** category.

2.66.1. accounting_start (ID: 03700001)

Default Severity	INFORMATIONAL
Log Message	Successfully received RADIUS Accounting START response from RADIUS Accounting server
Explanation	The unit received a valid response to an Accounting-Start event from the Accounting Server.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.2. invalid_accounting_start_server_response (ID: 03700002)

Default Severity	WARNING
Log Message	Received a RADIUS Accounting START response with an Identifier mismatch. Ignoring this packet
Explanation	The unit received a response with an invalid Identifier mismatch. This can be the result of a busy network, causing accounting event re-sends. This will be ignored.
Firewall Action	ignore_packet
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.3. no_accounting_start_server_response (ID: 03700003)

Default Severity	ALERT
Log Message	Did not receive a RADIUS Accounting START response. Accounting has been disabled
Explanation	The unit did not receive a response to an Accounting-Start event from the Accounting Server. Accounting features will be disabled.

Firewall Action	accounting_disabled
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	2
Context Parameters	User Authentication

2.66.4. invalid_accounting_start_server_response (ID: 03700004)

Default Severity	ALERT
Log Message	Received an invalid RADIUS Accounting START response from RADIUS Accounting server. Accounting has been disabled
Explanation	The unit received an invalid response to an Accounting-Start event from the Accounting Server Accounting features will be disabled.
Firewall Action	accounting_disabled
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	2
Context Parameters	User Authentication

2.66.5. no_accounting_start_server_response (ID: 03700005)

Default Severity	WARNING
Log Message	Logging out the authenticated user, as no RADIUS Accounting START response was received from RADIUS Accounting server
Explanation	The authenticated user is logged out as no response to the Accounting-Start event was received from the Accounting Server.
Firewall Action	logout_user
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	2
Context Parameters	User Authentication

2.66.6. invalid_accounting_start_server_response (ID: 03700006)

Default Severity	WARNING

Log Message	Logging out the authenticated user, as an invalid RADIUS Accounting START response was received from RADIUS Accounting server
Explanation	The authenticated user is logged out as an invalid response to the Accounting-Start event was received from the Accounting Server.
Firewall Action	logout_user
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	2
Context Parameters	User Authentication

2.66.7. failed_to_send_accounting_stop (ID: 03700007)

Default Severity	ALERT
Log Message	Failed to send Accounting STOP to Authentication Server. Accounting information will not be sent to Authentication Server.
Explanation	The unit failed to send an Accounting-Stop event to the Accounting Server. Accounting information will not be sent to the Accounting Server.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.8. accounting_stop (ID: 03700008)

Default Severity	NOTICE
Log Message	Successfully received RADIUS Accounting STOP response from RADIUS Accounting server. Bytes sent=<bytessent>, Bytes recv=<bytesrecv>, Packets sent=<packetssent>, Packets recv=<packetsrecv>, Session time=<sestime>
Explanation	The unit received a valid response to an Accounting-Stop event from the Accounting Server.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	bytessent bytesrecv packetssent packetsrecv

gigawrapsent
gigawraprecv
sestime

Context Parameters User Authentication

2.66.9. invalid_accounting_stop_server_response (ID: 03700009)

Default Severity WARNING

Log Message Received a RADIUS Accounting STOP response with an Identifier mismatch. Ignoring this packet

Explanation The unit received a response with an invalid Identifier mismatch. This can be the result of a busy network, causing accounting event re-sends. This will be ignored.

Firewall Action ignore_packet

Recommended Action None.

Revision 2

Context Parameters User Authentication

2.66.10. no_accounting_stop_server_response (ID: 03700010)

Default Severity ALERT

Log Message Did not receive a RADIUS Accounting STOP response. User statistics might not have been updated on the Accounting Server

Explanation The unit did not receive a response to an Accounting-Stop event from the Accounting Server. Accounting information might not have been propery received by the Accounting Server.

Firewall Action None

Recommended Action Verify that the RADIUS Accounting server daemon is running on the Accounting Server.

Revision 2

Context Parameters User Authentication

2.66.11. invalid_accounting_stop_server_response (ID: 03700011)

Default Severity ALERT

Log Message Received an invalid RADIUS Accounting STOP response from RADIUS

	Accounting server. User statistics might not have been updated on the Accounting Server
Explanation	The unit received an invalid response to an Accounting-Stop event from the Accounting Server. Accounting information might not have been propery received by the Accounting Server.
Firewall Action	None
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	2
Context Parameters	User Authentication

2.66.12. failure_init_radius_accounting (ID: 03700012)

Default Severity	ALERT
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accounting will be disabled
Explanation	The unit failed to send an Accounting-Start event to the Accounting Server. Accounting features will be disabled.
Firewall Action	accounting_disabled
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.13. invalid_accounting_start_request (ID: 03700013)

Default Severity	WARNING
Log Message	Logging out the authenticated user, as a RADIUS Accounting START request could not be sent to the RADIUS Accounting server
Explanation	The authenticated user is logged out as an Accounting-Start request did not get sent to the Accounting Server. This could be a result of missing a route from the unit to the Accounting Server.
Firewall Action	logout_user
Recommended Action	Verify that a route exists from the unit to the RADIUS Accounting server, and that it is properly configured.
Revision	2
Context Parameters	User Authentication

2.66.14. no_accounting_start_server_response (ID: 03700014)

Default Severity	ALERT
Log Message	Did not send a RADIUS Accounting START request. Accounting has been disabled
Explanation	The unit did not send an Accounting-Start event to the Accounting Server. Accounting features will be disabled. This could be a result of missing a route from the unit to the Accounting Server.
Firewall Action	accounting_disabled
Recommended Action	Verify that a route exists from the unit to the RADIUS Accounting server, and that it is properly configured.
Revision	2
Context Parameters	User Authentication

2.66.15. user_timeout (ID: 03700020)

Default Severity	NOTICE
Log Message	User timeout expired, user is automatically logged out
Explanation	The user is automatically logged out, as the configurated timeout expired.
Firewall Action	user_removed
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.16. group_list_too_long (ID: 03700030)

Default Severity	WARNING
Log Message	User <username> belongs in too many groups, keeping the 32 first groups
Explanation	A username can only be a member of a maximum of 32 groups. This username is a member of too many groups, and only the 32 first groups will be used.
Firewall Action	truncating_group_list
Recommended Action	Lower the number of groups that this user belongs to.
Revision	1
Parameters	username

2.66.17. accounting_alive (ID: 03700050)

Default Severity NOTICE

Log Message Successfully received RADIUS Accounting Interim response from RADIUS Accounting server. Bytes sent=<bytessent>, Bytes recv=<bytesrecv>, Packets sent=<packetssent>, Packets recv=<packetsrecv>, Session time=<sestime>

Explanation The unit successfully received a RADIUS Accounting Interim response to an Accounting-Interim request event from the Accounting Server. Accounting information has been updated on the Accounting Server.

Firewall Action None

Recommended Action None.

Revision 2

Parameters bytessent
bytesrecv
packetssent
packetsrecv
gigawrapsent
gigawraprecv
sestime

Context Parameters User Authentication

2.66.18. accounting_interim_failure (ID: 03700051)

Default Severity ALERT

Log Message Failed to send Accounting Interim to Authentication Server. Accounting information might not be properly updated on the Accounting Server.

Explanation The unit failed to send an Accounting-Interim event to the Accounting Server. The statistics on the Accounting Server might not have been properly synchronized.

Firewall Action None

Recommended Action Verify that the RADIUS Accounting server daemon is running on the Accounting Server.

Revision 2

Context Parameters User Authentication

2.66.19. no_accounting_interim_server_response (ID: 03700052)

Default Severity	ALERT
Log Message	Did not receive a RADIUS Accounting Interim response. User statistics might not have been updated on the Accounting Server
Explanation	The unit did not receive a response to an Accounting-Interim event from the Accounting Server. Accounting information might not have been propery received by the Accounting Server.
Firewall Action	None
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	2
Context Parameters	User Authentication

2.66.20. invalid_accounting_interim_server_response (ID: 03700053)

Default Severity	ALERT
Log Message	Received an invalid RADIUS Accounting Interim response from RADIUS Accounting server. User statistics might not have been updated on the Accounting Server
Explanation	The unit received an invalid response to an Accounting-Interm event from the Accounting Server. Accounting information might not have been propery received by the Accounting Server.
Firewall Action	None
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	2
Context Parameters	User Authentication

2.66.21. invalid_accounting_interim_server_response (ID: 03700054)

Default Severity	WARNING
Log Message	Received a RADIUS Accounting Interim response with an Identifier mismatch. Ignoring this packet
Explanation	The unit received a response with an invalid Identifier mismatch. This can be the result of a busy network, causing accounting event re-sends. This will be ignored.
Firewall Action	ignore_packet
Recommended Action	None.

Revision	2
Context Parameters	User Authentication

2.66.22. relogin_from_new_srcip (ID: 03700100)

Default Severity	WARNING
Log Message	User with the same username is logging in from another IP address, logging out current instance
Explanation	A user with the same username as an already authenticated user is logging in. The current instance is logged out.
Firewall Action	logout_current_user
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.23. already_logged_in (ID: 03700101)

Default Severity	WARNING
Log Message	This user is already logged in
Explanation	A user with the same username as an already authenticated user tried to logged in, and was rejected .
Firewall Action	disallowed_login
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.24. user_login (ID: 03700102)

Default Severity	NOTICE
Log Message	User logged in. Idle timeout: <idle_timeout>, Session timeout: <session_timeout>
Explanation	A user logged in and has been granted access, according to the group membership or user name information.
Firewall Action	None
Recommended Action	None.
Revision	2

Parameters	idle_timeout session_timeout [groups]
Context Parameters	User Authentication

2.66.25. bad_user_credentials (ID: 03700104)

Default Severity	NOTICE
Log Message	Unknown user or invalid password
Explanation	A user failed to log in. The entered username or password was invalid.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.26. radius_auth_timeout (ID: 03700105)

Default Severity	ALERT
Log Message	Timeout during RADIUS user authentication, contact with RADIUS server not established
Explanation	The unit did not receive a response from the RADIUS Authentication server, and the authentication process failed.
Firewall Action	None
Recommended Action	Verify that the RADIUS Authentication server daemon is running on the Authenication Server.
Revision	2
Context Parameters	User Authentication

2.66.27. manual_logout (ID: 03700106)

Default Severity	NOTICE
Log Message	User manually logged out
Explanation	A user manually logged out, and is no longer authenticated.
Firewall Action	None
Recommended Action	None.

Revision	2
Context Parameters	User Authentication

2.66.28. userauthrules_disallowed (ID: 03700107)

Default Severity	WARNING
Log Message	Denied access according to UserAuthRules rule-set
Explanation	The user is not allowed to authenticate according to the UserAuthRules rule-set.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.29. ldap_auth_error (ID: 03700109)

Default Severity	ALERT
Log Message	Error during LDAP user authentication, contact with LDAP server not established
Explanation	The unit did not receive a response from the LDAP Authentication server, and the authentication process failed.
Firewall Action	None
Recommended Action	Verify that the LDAP Authentication server daemon is running on the Authenication Server.
Revision	2
Context Parameters	User Authentication

2.66.30. user_logout (ID: 03700110)

Default Severity	NOTICE
Log Message	User logged out
Explanation	A user logged out, and is no longer authenticated.
Firewall Action	None
Recommended Action	None.
Revision	2

Context Parameters	User Authentication

2.66.31. ldap_session_new_out_of_memory (ID: 03700401)

Default Severity	ALERT
Log Message	Out of memory while trying to allocate new LDAP session
Explanation	The unit failed to allocate a LDAP session, as it is out of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.66.32. cant_create_new_request (ID: 03700402)

Default Severity	ERROR
Log Message	Can't create new user request. Authentication aborted
Explanation	Can't create new user request.
Firewall Action	authentication_failed
Recommended Action	Check LDAP context to work.
Revision	1

2.66.33. ldap_user_authentication_successful (ID: 03700403)

Default Severity	NOTICE
Log Message	LDAP Authentication successful for <user>
Explanation	Authentication attempt successful.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	user

2.66.34. ldap_user_authentication_failed (ID: 03700404)

Default Severity	NOTICE

Log Message	LDAP Authentication failed for <user>
Explanation	Authentication attempt failed.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	user

2.66.35. ldap_context_new_out_of_memory (ID: 03700405)

Default Severity	ALERT
Log Message	Out of memory while trying to allocate new LDAP Context
Explanation	The unit failed to allocate a LDAP Context, as it is out of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.66.36. user_req_new_out_of_memory (ID: 03700406)

Default Severity	ALERT
Log Message	Out of memory while trying to allocate new User Request
Explanation	The unit failed to allocate a User Request, as it is out of memory.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.66.37. failed_admin_bind (ID: 03700407)

Default Severity	ALERT
Log Message	Cannot bind to LDAP database <database>
Explanation	Cannot bind the the LDAP database using the configured username and password.
Firewall Action	database connection disabled

Recommended Action	Check configuration.
Revision	1
Parameters	database

2.66.38. invalid_username_or_password (ID: 03700408)

Default Severity	ERROR
Log Message	Invalid provided username or password
Explanation	Username or password does not contain any information.
Firewall Action	authentication_failed
Recommended Action	Verify connecting client username and password.
Revision	1

2.66.39. failed_retrieve_password (ID: 03700409)

Default Severity	ALERT
Log Message	Cannot retrieve user password from LDAP database <database>
Explanation	Cannot retrive the user password from LDAP database making user authentication impossible.
Firewall Action	user authentication failed
Recommended Action	Check configuration for password attribute.
Revision	1
Parameters	database

2.66.40. ldap_timed_out_server_request (ID: 03700423)

Default Severity	NOTICE
Log Message	LDAP timed out server request
Explanation	LDAP timed out server request.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	SessionID user ldap_server_ip

2.66.41. ldap_no_working_server_found (ID: 03700424)

Default Severity	NOTICE
Log Message	LDAP no working server found
Explanation	LDAP no working server found.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	SessionID user

2.66.42. no_shared_ciphers (ID: 03700500)

Default Severity	ERROR
Log Message	SSL Handshake: No shared ciphers exists. Closing down SSL connection
Explanation	No shared ciphers were found between the client and the unit, and the SSL connection can not be established.
Firewall Action	ssl_close
Recommended Action	Make sure that the client and unit share atleast one cipher.
Revision	1
Parameters	client_ip

2.66.43. disallow_clientkeyexchange (ID: 03700501)

Default Severity	ERROR
Log Message	SSL Handshake: Disallow ClientKeyExchange. Closing down SSL connection
Explanation	The SSL connection will be closed because there are not enough resources to process any ClientKeyExchange messages at the moment. This could be a result of SSL handshake message flooding. This action is triggered by a system that monitors the amount of resources that is spent on key exchanges. This system is controlled by the advanced setting SSL_ProcessingPriority.
Firewall Action	ssl_close
Recommended Action	Investigate the source of this, and try to find out if it is a part of a possible attack, or normal traffic.

Revision	2
Parameters	client_ip

2.66.44. bad_packet_order (ID: 03700502)

Default Severity	ERROR
Log Message	Bad SSL Handshake packet order. Closing down SSL connection
Explanation	Two or more SSL Handshake message were received in the wrong order, and the SSL connection is closed.
Firewall Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.66.45. bad_clienthello_msg (ID: 03700503)

Default Severity	ERROR
Log Message	SSL Handshake: Bad ClientHello message. Closing down SSL connection
Explanation	The ClientHello message (which is the first part of a SSL handshake) is invalid, and the SSL connection is closed.
Firewall Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.66.46. bad_changecipher_msg (ID: 03700504)

Default Severity	ERROR
Log Message	SSL Handshake: Bad ChangeCipher message. Closing down SSL connection
Explanation	The ChangeCipher message (which is a part of a SSL handshake) is invalid, and the SSL connection is closed.
Firewall Action	ssl_close
Recommended Action	None.
Revision	1

Parameters client_ip

2.66.47. bad_clientkeyexchange_msg (ID: 03700505)

Default Severity ERROR

Log Message SSL Handshake: Bad ClientKeyExchange message. Closing down SSL connection

Explanation The ClientKeyExchange message (which is a part of a SSL handshake) is invalid, and the SSL connection is closed.

Firewall Action ssl_close

Recommended Action None.

Revision 1

Parameters client_ip

2.66.48. bad_clientfinished_msg (ID: 03700506)

Default Severity ERROR

Log Message SSL Handshake: Bad ClientFinished message. Closing down SSL connection

Explanation The ClientFinished message (which is a part of a SSL handshake) is invalid, and the SSL connection is closed.

Firewall Action ssl_close

Recommended Action None.

Revision 1

Parameters client_ip

2.66.49. bad_alert_msg (ID: 03700507)

Default Severity ERROR

Log Message Bad Alert message. Closing down SSL connection

Explanation The Alert message (which can be a part of a SSL handshake) is invalid, and the SSL connection is closed.

Firewall Action ssl_close

Recommended Action None.

Revision 1

Parameters client_ip

2.66.50. unknown_ssl_error (ID: 03700508)

Default Severity	ERROR
Log Message	Unknown SSL error. Closing down SSL connection
Explanation	An unknown error occured in the SSL connection, and the SSL connection is closed.
Firewall Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.66.51. negotiated_cipher_does_not_permit_the_chosen_certificate_size (ID: 03700509)

Default Severity	ERROR
Log Message	The negotiated cipher does not permit the chosen certificate size. Closing down SSL connection
Explanation	The negotiated cipher was an export cipher, which does not allow the chosen certification size. The certificate can not be sent, and the SSL connection is closed.
Firewall Action	ssl_close
Recommended Action	Change ciphers and/or certificate.
Revision	1
Parameters	client_ip

2.66.52. received_sslalert (ID: 03700510)

Default Severity	ERROR
Log Message	Received SSL Alert. Closing down SSL connection
Explanation	A SSL Alert message was received during an established SSL connection, and the SSL connection will be closed.
Firewall Action	close
Recommended Action	None.
Revision	1
Parameters	client_ip level

description

2.66.53. sent_sslalert (ID: 03700511)

Default Severity	ERROR
Log Message	Sent SSL Alert. Closing down SSL connection
Explanation	The unit has sent a SSL Alert message to the client, due to some abnormal event. The connection will be closed down.
Firewall Action	close
Recommended Action	Consult the "description" parameter, which contains the reason for this.
Revision	1
Parameters	client_ip level description

2.66.54. user_login (ID: 03707000)

Default Severity	NOTICE
Log Message	User logged in. Idle timeout: <idle_timeout>, Session timeout: <session_timeout>
Explanation	A user logged in and has been granted access. Auth Rule grants immediate access.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	idle_timeout session_timeout
Context Parameters	User Authentication

2.66.55. userauthrules_disallowed (ID: 03707001)

Default Severity	WARNING
Log Message	Denied access according to UserAuthRules rule-set
Explanation	The user is not allowed to authenticate according to the UserAuthRules rule-set.
Firewall Action	None

Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.56. user_login (ID: 03707002)

Default Severity	NOTICE
Log Message	User logged in. Idle timeout: <idle_timeout>, Session timeout: <session_timeout>
Explanation	A user logged in and has been granted access. The MAC address has been found.
Firewall Action	None
Recommended Action	None.
Revision	2
Parameters	idle_timeout session_timeout
Context Parameters	User Authentication

2.66.57. bad_user_credentials (ID: 03707003)

Default Severity	NOTICE
Log Message	Unknown user
Explanation	A user failed to log in. The MAC address does not exist.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.66.58. ldap_auth_error (ID: 03707004)

Default Severity	ALERT
Log Message	Error during LDAP user authentication, contact with LDAP server not established
Explanation	The unit did not receive a response from the LDAP Authentication server, and the authentication process failed.
Firewall Action	None

Recommended Action	Verify that the LDAP Authentication server daemon is running on the Authenication Server.
Revision	2
Context Parameters	User Authentication

2.66.59. bad_user_credentials (ID: 03707005)

Default Severity	NOTICE
Log Message	Unknown user
Explanation	A user failed to log in.
Firewall Action	None
Recommended Action	None.
Revision	2
Context Parameters	User Authentication

2.67. VFS

These log messages refer to the **VFS (VFS file handling events)** category.

2.67.1. odm_execute_failed (ID: 05200001)

Default Severity	NOTICE
Log Message	Usage of file "<filename>" failed. File validated as "<description>".
Explanation	An uploaded file ([filename]) was validated as "[description]". An error occured while using this file.
Firewall Action	None
Recommended Action	Check the origin of the file and make sure that the file is of the correct format.
Revision	2
Parameters	filename description reason

2.67.2. odm_execute_action_reboot (ID: 05200002)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) was validated as "<description>". Rebooting system.
Explanation	An uploaded file was validated, and executed. The system will now reboot.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	filename description

2.67.3. odm_execute_action_reconfigure (ID: 05200003)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) was validated as "<description>". Doing system RECONFIGURE .
Explanation	An uploaded file was validated, and executed. The system will now RECONFIGURE.
Firewall Action	None

Recommended Action	None.
Revision	1
Parameters	filename description

2.67.4. odm_execute_action_none (ID: 05200004)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) could not be recognized as a known type.
Explanation	An uploaded file could not be recognized as a known type.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	filename description

2.67.5. pkg_execute_fail (ID: 05200005)

Default Severity	WARNING
Log Message	Uploaded package file (<filename>) could not be executed correctly.
Explanation	An uploaded file was validated but could not be executed correctly. This could be because the unit is out of disk space or that the disk is corrupt.
Firewall Action	None
Recommended Action	Check that the disk is intact and that it has enough space.
Revision	1
Parameters	filename

2.67.6. upload_certificate_fail (ID: 05200006)

Default Severity	NOTICE
Log Message	Certificate data in file <filename>, could not be added to the configuration
Explanation	Certificate data could not be added to the configuration.
Firewall Action	None

Recommended Action	Make sure that the certificate data is of the correct format.
Revision	1
Parameters	filename

2.67.7. upload_certificate_fail (ID: 05200007)

Default Severity	NOTICE
Log Message	Certificate data in file <filename>, could not be added to the configuration
Explanation	Certificate data could not be added to the configuration.
Firewall Action	None
Recommended Action	Make sure that the certificate data is of the correct format.
Revision	1
Parameters	filename

2.67.8. odm_license_warn (ID: 05200008)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) was validated as "<description>". Warned user to take action.
Explanation	A license file was validated, and executed. Warned user to take action.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	filename description

2.67.9. secaas_lic_installed (ID: 05208002)

Default Severity	NOTICE
Log Message	License file has been installed. Doing system RECONFIGURE.
Explanation	License file has been validated, and installed. The system will now RECONFIGURE.
Firewall Action	None
Recommended Action	None.

Revision	1

2.67.10. secaas_lic_installation_failed (ID: 05208003)

Default Severity	EMERGENCY
Log Message	License file could not be installed.
Explanation	None.
Firewall Action	None
Recommended Action	None.
Revision	1

2.68. ZEROTOUCH

These log messages refer to the **ZEROTOUCH (ZeroTouch)** category.

2.68.1. zerotouch_disabled (ID: 08600900)

Default Severity	WARNING
Log Message	ZeroTouch is now disabled. Reason: <reason>
Explanation	The Zerotouch system has been disabled.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.68.2. netconpsk_generated (ID: 08600901)

Default Severity	INFORMATIONAL
Log Message	Netcon PSK Generated.
Explanation	The Netcon PSK for ZeroTouch configuration has been successfully generated.
Firewall Action	None
Recommended Action	None.
Revision	1

2.68.3. deviceid_generated (ID: 08600902)

Default Severity	INFORMATIONAL
Log Message	Device ID Generated.
Explanation	The Device ID for ZeroTouch configuration has been successfully generated.
Firewall Action	None
Recommended Action	None.
Revision	1

2.68.4. mgmt_ip_found (ID: 08600903)

Default Severity	INFORMATIONAL
Log Message	Management IP address received: <ipaddr>.
Explanation	The Management server's IP address has been successfully received.
Firewall Action	None
Recommended Action	None.
Revision	1
Parameters	ipaddr

2.68.5. mgmt_ip_resolve_failed (ID: 08600904)

Default Severity	INFORMATIONAL
Log Message	Management IP address failed to resolve.
Explanation	Unable to resolve the Management server's IP address. Retrying.
Firewall Action	None
Recommended Action	Check routable DNS servers are configured for this device.
Revision	1

2.68.6. mgmt_ip_query_failed (ID: 08600905)

Default Severity	INFORMATIONAL
Log Message	Management IP address query failed to start.
Explanation	Unable to start query for the Management server's IP address. Retrying.
Firewall Action	None
Recommended Action	Check DNS servers are configured for the device.
Revision	1

2.69. ZONEDEFENSE

These log messages refer to the **ZONEDEFENSE (ZoneDefense events)** category.

2.69.1. unable_to_allocate_send_entries (ID: 03800001)

Default Severity	WARNING
Log Message	Unable to allocate send entry. Sending of request to <switch> abandoned.
Explanation	Unable to allocate send entry. Unit is low on RAM.
Firewall Action	no_msg_sent
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	switch

2.69.2. unable_to_allocate_exclude_entry (ID: 03800002)

Default Severity	WARNING
Log Message	Unable to allocate exclude entry for <host>.
Explanation	Unable to allocate exclude entry. Unit is low on memory.
Firewall Action	no_exclude
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	host

2.69.3. unable_to_allocate_block_entry (ID: 03800003)

Default Severity	WARNING
Log Message	Unable to allocate block entry. Host <host> remains unblocked.
Explanation	Unable to allocate block entry. Unit is low on memory.
Firewall Action	no_block
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	host

2.69.4. switch_out_of_ip_profiles (ID: 03800004)

Default Severity	WARNING
Log Message	Unable to accommodate block request since out of IP profiles on <switch>.
Explanation	There are no free IP profiles left on the switch. No more hosts can be be blocked/excluded on this switch.
Firewall Action	no_block
Recommended Action	Check if it is possible to unblock some hosts.
Revision	1
Parameters	switch

2.69.5. out_of_mac_profiles (ID: 03800005)

Default Severity	WARNING
Log Message	Unable to accommodate block request since out of MAC profiles on <switch>.
Explanation	There are no free MAC profiles left on the switch. No more hosts can be be blocked/excluded on this switch.
Firewall Action	no_block
Recommended Action	None.
Revision	1
Parameters	switch

2.69.6. failed_to_create_profile (ID: 03800006)

Default Severity	CRITICAL
Log Message	Failed to create <type> profile <profile> on <switch>.
Explanation	The switch returned an error while creating a profile on the switch.
Firewall Action	no_profile
Recommended Action	Verify that the configured switch model is correct.
Revision	1
Parameters	type profile switch

2.69.7. no_response_trying_to_create_rule (ID: 03800007)

Default Severity	CRITICAL
Log Message	No response from switch <switch> while trying to create <type> rule in profile <profile>.
Explanation	Several attempts to create a rule in the switch has timed out. No more attempts will be made.
Firewall Action	no_rule
Recommended Action	Verify that the firewall is able to communicate with the switch.
Revision	1
Parameters	type profile switch

2.69.8. failed_writing_zonededense_state_to_media (ID: 03800008)

Default Severity	CRITICAL
Log Message	Failed to write ZoneDefense state to media.
Explanation	Failed to write list of ZoneDefense state to media. The media might be corrupt.
Firewall Action	None
Recommended Action	Verify that the media is intact.
Revision	1

2.69.9. failed_to_create_access_rule (ID: 03800009)

Default Severity	CRITICAL
Log Message	Failed to create <ruletype> access rule to add <network> on <switch>.
Explanation	The switch returned an error while creating a rule.
Firewall Action	None
Recommended Action	Verify that the configured switch model is correct.
Revision	1
Parameters	ruletype network switch

2.69.10. no_response_trying_to_erase_profile (ID: 03800010)

Default Severity	CRITICAL
Log Message	No response from switch <switch> while trying to erase <type> profile <profile>.
Explanation	Several attempts to erase a profile in the switch has timed out. No more attempts will be made.
Firewall Action	None
Recommended Action	Verify that the firewall is able to communicate with the switch.
Revision	1
Parameters	type profile switch

2.69.11. failed_to_erase_profile (ID: 03800011)

Default Severity	CRITICAL
Log Message	Failed to erase <type> profile <profile> on <switch>.
Explanation	The switch returned an error while erasing a profile.
Firewall Action	None
Recommended Action	Verify that the configured switch model is correct.
Revision	1
Parameters	type profile switch

2.69.12. failed_to_save_configuration (ID: 03800012)

Default Severity	CRITICAL
Log Message	Failed to save configuration on <switch>.
Explanation	The switch returned an error while saving the configuration.
Firewall Action	None
Recommended Action	Verify that the configured switch model is correct.
Revision	1
Parameters	switch

2.69.13. timeout_saving_configuration (ID: 03800013)

Default Severity	CRITICAL
Log Message	Timeout to save configuration on <switch>.
Explanation	Several attempts to save the configuration in the switch has timed out. No more attempts will be made.
Firewall Action	None
Recommended Action	Verify that the firewall is able to communicate with the switch.
Revision	1
Parameters	switch

2.69.14. zd_block (ID: 03800014)

Default Severity	WARNING
Log Message	ZoneDefense blocking host <host>. Alert Type: <type>.
Explanation	A configured action of type [type] has triggered ZoneDefense to block the host [host] at the configured ZoneDefense switches.
Firewall Action	block
Recommended Action	Unblock the specified host using the ZoneDefense status page to allow the host to regain access to the network.
Revision	1
Parameters	type host

2.69.15. mac_address_blocking_not_supported (ID: 03800015)

Default Severity	WARNING
Log Message	Unable to accommodate block request since MAC address blocking is not supported.
Explanation	This switch implements universal MIB that does not support MAC address blocking.
Firewall Action	no_block
Recommended Action	None.
Revision	1
Parameters	switch mac

2.69.16. zonedefense_table_exhausted (ID: 03800016)

Default Severity	WARNING
Log Message	Unable to accommodate block request since free space in Zone Defense table is exhausted.
Explanation	Number of free row in Zone Defense table is 0. Can not block more hosts.
Firewall Action	no_block
Recommended Action	Unblocking of the host can make a room in Zone Defense table.
Revision	1
Parameters	switch

2.69.17. zonedefense_disabled (ID: 03800017)

Default Severity	WARNING
Log Message	ZoneDefense is disabled on <switch>. The system will try to enable it.
Explanation	The switch responded that it has the ZoneDefense feature disabled. System will try once to enable it.
Firewall Action	enabling_zonedefense
Recommended Action	None.
Revision	1
Parameters	switch

2.69.18. zonedefense_enabled (ID: 03800018)

Default Severity	NOTICE
Log Message	ZoneDefense has been successfully enabled on <switch>.
Explanation	The system has successfully enabled ZoneDefense on the switch. No manual action is needed.
Firewall Action	getting_acl_number
Recommended Action	None.
Revision	1
Parameters	switch

2.69.19. enabling_zonedefense_failed (ID: 03800019)

Default Severity	CRITICAL
Log Message	ZoneDefense has failed to be enabled on <switch>.
Explanation	An attempt to automatically enable the ZoneDefense feaure has been made but failed. No further attempts will be made.
Firewall Action	None
Recommended Action	Enable the ZoneDefense feature on the switch manually.
Revision	1
Parameters	switch

2.69.20. zd_unblock (ID: 03800911)

Default Severity	INFORMATIONAL
Log Message	ZoneDefense unblocking <unblock_type> blocked host <host>.
Explanation	A dynamically blocked host has been unblocked by ZoneDefense.
Firewall Action	unblock
Recommended Action	None.
Revision	1
Parameters	host type unblock_type

2.69.21. zd_unblock (ID: 03800912)

Default Severity	WARNING
Log Message	ZoneDefense failed to unblock <unblock_type> blocked host <host>.
Explanation	A dynamically blocked host could not be unblocked by ZoneDefense.
Firewall Action	unblock
Recommended Action	None.
Revision	1
Parameters	host type unblock_type