D-Link®
Building Networks for People

NetDefend SOHO UTM Firewall
Log Reference Guide

DFL-160

Ver 2.27.00

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

Log Reference Guide

D-Link DFL-160 Firewall
NetDefendOS Version 2.27.00

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

Published 2010-05-25

Log Reference Guide

D-Link DFL-160 Firewall

NetDefendOS Version 2.27.00

Published 2010-05-25

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:

Table 1. Abbreviations

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
IDP	Intrusion Detection Prevention System
IP	Internet Protocol
IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
NAT	Network Address Translation
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

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.

Gateway 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.

[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.

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.

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.

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.
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***.

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.
Gateway 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.
Gateway 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.
Gateway 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.
Gateway 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.
Gateway 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.

Gateway 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. 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.

Gateway 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

2.1.8. 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.

Gateway 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

2.1.9. 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.
Gateway 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

2.1.10. 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.
Gateway 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

2.1.11. 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.
Gateway 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

2.1.12. 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.
Gateway 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

2.1.13. 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.
Gateway 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

2.1.14. 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.
Gateway 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

2.1.15. 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.
Gateway Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename filetype contenttype
Context Parameters	ALG Module Name ALG Session ID

2.1.16. 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.
Gateway Action	replace
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.17. content_filtering_disabled (ID: 00200115)

Default Severity	ERROR
Log Message	HTTPALG: Web Content Filtering disabled
Explanation	Web Content Filtering has been disabled due to license restriction.
Gateway Action	no_valid_license
Recommended Action	Extend valid time for Content Filtering.
Revision	2
Context Parameters	ALG Module Name

2.1.18. 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.
Gateway 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

2.1.19. 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.
Gateway 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

2.1.20. 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.
Gateway Action	none
Recommended Action	Try to free up some RAM by changing configuration parameters.
Revision	1
Context Parameters	ALG Module Name

2.1.21. 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. Verify that the unit has been configured with Internet access.
Gateway Action	none
Recommended Action	Check_configuration.
Revision	2
Context Parameters	ALG Module Name

2.1.22. 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.
Gateway 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

2.1.23. 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.
Gateway Action	switching_server
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.24. wcf_connecting (ID: 00200122)

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

2.1.25. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	server
Context Parameters	ALG Module Name

2.1.26. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.27. 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.
Gateway Action	allow
Recommended Action	None.
Revision	2
Parameters	categories audit override url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.28. 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.
Gateway Action	block
Recommended Action	None.
Revision	2

Parameters	categories audit override url algname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.29. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.30. 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.
Gateway Action	restarting
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.31. 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.

Gateway 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

2.1.32. out_of_memory (ID: 00200130)

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

2.1.33. 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.
Gateway Action	compensating
Recommended Action	None.
Revision	1
Parameters	url_orig url_req url_reply
Context Parameters	ALG Module Name

2.1.34. restricted_site_notice (ID: 00200132)

Default Severity	WARNING

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

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

Gateway Action allow

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

Revision 2

Parameters url
algname

Context Parameters Connection
Connection
ALG Module Name
ALG Session ID

2.1.35. 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.

Gateway 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

2.1.36. request_url (ID: 00200135)

Default Severity NOTICE

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

Explanation The URL has been requested.

Gateway Action allow

Recommended Action None.

Revision 1

Parameters categories
audit
override
url
user
algname

Context Parameters Connection
Connection
ALG Module Name
ALG Session ID

2.1.37. request_url (ID: 00200136)

Default Severity NOTICE

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

Explanation The URL has been requested.

Gateway Action allow_audit_mode

Recommended Action None.

Revision 2

Parameters categories
audit
override
url
user
algname

Context Parameters Connection
Connection
ALG Module Name
ALG Session ID

2.1.38. request_url (ID: 00200137)

Default Severity NOTICE

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

Explanation The URL has been requested.

Gateway Action block

Recommended Action None.

Revision 2

Parameters categories
audit
override

url
user
algname

Context Parameters Connection
Connection
ALG Module Name
ALG Session ID

2.1.39. restricted_site_notice (ID: 00200138)

Default Severity WARNING

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

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

Gateway Action allow

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

Revision 2

Parameters url
user
algname

Context Parameters Connection
Connection
ALG Module Name
ALG Session ID

2.1.40. url_reclassification_request (ID: 00200139)

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.

Gateway Action allow

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

Revision 2

Parameters newcat
url
user
algname

Context Parameters Connection
Connection
ALG Module Name

ALG Session ID

2.1.41. 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.
Gateway Action	optimizing
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.42. 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.
Gateway 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

2.1.43. 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.
Gateway Action	session_rejected
Recommended Action	This can be a possible DOS attack.

Revision	2
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.44. 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.
Gateway 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

2.1.45. 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.
Gateway Action	close
Recommended Action	None.
Revision	3
Context Parameters	ALG Module Name ALG Session ID

2.1.46. 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.
Gateway Action	close
Recommended Action	If possible, verify response codes sent from server.
Revision	3

Context Parameters	Connection ALG Module Name ALG Session ID

2.1.47. 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.
Gateway 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

2.1.48. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.49. 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.
Gateway Action	reject

Recommended Action None.

Revision 1

Parameters sender_email_address
recipient_email_addresses

Context Parameters ALG Module Name
ALG Session ID

2.1.50. 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.

Gateway 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

2.1.51. 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.

Gateway 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

2.1.52. 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.
Gateway 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

2.1.53. 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.
Gateway 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

2.1.54. 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.
Gateway 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

2.1.55. 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.

Gateway 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

2.1.56. 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.

Gateway 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

2.1.57. 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.

Gateway Action reject

Recommended Action None.

Revision 1

Parameters sender_email_address
recipient_email_addresses

Context Parameters ALG Module Name
ALG Session ID

2.1.58. 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.

Gateway Action close

Recommended Action Try to free up unwanted memory.

Revision 3

Context Parameters ALG Module Name
ALG Session ID

2.1.59. 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.

Gateway 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

2.1.60. 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.
Gateway Action	none
Recommended Action	None.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.61. 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).
Gateway Action	reject
Recommended Action	None.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.62. cmd_empty (ID: 00200180)

Default Severity	DEBUG
Log Message	SMTPALG: Received empty command.
Explanation	The SMTP command line was empty. Ignoring command.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

ALG Session ID

2.1.63. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.64. 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.
Gateway Action	allow
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.65. 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.
Gateway Action	capability_removed
Recommended Action	None.
Revision	1
Parameters	capa
Context Parameters	ALG Module Name ALG Session ID

2.1.66. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.67. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	violation
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.68. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	sender_email_address

Context Parameters	ALG Module Name ALG Session ID

2.1.69. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.1.70. hybrid_data (ID: 00200206)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Hybrid connection made
Explanation	A hybrid connection was successfully created.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.1.71. hybrid_data (ID: 00200209)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Hybrid data channel closed
Explanation	A hybrid data channel was closed.
Gateway Action	None
Recommended Action	None.

Revision 1

Context Parameters ALG Module Name
ALG Session ID
Rule Information
Connection

2.1.72. 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.

Gateway 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

2.1.73. 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.

Gateway 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

2.1.74. 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.
Gateway 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

2.1.75. 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.
Gateway 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

2.1.76. 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.
Gateway 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

2.1.77. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters peer
string

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.78. 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 that it's own. This is not allowed, and the command will be rejected.

Gateway 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

2.1.79. 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.

Gateway 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

2.1.80. 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.

Gateway Action None

Recommended Action None.

Revision 1

Parameters
peer
connection
string

Context Parameters
ALG Module Name
ALG Session ID
Connection

2.1.81. 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.

Gateway 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

2.1.82. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters peer

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.83. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters peer

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.84. 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.
Gateway Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.85. 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.
Gateway Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.86. 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.
Gateway 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

2.1.87. 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.

Gateway Action rejecting_command

Recommended Action None.

Revision 1

Parameters peer
string

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.88. 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.

Gateway 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

2.1.89. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer reply string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.90. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer reply string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.91. 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.

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

2.1.92. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.93. 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.
Gateway 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

2.1.94. 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 that it's own. This is not allowed, and the connection will be closed.
Gateway 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

2.1.95. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer connection string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.96. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer connection
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.97. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.98. 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.
Gateway Action	close
Recommended Action	Contact the support.
Revision	1
Context Parameters	ALG Module Name

2.1.99. 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.
Gateway Action	close
Recommended Action	Contact the support.
Revision	1
Context Parameters	ALG Module Name

2.1.100. 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.
Gateway 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

2.1.101. 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.
Gateway 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

2.1.102. 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.
Gateway 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

2.1.103. 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.
Gateway Action	data_blocked_control_and_data_channel_closed
Recommended Action	None.
Revision	1
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.104. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.105. 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.
Gateway 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

2.1.106. 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.
Gateway 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

2.1.107. 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.
Gateway 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

2.1.108. 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.

Gateway Action none

Recommended Action None.

Revision 1

Context Parameters ALG Module Name

2.1.109. 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.

Gateway 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

2.1.110. 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.

Gateway Action reject

Recommended Action None.

Revision	1
Parameters	packet_length
Context Parameters	ALG Module Name Connection

2.1.111. 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.
Gateway 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

2.1.112. command_not_allowed (ID: 00200353)

Default Severity	WARNING
Log Message	TFTPALG: <command> command not allowed
Explanation	Command (GET or PUT) not allowed. Closing connection.
Gateway 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

2.1.113. option_value_invalid (ID: 00200354)

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

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

2.1.114. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.115. 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.
Gateway 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

2.1.116. unknown_option_blocked (ID: 00200357)

Default Severity	WARNING
Log Message	TFTPALG: Request contained unknown option <option>
Explanation	Request contained unknown option.Closing connection.
Gateway 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

2.1.117. 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.
Gateway 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

2.1.118. unknown_option_blocked (ID: 00200359)

Default Severity	WARNING
Log Message	TFTPALG: Request contained unknown option <option>
Explanation	Request contained unknown option.Closing connection.
Gateway 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

2.1.119. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	option
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.120. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	option value
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.121. 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.
Gateway Action	close
Recommended Action	None.

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

2.1.122. 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.
Gateway 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

2.1.123. 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.
Gateway 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

2.1.124. 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.

Gateway 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

2.1.125. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters opcode
packet_length

Context Parameters ALG Module Name
ALG Session ID
Connection

2.1.126. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters error_code

Context Parameters ALG Module Name
ALG Session ID

2.1.127. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.128. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.129. 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.
Gateway 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

2.1.130. 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.
Gateway 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

2.1.131. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.132. 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.
Gateway Action	close
Recommended Action	None.
Revision	1

Parameters	error_code
Context Parameters	ALG Module Name

2.1.133. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	opcode packet_length
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.134. 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.
Gateway 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

2.1.135. 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.
Gateway 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

2.1.136. 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.
Gateway 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

2.1.137. 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.
Gateway Action	close
Recommended Action	Try to free up unwanted memory.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.138. 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.
Gateway 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

2.1.139. 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.
Gateway Action	block
Recommended Action	None.
Revision	1
Parameters	command" response
Context Parameters	ALG Module Name ALG Session ID

2.1.140. 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.
Gateway 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

2.1.141. 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.
Gateway 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

2.1.142. 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.
Gateway Action	block
Recommended Action	None.
Revision	1
Parameters	len linebegin"
Context Parameters	ALG Module Name ALG Session ID

2.1.143. 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.
Gateway Action	block
Recommended Action	None.
Revision	1
Parameters	command" len
Context Parameters	ALG Module Name ALG Session ID

2.1.144. 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.
Gateway Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename filetype sender_email_address
Context Parameters	ALG Module Name

2.1.145. 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.
Gateway Action	allow
Recommended Action	Content type should be matched.
Revision	2
Parameters	filename filetype sender_email_address
Context Parameters	ALG Module Name

2.1.146. 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.
Gateway Action	block

Recommended Action None.

Revision 1

Parameters command"
argument

Context Parameters ALG Module Name
ALG Session ID

2.1.147. 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.

Gateway 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

2.1.148. 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.

Gateway 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

2.1.149. 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..
Gateway 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

2.1.150. invalid_line_endings (ID: 00200397)

Default Severity	WARNING
Log Message	POP3ALG: Mail contains invalid line endings.
Explanation	Mail contains invalid line endings.
Gateway Action	block
Recommended Action	Research why mail contains invalid line endings.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.151. 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 Security Gateway.
Gateway Action	block
Recommended Action	None.
Revision	1
Parameters	len retrigs
Context Parameters	ALG Module Name ALG Session ID

2.1.152. 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.
Gateway 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

2.1.153. 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.
Gateway 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

2.1.154. 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.
Gateway 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

2.1.155. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	alert level algname
Context Parameters	ALG Module Name ALG Session ID

2.1.156. 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.
Gateway Action	tls_alert_sent
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.157. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	alert level algname

Context Parameters ALG Module Name
ALG Session ID

2.1.158. 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.

Gateway Action close

Recommended Action Change cipher suites and/or certificate.

Revision 1

Parameters algname

Context Parameters ALG Module Name
ALG Session ID

2.1.159. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters algname

Context Parameters ALG Module Name
ALG Session ID

2.1.160. 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.
Gateway 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

2.1.161. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	message_type algname
Context Parameters	ALG Module Name ALG Session ID

2.1.162. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.163. 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.
Gateway 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

2.1.164. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.165. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name

ALG Session ID

2.1.166. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	algname
Context Parameters	ALG Module Name ALG Session ID

2.1.167. 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.
Gateway 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

2.1.168. 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.
Gateway 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

2.1.169. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.170. 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 security gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Session ID ALG Module Name

2.1.171. pptp_tunnel_removed_client (ID: 00200605)

Default Severity	NOTICE
Log Message	PPTPALG: PPTP tunnel between client and security gateway removed
Explanation	A PPTP tunnel has been removed between the PPTP client and the PPTP-ALG.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Session ID

ALG Module Name

2.1.172. pptp_tunnel_removed_server (ID: 00200606)

Default Severity NOTICE

Log Message PPTPALG: PPTP tunnel between server and security gateway removed

Explanation A PPTP tunnel has been removed betweem the PPTP server and the PPTP-ALG.

Gateway Action None

Recommended Action None.

Revision 1

Context Parameters ALG Session ID
ALG Module Name

2.1.173. pptp_session_established (ID: 00200607)

Default Severity NOTICE

Log Message PPTPALG: PPTP session established

Explanation A PPTP session has been established.

Gateway Action None

Recommended Action None.

Revision 1

Context Parameters ALG Session ID
ALG Module Name

2.1.174. pptp_session_removed (ID: 00200608)

Default Severity NOTICE

Log Message PPTPALG: PPTP session removed

Explanation A PPTP session has been removed.

Gateway Action None

Recommended Action None.

Revision 1

Context Parameters ALG Session ID
ALG Module Name

2.1.175. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.1.176. 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 security gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Session ID ALG Module Name

2.2. ANTIVIRUS

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

2.2.1. virus_found (ID: 05800001)

Default Severity	WARNING
Log Message	Virus found in file <filename>. Virus Name: <virusname>. Signature: <virussig>. Advisory ID: <advisoryid>.
Explanation	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.
Gateway Action	block_data
Recommended Action	If the infected file is local, run anti-virus program to clean the file.
Revision	1
Parameters	filename virusname virussig advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.2. virus_found (ID: 05800002)

Default Severity	WARNING
Log Message	Virus found in file <filename>. Virus Name: <virusname>. Signature: <virussig>. Advisory ID: <advisoryid>.
Explanation	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.
Gateway Action	allow_data
Recommended Action	If the infected file is local, run anti-virus program to clean the file.
Revision	1
Parameters	filename virusname virussig advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.3. 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.

Gateway 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

2.2.4. 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.

Gateway 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

2.2.5. 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.
Gateway 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

2.2.6. compression_ratio_violation (ID: 05800006)

Default Severity	WARNING
Log Message	Compression ratio violation for file <filename>. Compression ratio threshold: <comp_ratio>
Explanation	Anti-virus has scanned a compresed file with a compression ratio higher than the specified value. Action is set to continue scan.
Gateway Action	continue_scan
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DOS attack.
Revision	1
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.7. 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 compresed file with a compression ratio higher than the specified value. Action is set to continue scan.
Gateway Action	abort_scan
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DOS attack.

Revision	1
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.8. 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 compresed file with a compression ratio higher than the specified value. Action is set to continue scan.
Gateway Action	block_data
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DOS attack.
Revision	1
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.9. 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.
Gateway 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

2.2.10. 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.
Gateway 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

2.2.11. 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.
Gateway Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.12. 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.

Gateway Action allow_data

Recommended Action None.

Revision 1

Parameters filename
[layer7_srcinfo]
[layer7_dstinfo]

Context Parameters ALG Module Name
ALG Session ID
Connection

2.2.13. 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.

Gateway 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

2.2.14. no_signature_database (ID: 05800016)

Default Severity CRITICAL

Log Message AVSE: Virus scanning aborted. No virus signatures present.

Explanation Anti-virus scanning is aborted since there is no local anti-virus signature database.

Gateway Action av_scanning_denied

Recommended Action Connect your gateway to the Internet and download the anti-virus database or configure automatic updates of anti-virus.

Revision 2

Context Parameters ALG Session ID

2.2.15. 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.

Gateway Action av_scanning_aborted

Recommended Action Try to restart the unit in order to solve this issue.

Revision 2

Context Parameters ALG Session ID

2.2.16. 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.

Gateway Action av_scanning_denied

Recommended Action Review your configuration in order to free up more RAM.

Revision 2

Context Parameters ALG Session ID

2.2.17. 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.

Gateway 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

2.2.18. 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.

Gateway 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

2.2.19. 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.

Gateway 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

2.2.20. 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.

Gateway 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. ARP

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

2.3.1. already_exists (ID: 00300001)

Default Severity	NOTICE
Log Message	An entry for this IP address already exists
Explanation	The entry was not added as a previous entry for this IP address already exists in the ARP table.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.2. 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.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.3. 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.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.4. 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.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.5. 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.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.6. 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.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.7. 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.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.8. 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.
Gateway 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

2.3.9. 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].
Gateway Action	None
Recommended Action	Update your license to allow a greater amount of concurrent ARP entries.
Revision	1
Parameters	limit

2.3.10. 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 verfied according to the "access" section, and the packet is dropped.
Gateway Action	drop
Recommended Action	If all ARP sender IP addresses should be accepted without validation, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.11. 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.
Gateway Action	access_allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.12. 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.
Gateway Action	drop
Recommended Action	Verify that no fault network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.13. 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.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.14. 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.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.15. 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.
Gateway 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

2.3.16. 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.
Gateway 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

2.4. AVUPDATE

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

2.4.1. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.4.2. 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.
Gateway Action	using_new_database
Recommended Action	None.
Revision	2

2.4.3. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

2.4.4. 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.
Gateway Action	None
Recommended Action	Check the system's time and/or purchase a subscription.
Revision	1

2.4.5. 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.
Gateway Action	antivirus_disabled
Recommended Action	Check and set the system time correct and perform a manual antivirus update.
Revision	1
Parameters	date

2.4.6. downloading_new_database (ID: 05000007)

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

2.4.7. 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.
Gateway Action	downloading_new_database

Recommended Action	None.
Revision	1

2.5. BUFFERS

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

2.5.1. 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.
Gateway Action	None
Recommended Action	If this is a reoccurring event, try increasing the number of HighBuffers.
Revision	1
Parameters	duration buf_usage

2.5.2. 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.
Gateway Action	None
Recommended Action	Nothing.
Revision	1
Parameters	numstop duration reason
Context Parameters	Packet Buffer

2.6. CONN

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

2.6.1. conn_open (ID: 00600001)

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

2.6.2. conn_close (ID: 00600002)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Connection

2.6.3. 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.
Gateway Action	replacing_conn
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

Connection

2.6.4. conn_open_natsat (ID: 00600004)

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

2.6.5. conn_close_natsat (ID: 00600005)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Connection

2.6.6. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.6.7. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.6.8. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	protocol
Context Parameters	Rule Name Packet Buffer

2.6.9. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1

Parameters	protocol
Context Parameters	Rule Name Packet Buffer

2.6.10. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.6.11. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.6.12. 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.
Gateway Action	drop

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

2.6.13. 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.
Gateway Action	drop
Recommended Action	If the packet is wanted, change the UDP source port 0 setting.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.6.14. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.6.15. conn_usage (ID: 00600023)

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

Context Parameters	Packet Buffer

2.6.16. active_data (ID: 00600100)

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

2.6.17. passive_data (ID: 00600101)

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

2.6.18. active_data (ID: 00600102)

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

Connection

2.6.19. passive_data (ID: 00600103)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Passive data channel closed
Explanation	A passive data channel was closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.7. DHCP

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

2.7.1. 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.
Gateway Action	restart
Recommended Action	Check network for statically configured hosts or incorrectly proxy ARPed routes.
Revision	1
Parameters	iface ip4addr

2.7.2. 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.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	iface
Context Parameters	Packet Buffer

2.7.3. lease_acquired (ID: 00700003)

Default Severity	NOTICE
Log Message	Interface <iface> have successfully acquired a lease
Explanation	An interface have successfully acquired a lease.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	iface ip netmask bcast gw
Context Parameters	Packet Buffer

2.7.4. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface valid_seconds
Context Parameters	Packet Buffer

2.7.5. 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.
Gateway Action	restart
Recommended Action	Check connection and DHCP server reachability.
Revision	1
Parameters	iface

2.7.6. 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.
Gateway 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

2.7.7. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface server_id
Context Parameters	Packet Buffer

2.7.8. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface netmask
Context Parameters	Packet Buffer

2.7.9. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface broadcast
Context Parameters	Packet Buffer

2.7.10. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface offered_ip
Context Parameters	Packet Buffer

2.7.11. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface gateway
Context Parameters	Packet Buffer

2.7.12. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface
Context Parameters	Packet Buffer

2.7.13. 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.
Gateway 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

2.7.14. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration and SG interface configuration.
Revision	1
Parameters	iface dhcp_route configured_route

Context Parameters Packet Buffer

2.8. DHCPRELAY

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

2.8.1. 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.
Gateway Action	None
Recommended Action	Check disk usage and health.
Revision	1

2.8.2. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

2.8.3. 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.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.8.4. 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.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.8.5. 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.
Gateway Action	None
Recommended Action	Verify packets-per-minute limit.
Revision	1
Context Parameters	Packet Buffer

2.8.6. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	packets_dropped
Context Parameters	Packet Buffer

2.8.7. 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.

Gateway Action	None
Recommended Action	Verify maximum-hop-limit setting.
Revision	1
Context Parameters	Packet Buffer

2.8.8. 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.
Gateway Action	relay_canceled
Recommended Action	None.
Revision	1
Parameters	client_ip
Context Parameters	Packet Buffer

2.8.9. 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.
Gateway Action	drop
Recommended Action	Check the network environment for errors.
Revision	1
Parameters	client_hw
Context Parameters	Packet Buffer

2.8.10. maximum_dhcp_client_relay_routes_reached (ID: 00800010)

Default Severity	WARNING
Log Message	The limit for DHCP relay routes have been reached. Dropping
Explanation	The DHCP relay routes limit have been reached.
Gateway Action	drop

Recommended Action	Verify max-relay-routes-limit.
Revision	1
Context Parameters	Rule Name

2.8.11. 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.
Gateway Action	drop
Recommended Action	Check firewall memory consumption.
Revision	1
Context Parameters	Rule Name

2.8.12. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.8.13. no_message_type (ID: 00800013)

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

2.8.14. 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.

Gateway Action drop

Recommended Action Investigate what client implementation is being used.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.8.15. 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.

Gateway Action drop

Recommended Action Investigate what client implementation is being used.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.8.16. 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.

Gateway Action drop

Recommended Action Verify max-relay-per-interface setting.

Revision 1

Parameters	max_relays
Context Parameters	Rule Name Packet Buffer

2.8.17. 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.
Gateway 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

2.8.18. 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.
Gateway Action	drop
Recommended Action	Verify max-transaction-count setting.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.8.19. 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.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.

Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name Packet Buffer

2.8.20. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	type client_hw dest_ip
Context Parameters	Rule Name Packet Buffer

2.8.21. relayed_request (ID: 00800021)

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

2.8.22. 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.
Gateway Action	drop
Recommended Action	Verify security-equivalent-interface setting.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.8.23. 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.
Gateway Action	drop
Recommended Action	Verify allowed-lease-addresses setting.
Revision	1
Parameters	iface server_ip ip
Context Parameters	Rule Name Packet Buffer

2.8.24. 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.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	server_ip ip
Context Parameters	Rule Name Packet Buffer

2.8.25. 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.
Gateway Action	drop
Recommended Action	Review previous configured host route for client.
Revision	1
Parameters	dest_ip
Context Parameters	Rule Name Packet Buffer

2.8.26. relayed_dhcp_reply (ID: 00800026)

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

2.8.27. relayed_bootp_reply (ID: 00800027)

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

2.8.28. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	type gateway_ip
Context Parameters	Rule Name Packet Buffer

2.8.29. relayed_bootp_reply (ID: 00800029)

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

2.9. DHCPSERVER

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

2.9.1. 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.
Gateway Action	None
Recommended Action	Check buffer consumption.
Revision	1

2.9.2. 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.
Gateway Action	drop
Recommended Action	Reduce the number of used DHCP options.
Revision	1

2.9.3. 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.
Gateway Action	None
Recommended Action	Make sure that there is sufficient diskspace available.
Revision	1

2.9.4. 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.

Gateway Action	None
Recommended Action	None.
Revision	1

2.9.5. 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.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.9.6. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.9.7. 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.

Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.9.8. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.9.9. 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.
Gateway Action	None
Recommended Action	Extend the pools to support more clients.
Revision	1
Context Parameters	Packet Buffer

2.9.10. 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.

Gateway Action	drop
Recommended Action	Check network equipment for errors.
Revision	1
Context Parameters	Packet Buffer

2.9.11. 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.
Gateway Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip client_hw
Context Parameters	Rule Name

2.9.12. 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.
Gateway Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip client_hw
Context Parameters	Rule Name

2.9.13. 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.
Gateway Action	None
Recommended Action	Extend the pools to support more clients.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.9.14. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw offer_ip
Context Parameters	Rule Name Packet Buffer

2.9.15. 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.
Gateway Action	None
Recommended Action	Extend the pool to support more clients.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.9.16. 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.
Gateway Action	nak
Recommended Action	None.
Revision	1

Parameters	client_hw client_wanted client_offered
Context Parameters	Rule Name Packet Buffer

2.9.17. 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.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	client_hw client_wanted bound
Context Parameters	Rule Name Packet Buffer

2.9.18. 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.
Gateway Action	new_lease
Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.9.19. client_renewed (ID: 00900020)

Default Severity	NOTICE
Log Message	Client <client_hw> renewed IP <client_ip>
Explanation	Client successfully renewed its lease.
Gateway Action	renew

Recommended Action None.

Revision 1

Parameters client_hw
client_ip

Context Parameters Rule Name
Packet Buffer

2.9.20. 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.

Gateway Action acknowledging

Recommended Action None.

Revision 1

Parameters client_hw
client_ip

Context Parameters Rule Name
Packet Buffer

2.9.21. 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.

Gateway 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

2.9.22. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.9.23. 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.
Gateway 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

2.9.24. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.9.25. 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.
Gateway 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

2.9.26. 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.
Gateway Action	lease_released
Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.10. FRAG

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

2.10.1. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.2. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Dropped Fragments Rule Name

2.10.3. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip

destip
ipproto
fragid
fragact
frags

Context Parameters Dropped Fragments
Rule Name

2.10.4. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters srcip
destip
ipproto
fragid
fragact
frags

Context Parameters Dropped Fragments
Rule Name

2.10.5. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters srcip
destip
ipproto
fragid
fragact
frags

Context Parameters Dropped Fragments

Rule Name

2.10.6. 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.

Gateway Action
drop

Recommended Action
None.

Revision
1

Parameters
srcip
destip
ipproto
fragid
fragact
frags

Context Parameters
Dropped Fragments
Rule Name

2.10.7. 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.

Gateway Action
drop

Recommended Action
None.

Revision
1

Parameters
srcip
destip
ipproto
fragid
fragact
frags

Context Parameters
Dropped Fragments
Rule Name

2.10.8. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.10.9. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.10.10. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters srcip
destip
ipproto
fragid
fragact
frags

Context Parameters Dropped Fragments
Rule Name

2.10.11. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters state

Context Parameters Dropped Fragments
Rule Name

2.10.12. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.10.13. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.14. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	minipdatalen maxipdatalen
Context Parameters	Rule Name Packet Buffer

2.10.15. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.16. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen
Context Parameters	Rule Name Packet Buffer

2.10.17. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	maxipdatalen
Context Parameters	Rule Name Packet Buffer

2.10.18. overlapping_frag (ID: 02000018)

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

2.10.19. bad_offs (ID: 02000019)

Default Severity	ERROR
Log Message	Bad fragment offset
Explanation	The fragment has an invalid offset. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.20. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.21. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.22. partial_overlap (ID: 02000022)

Default Severity	ERROR
Log Message	Fragments partially overlap
Explanation	Two fragments partially overlap. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.23. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.24. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.25. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.26. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.27. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.28. 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.

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

2.10.29. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Dropped Fragments Rule Name

2.11. IDP

These log messages refer to the **IDP (Intrusion Detection & Prevention events)** category.

2.11.1. 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>. Closing connection.

Explanation

A scan signature mapped to the "protect" action matched the traffic, closing connection.

Gateway Action

close

Recommended Action

Research the advisory (searchable by the unique ID), if you suspect an attack.

Revision

1

Parameters

description
signatureid
idrule
ipproto
srcip
srcport
destip
destport

Context Parameters

Rule Name
Deep Inspection

2.11.2. 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>. Closing connection.

Explanation

A notice signature mapped to the "protect" action matched the traffic, closing connection.

Gateway Action

close

Recommended Action

This is probably not an attack, but you may research the advisory (searchable by the unique ID).

Revision

1

Parameters

description
signatureid
idrule
ipproto
srcip

srcport
destip
destport

Context Parameters Rule Name
Deep Inspection

2.11.3. 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>. Closing connection.

Explanation An attack signature mapped to the "protect" action matched the traffic.

Gateway Action close

Recommended Action Research the advisory (searchable by the unique ID).

Revision 1

Parameters description
signatureid
idrule
ipproto
srcip
srcport
destip
destport

Context Parameters Rule Name
Deep Inspection

2.11.4. 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>. Closing connection.

Explanation A virus signature mapped to the "protect" action matched the traffic.

Gateway Action close

Recommended Action Research the advisory (searchable by the unique ID).

Revision 1

Parameters description
signatureid
idrule
ipproto
srcip
srcport

destip
destport

Context Parameters Rule Name
Deep Inspection

2.11.5. 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>.

Explanation A scan signature matched the traffic.

Gateway Action None

Recommended Action Research the advisory (searchable by the unique ID).

Revision 1

Parameters description
signatureid
idrule
ipproto
srcip
srcport
destip
destport

Context Parameters Rule Name
Deep Inspection

2.11.6. 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>.

Explanation A notice signature matched the traffic.

Gateway Action None

Recommended Action This is probably not an attack, but you may research the advisory (searchable by the unique ID).

Revision 1

Parameters description
signatureid
idrule
ipproto
srcip
srcport
destip
destport

Context Parameters Rule Name
Deep Inspection

2.11.7. 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>.
Explanation	An attack signature matched the traffic.
Gateway Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.11.8. 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>.
Explanation	A virus signature matched the traffic.
Gateway Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.11.9. 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.
Gateway 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

2.11.10. 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.
Gateway 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

2.11.11. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters idrule
srcip
srcport
destip
destport

Context Parameters Rule Name

2.11.12. 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.

Gateway Action ignore

Recommended Action None.

Revision 1

Parameters idrule
srcip
srcport
destip
destport

Context Parameters Rule Name

2.11.13. 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.

Gateway Action close

Recommended Action Review your configuration.

Revision 1

Parameters idrule
srcip
srcport
destip
destport

Context Parameters Rule Name

2.11.14. 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.

Gateway Action ignore

Recommended Action Review your configuration.

Revision 1

Parameters idrule
srcip
srcport
destip
destport

Context Parameters Rule Name

2.11.15. 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.

Gateway Action close

Recommended Action None.

Revision 1

Parameters idrule
srcip
srcport
destip
destport
reason

Context Parameters	Rule Name

2.11.16. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport reason
Context Parameters	Rule Name

2.12. IDPUPDATE

These log messages refer to the **IDPUPDATE (Intrusion Detection & Prevention Database update)** category.

2.12.1. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.12.2. 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.
Gateway Action	using_new_database
Recommended Action	None.
Revision	2

2.12.3. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

2.12.4. 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.
Gateway Action	None
Recommended Action	Check the system's time and/or purchase a subscription.
Revision	1

2.12.5. 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.
Gateway Action	idp_disabled
Recommended Action	Check and set the system time correct and perform a manual IDP update.
Revision	1
Parameters	date

2.12.6. 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.
Gateway Action	downloading_new_database
Recommended Action	None.
Revision	1

2.12.7. 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.
Gateway Action	downloading_new_database
Recommended Action	None.
Revision	1

2.13. IGMP

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

2.13.1. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	iface

2.13.2. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dest iface

2.13.3. 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.
Gateway Action	drop
Recommended Action	Identify the offending application, upgrade if possible.
Revision	1
Parameters	recv_if ip_dest

Context Parameters	Packet Buffer

2.13.4. 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.
Gateway 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

2.13.5. 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.
Gateway Action	None
Recommended Action	Reboot the system.
Revision	1

2.13.6. 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.
Gateway 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

2.13.7. 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.
Gateway 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

2.13.8. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	if rip igmpver grp src name

2.13.9. 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.

Gateway Action allow

Recommended Action None.

Revision 1

Parameters if
rip
igmpver
grp
src
sgrp
ssrc
name
action

2.13.10. 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.

Gateway 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

2.13.11. 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.

Gateway Action allow

Recommended Action None.

Revision 1

Parameters if
hip
igmpver
grp
src
sgrp
ssrc
name
action

2.13.12. 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.

Gateway 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

2.13.13. 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.

Gateway 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

2.13.14. 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.

Gateway Action drop

Recommended Action Specifically check for inconsistent SAT/NAT information in the IGMP config.

Revision 1

Parameters grp
iface

2.13.15. 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.

Gateway 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

2.13.16. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters

if
hip
igmpver
grp
src
sat_grp
sat_src
name

2.13.17. 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.

Gateway Action

drop

Recommended Action

None.

Revision

1

Parameters

name
src
grp
iface

2.13.18. 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. .

Gateway Action

drop

Recommended Action

Assign a different IP to the offending application.

Revision

1

Parameters

src
iface

Context Parameters

Packet Buffer

2.13.19. 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.
Gateway Action	drop
Recommended Action	Increase global IGMPMaxReqs per second limit if more requests are wanted.
Revision	1
Parameters	ipsrc iface

2.13.20. 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.
Gateway Action	drop
Recommended Action	Increase IGMPMaxReqsIf per second limit if more requets are wanted.
Revision	1
Parameters	ipsrc iface

2.13.21. disallowed_igmp_version (ID: 04200022)

Default Severity	NOTICE
Log Message	Disallowed IGMP Version
Explanation	A system is using a too old IGMP version.
Gateway 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

2.13.22. received_unknown_igmp_type (ID: 04200023)

Default Severity	NOTICE

Log Message	Dropped IGMP message with unknown type.
Explanation	Invalid IGMP message type received.
Gateway 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

2.13.23. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface rip igmpver

2.13.24. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface igmpver nigmpver

2.14. IPSEC

These log messages refer to the **IPSEC (IPsec (VPN) events)** category.

2.14.1. fatal_ipsec_event (ID: 01800100)

Default Severity	ALERT
Log Message	Fatal event occured, because of <reason>
Explanation	Fatal event occured in IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.14.2. warning_ipsec_event (ID: 01800101)

Default Severity	WARNING
Log Message	Warning event occured, because of <reason>
Explanation	Warning event from IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.14.3. audit_event (ID: 01800103)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	An audit event occured in the IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.14.4. audit_flood (ID: 01800104)

Default Severity	NOTICE
Log Message	<reason>.
Explanation	The rate limit for audit messages was reached.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.14.5. ike_delete_notification (ID: 01800105)

Default Severity	NOTICE
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.14.6. ike_invalid_payload (ID: 01800106)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.14.7. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.14.8. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.14.9. ike_quickmode_failed (ID: 01800109)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies

reason

2.14.10. packet_corrupt (ID: 01800110)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Received a corrupt packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.14.11. icv_failure (ID: 01800111)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The computed and ICV of the received packet did not match.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.14.12. sequence_number_failure (ID: 01800112)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet did not fall within the sliding window.
Gateway Action	drop

Recommended Action None.

Revision 1

Parameters source_ip
dest_ip
spi
seq
protocol
reason

2.14.13. sa_lookup_failure (ID: 01800113)

Default Severity NOTICE

Log Message Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.

Explanation The received packet could not be mapped to an appropriate SA.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters source_ip
dest_ip
spi
seq
protocol
reason

2.14.14. ip_fragment (ID: 01800114)

Default Severity NOTICE

Log Message Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.

Explanation The packet offered to AH/ESP processing appears to be an IP fragment.

Gateway Action None

Recommended Action None.

Revision 1

Parameters source_ip
dest_ip
spi
seq
protocol
reason

2.14.15. sequence_number_overflow (ID: 01800115)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	An attempt to transmit a packet that would result in sequence number overflow.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.14.16. bad_padding (ID: 01800116)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet has incorrect padding.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.14.17. hardware_accelerator_congested (ID: 01800117)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Hardware accleration failed due to resource shortage.
Gateway Action	drop
Recommended Action	None.
Revision	1

Parameters	source_ip dest_ip spi seq protocol reason

2.14.18. hardware_acceleration_failure (ID: 01800118)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Hardware acceleration failed due to resource shortage, a corrupt packet or other hardware related error.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.14.19. commit_failed (ID: 01800200)

Default Severity	CRITICAL
Log Message	Failed to commit IPsec configuration
Explanation	Failed to commit IPsec configuration.
Gateway Action	IPsec_configuration_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.14.20. 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.
Gateway Action	None
Recommended Action	None.

Revision	1

2.14.21. IPsec_successfully_started (ID: 01800202)

Default Severity	INFORMATIONAL
Log Message	IPsec is up and running
Explanation	IPsec configured and started.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.22. x509_init_failed (ID: 01800203)

Default Severity	CRITICAL
Log Message	Failed to initilaze x509 library
Explanation	Failed to initilaze x509 library.
Gateway Action	IPsec_configuration_disabled
Recommended Action	None.
Revision	1

2.14.23. pm_create_failed (ID: 01800204)

Default Severity	ERROR
Log Message	Failed to create policymanager
Explanation	Failed to create policymanager. Out of memory.
Gateway Action	reduce_number_of_tunnels
Recommended Action	None.
Revision	1

2.14.24. failed_to_start_ipsec (ID: 01800206)

Default Severity	ERROR
Log Message	Disable all IPsec tunnels
Explanation	Disable all IPsec tunnels due to memory limitations.
Gateway Action	disable_all_ipsec_interfaces
Recommended Action	None.

Revision	1

2.14.25. failed_create_audit_module (ID: 01800207)

Default Severity	ERROR
Log Message	Failed to create audit module.
Explanation	Failed to create audit module.
Gateway Action	IPsec_audit_disabled
Recommended Action	None.
Revision	1

2.14.26. failed_to_configure_IPsec (ID: 01800210)

Default Severity	CRITICAL
Log Message	Failed during configuration with error: <error_msg>
Explanation	Failed to set IPsec configuration.
Gateway Action	IPsec_configuration_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1
Parameters	error_msg

2.14.27. reconfig_IPsec (ID: 01800211)

Default Severity	INFORMATIONAL
Log Message	Reconfiguration of IPsec started
Explanation	Reconfiguration of IPsec started.
Gateway Action	ipsec_reconfigured
Recommended Action	None.
Revision	2

2.14.28. IPsec_init_failed (ID: 01800213)

Default Severity	CRITICAL
Log Message	Failed to initialize IPsec
Explanation	Failed to start IPsec.
Gateway Action	IPsec_configuration_disabled

Recommended Action	Restart.
Revision	1

2.14.29. ipsec_started_successfully (ID: 01800214)

Default Severity	INFORMATIONAL
Log Message	IPsec started successfully
Explanation	Succeeded to create Policymanger and commit IPsec configuration.
Gateway Action	ipsec_started
Recommended Action	None.
Revision	2

2.14.30. 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.
Gateway Action	certificate_disabled
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	certificate tunnel

2.14.31. 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.
Gateway Action	Use_default_IKE_DH_groups
Recommended Action	None.
Revision	1
Parameters	tunnel

2.14.32. 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.
Gateway Action	use_default_values_for_algorithm
Recommended Action	None.
Revision	1
Parameters	alg tunnel

2.14.33. failed_to_set_algorithm_properties (ID: 01800305)

Default Severity	ERROR
Log Message	Failed to set properties for IKE algorithm <alg>, for tunnel <tunnel>
Explanation	Failed to set specified properties (keysize, lifetimes) for IKE algorithm.
Gateway Action	use_default_values_for_algorithm
Recommended Action	None.
Revision	1
Parameters	alg tunnel

2.14.34. 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.
Gateway Action	disable_certificate
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	certificate tunnel

2.14.35. dns_resolve_failed (ID: 01800308)

Default Severity	WARNING
Log Message	Failed to resolve remote gateway <gateway> for IPsec Tunnel

	<ipsectunnel>. Keeping old IP <old_ip>
Explanation	Failed to resolve remote gateway through DNS.
Gateway Action	keeping_old_ip
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel old_ip

2.14.36. dns_resolve_failed (ID: 01800309)

Default Severity	WARNING
Log Message	Failed to resolve remote gateway <gateway> for IPsec Tunnel <ipsectunnel>. Disabling IPsec tunnel
Explanation	Failed to resolve remote gateway through DNS.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel

2.14.37. failed_to_add_peer (ID: 01800312)

Default Severity	ERROR
Log Message	Failed to add remote gateway: <gateway> resolved by DNS for IPsec tunnel: <ipsectunnel>
Explanation	Failed to add remote gateway, that have been resolved by DNS, to tunnel.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel

2.14.38. failed_to_add_rules (ID: 01800313)

Default Severity	ERROR
Log Message	Failed to add rules after remote gw: <gateway> have been resolved by DNS for IPsec tunnel: <ipsectunnel>

Explanation
Failed to add rules to tunnel after remote gateway have been resolved by DNS.

Gateway Action
IPsec_tunnel_disabled

Recommended Action
None.

Revision
1

Parameters
gateway
ipsectunnel

2.14.39. failed_to_add_rules (ID: 01800314)

Default Severity
ERROR

Log Message
Failed to commit rules after remote gw: <gateway> have been resolved by DNS for IPsec tunnel: <ipsectunnel>

Explanation
Failed to add rules to tunnel after remote gateway have been resolved by DNS.

Gateway Action
IPsec_tunnel_disabled

Recommended Action
None.

Revision
1

Parameters
gateway
ipsectunnel

2.14.40. new_remote_gw_ip (ID: 01800315)

Default Severity
INFORMATIONAL

Log Message
Resolved remote-gateway <gateway> to IP <ip> for IPsec tunnel <ipsectunnel>

Explanation
Tunnel have succesfully been reconfigured after remote gateway have been resolved.

Gateway Action
None

Recommended Action
None.

Revision
1

Parameters
gateway
ipsectunnel
ip

2.14.41. 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.
Gateway Action	ipsec_out_of_work
Recommended Action	Restart.
Revision	1

2.14.42. 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.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	peer

2.14.43. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.44. 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 authantication will be disabled.
Gateway Action	IPsec_disabled
Recommended Action	Restart.
Revision	1

Parameters	status_msg

2.14.45. 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.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1
Parameters	certificate tunnel

2.14.46. failed_to_set_remote_ID (ID: 01800323)

Default Severity	ERROR
Log Message	Invalid type for ID in remote access idlist: <type>, for tunnel <tunnel>
Explanation	Invalid type for ID in remote access idlist have been specified in configuration.
Gateway Action	vpntunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	type tunnel

2.14.47. failed_to_create_authorization (ID: 01800327)

Default Severity	CRITICAL
Log Message	Failed to create local authorization object
Explanation	Failed to create local authorization object. configured remote access groups will not be posible to use.
Gateway Action	IPsec_disabled
Recommended Action	None.
Revision	1

2.14.48. Failed_to_set_xauth (ID: 01800328)

Default Severity	ERROR
Log Message	Failed set XAuth for tunnel <tunnel>
Explanation	Failed to set extended authentication (XAuth) for the tunnel.
Gateway Action	None
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	tunnel

2.14.49. Failed_to_create_xauth_group (ID: 01800329)

Default Severity	CRITICAL
Log Message	Failed create XAuth group
Explanation	Failed to create extended authentication (XAuth) group.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.50. IPSec_tunnel_added (ID: 01800333)

Default Severity	INFORMATIONAL
Log Message	IPsec tunnel added to the configuration
Explanation	An IPsec tunnel has been enabled or added to the configuration.
Gateway Action	reconfiguration
Recommended Action	None.
Revision	1
Parameters	username client_ip IPsec_tunnel

2.14.51. IPSec_tunnel_added_bySGW (ID: 01800334)

Default Severity	INFORMATIONAL
Log Message	IPsec tunnel added by the Security Gateway
Explanation	An IPsec tunnel has been added by the Security Gateway.
Gateway Action	reconfiguration_by_SGW

Recommended Action	None.
Revision	1
Parameters	username client_ip IPsec_tunnel

2.14.52. IPSec_tunnel_modified_bySGW (ID: 01800335)

Default Severity	INFORMATIONAL
Log Message	IPsec tunnel changed by the Security Gateway
Explanation	An IPsec tunnel has been changed by the Security Gateway.
Gateway Action	reconfiguration_by_SGW
Recommended Action	None.
Revision	1
Parameters	username client_ip IPsec_tunnel

2.14.53. IPSec_tunnel_modified (ID: 01800336)

Default Severity	INFORMATIONAL
Log Message	IPsec tunnel configuration modified
Explanation	An IPsec tunnel has been modified.
Gateway Action	reconfiguration
Recommended Action	None.
Revision	1
Parameters	client_ip username IPsec_tunnel

2.14.54. IPSec_tunnel_removed (ID: 01800337)

Default Severity	INFORMATIONAL
Log Message	IPsec tunnel removed from the configuration
Explanation	An IPsec tunnel has been disabled or removed from the configuration.
Gateway Action	reconfiguration
Recommended Action	None.
Revision	1

Parameters	client_ip username IPsec_tunnel

2.14.55. tunnel_disabled (ID: 01800340)

Default Severity	WARNING
Log Message	Tunnel <tunnel> disabled due to configuration error.
Explanation	Tunnel [tunnel] disabled due to configuration error.
Gateway Action	tunnel_disabled
Recommended Action	Tunnel_disabled.
Revision	1
Parameters	tunnel

2.14.56. tunnel_cfg_error (ID: 01800341)

Default Severity	CRITICAL
Log Message	Critical configuration error on tunnel <tunnel>.
Explanation	Critical configuration error on tunnel [tunnel].
Gateway Action	restart
Recommended Action	Restart.
Revision	1
Parameters	tunnel

2.14.57. 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.
Gateway Action	None
Recommended Action	Update your config mode configuration.
Revision	1
Parameters	ippool

2.14.58. cfgmode_ip_freed (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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	ip

2.14.59. 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.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	2

2.14.60. 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.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.14.61. 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.
Gateway 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

2.14.62. 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.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.14.63. 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.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.14.64. ping_keepalive_failed_in_tunnel (ID: 01800505)

Default Severity	ERROR
Log Message	IPsec ping monitor detects loss if ping replies of packets INSIDE the tunnel
Explanation	IPsec ping monitor detects loss if ping replies of packets INSIDE the tunnel.
Gateway Action	tunnel_will_disabled_after_8_number_of_lost_packets
Recommended Action	None.
Revision	1

2.14.65. ipsec_interface_disabled (ID: 01800506)

Default Severity	ERROR
Log Message	IPsec interface disabled
Explanation	IPsec interface disabled.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.66. maximum_allowed_tunnels_limit_reached (ID: 01800900)

Default Severity	ALERT
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.
Gateway Action	negotiation_aborted
Recommended Action	None.
Revision	1
Parameters	allowed_tunnels

2.14.67. SAs_not_killed_for_remote_peer (ID: 01800901)

Default Severity	CRITICAL
Log Message	Failed to kill associated SA:s for <remotepeer> peer(s)
Explanation	This happens if there is no tunnel established with the given peer.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remotepeer

2.14.68. sa_write_congestion (ID: 01801337)

Default Severity	INFORMATIONAL
Log Message	Failed to write SA to Nitrox II due to congestion. <dir> SPI <spi>
Explanation	There was not enough free buffers to write the SA to Nitrox II. Every new packet on the SA will trigger a new try.

Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dir spi

2.14.69. sa_write_congestion (ID: 01801338)

Default Severity	WARNING
Log Message	Failed to write SA to Nitrox II; the request timed out. <dir> SPI <spi>
Explanation	A request to write an SA to Nitrox II timed out\r\n.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dir spi

2.14.70. 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.
Gateway Action	dropping_request
Recommended Action	None.
Revision	1
Parameters	proto

2.14.71. 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.
Gateway Action	dropping_request
Recommended Action	None.
Revision	1

2.14.72. malformed_packet (ID: 01802003)

Default Severity	WARNING
Log Message	Malformed packet for trigger.Dropping request for policy
Explanation	Malformed packet for trigger, dropping request.
Gateway Action	dropping_request
Recommended Action	None.
Revision	1

2.14.73. 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.
Gateway Action	rekey_not_done
Recommended Action	None.
Revision	1

2.14.74. max_number_of_tunnels_reached (ID: 01802011)

Default Severity	WARNING
Log Message	Negotiation aborted due to license restrictions <maxtunnels>
Explanation	Reached max number of allowed active VPN tunnels according to license.
Gateway Action	ike_negotiation_aborted
Recommended Action	Reconfigure_IPsec.
Revision	1
Parameters	maxtunnels

2.14.75. ike_sa_failed (ID: 01802022)

Default Severity	WARNING
Log Message	Ike SA negotiation failed: <statusmsg> Local IKE peer: <local_peer> Remote IKE peer: <remote_peer> Initiator SPI: <initiator_spi>.

Explanation Negotiation of IKE SA failed.

Gateway Action no_ike_sa

Recommended Action None.

Revision 2

Parameters statusmsg
local_peer
remote_peer
initiator_spi

2.14.76. ike_sa_negotiation_completed (ID: 01802024)

Default Severity INFORMATIONAL

Log Message IKE SA <options> negotiation completed: <mode> using <auth> (<encryption><keysize> - <hash>) Diffie-Hellman group <dhgroup> (<bits>) Lifetime: <lifetime> seconds

Explanation Negotiation of IKE SA completed.

Gateway Action None

Recommended Action None.

Revision 1

Parameters options
mode
auth
encryption
keysize
hash
dhgroup
bits
lifetime

2.14.77. ike_sa_negotiation_failed (ID: 01802030)

Default Severity INFORMATIONAL

Log Message No IKE SA negotiations done. Reason: The authentication credentials were not specified or private key was not available

Explanation No IKE SA negotiations done because of authentication problems.

Gateway Action no_ike_sa

Recommended Action None.

Revision 1

2.14.78. ike_sa_negotiation_failed (ID: 01802031)

Default Severity	WARNING
Log Message	Type of the local ID <localid> is not KEY-ID for the mamros-pskeyext negotiation. The negotiation might fail.
Explanation	Type of the local ID is not KEY-ID for the mamros-pskeyext negotiation. The negotiation might fail.
Gateway Action	no_ike_sa
Recommended Action	None.
Revision	1
Parameters	localid

2.14.79. ipsec_sa_negotiation_completed (ID: 01802040)

Default Severity	INFORMATIONAL
Log Message	IPsec SA <sa> <info> negotiation completed:
Explanation	Child SA negotiatiion successfully completed.
Gateway Action	ipsec_sa_enabled
Recommended Action	None.
Revision	3
Parameters	sa info local_peer remote_peer spi_in spi_out [local_ts] [remote_ts]

2.14.80. ipsec_sa_informal (ID: 01802041)

Default Severity	INFORMATIONAL
Log Message	PFS using Diffie-Hellman group: <dhgroup> (<bits>)
Explanation	Information about PFS and Diffie Hellman group used for Child SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dhgroup bits

2.14.81. ipsec_sa_informal (ID: 01802043)

Default Severity	INFORMATIONAL
Log Message	Inbound SPI:<spiin> | Outbound SPI:<spiout> | Algorithm:<alg> <keysize> <mac>
Explanation	Log information about SPI-values and algorithms for Child SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	spiin spiout alg keysize mac

2.14.82. ipsec_sa_informal (ID: 01802044)

Default Severity	INFORMATIONAL
Log Message	Inbound SPI:<spiin> | Outbound SPI:<spiout> | Algoritm:<mac>
Explanation	Log information about SPI-values and algorithms fro Child SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	spiin spiout mac

2.14.83. ipsec_sa_lifetime (ID: 01802045)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: <kb> kilobytes, <sec> seconds
Explanation	Inform about lifetime for child SA:.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	kb sec

2.14.84. ipsec_sa_lifetime (ID: 01802046)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: <sec> seconds
Explanation	Inform about lifetime for child SA:.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	sec

2.14.85. ipsec_sa_lifetime (ID: 01802047)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: <kb> kilobytes
Explanation	Inform about lifetime for child SA:.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	kb

2.14.86. ipsec_sa_lifetime (ID: 01802048)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: infinite
Explanation	Inform about lifetime for child SA.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.87. ipsec_sa_informal (ID: 01802058)

Default Severity	INFORMATIONAL
Log Message	Local Proxy ID: <local_id>, Remote Proxy ID: <remote_id>
Explanation	Information about Proxy ID's for Child SA.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	local_id remote_id

2.14.88. ipsec_invalid_protocol (ID: 01802059)

Default Severity	ERROR
Log Message	Invalid protocol <proto> received for SA
Explanation	Invalid protocol received for SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	proto

2.14.89. 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.
Gateway Action	ipsec_sa_negotiation_aborted
Recommended Action	None.
Revision	1

2.14.90. create_rules_failed (ID: 01802080)

Default Severity	ERROR
Log Message	Cannot insert this rule, the forced NAT protocol type does not match rule protocol
Explanation	Failed to insert rule since forced NAT protocol do not match rule protocol.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.14.91. create_rules_failed (ID: 01802081)

Default Severity	ERROR
Log Message	Cannot insert this rule, the forced NAT protocol type does not match

	rule protocol
Explanation	Failed to insert rule since forced NAT protocol do not match rule protocol.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.14.92. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.14.93. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.14.94. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.

Revision	1

2.14.95. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.96. invalid_rule_setting (ID: 01802106)

Default Severity	ERROR
Log Message	The AUTHENTICATION-ONLY can be specified only for PASS rules
Explanation	Can only specify AUTHENTICATION-ONLY with PASS rules.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.97. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.98. invalid_rule_setting (ID: 01802108)

Default Severity	ERROR
Log Message	No from-tunnel specified for an AUTHENTICATION-ONLY rule
Explanation	From-tunnel must be specified for an AUTHENTICATION-ONLY rule.

Gateway Action	None
Recommended Action	None.
Revision	1

2.14.99. invalid_rule_setting (ID: 01802109)

Default Severity	ERROR
Log Message	To-tunnel specified for an AUTHENTICATION-ONLY rule
Explanation	To-tunnel can not be specified for an AUTHENTICATION-ONLY rule.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.100. 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.
Gateway Action	VPN_configuration_disabled
Recommended Action	Review the advanced setting IPsecMaxRules.
Revision	2

2.14.101. 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.
Gateway Action	the_rule_might_not_work
Recommended Action	Reconfigure_IPsec.
Revision	2

2.14.102. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.14.103. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.14.104. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.14.105. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.14.106. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2
Parameters	tunnel

2.14.107. 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].
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.14.108. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.

Revision	1
Parameters	tunnel

2.14.109. 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!.
Gateway Action	VPN_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	tunnel

2.14.110. invalid_key_size (ID: 01802214)

Default Severity	ERROR
Log Message	Invalid key sizes specified for algorithms
Explanation	Invalid key sizes specified for algorithms.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.14.111. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.14.112. 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.

Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.14.113. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2
Parameters	alg

2.14.114. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize max

2.14.115. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	alg

2.14.116. 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.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize max

2.14.117. malformed_tunnel_id_configured (ID: 01802225)

Default Severity	ERROR
Log Message	Malformed identity <id> configured for tunnel
Explanation	Malformed identity specified in configuration.
Gateway Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_remote_id.
Revision	1
Parameters	id

2.14.118. malformed_psk_configured (ID: 01802229)

Default Severity	ERROR
Log Message	Malformed IKE secret (PSK) configured for tunnel
Explanation	Malformed IKE secret specified in configuration.
Gateway Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_PSK.
Revision	1

2.14.119. rule_selection_failed (ID: 01802300)

Default Severity	NOTICE
Log Message	Rule selection failed: <info>. Internal severity level: <int_severity>
Explanation	Rule selection failed!.

Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	info int_severity

2.14.120. max_phase1_sa_reached (ID: 01802400)

Default Severity	NOTICE
Log Message	The maximum number of active Phase-1 SAs reached
Explanation	Maximum number of active Phase-1 SAs reached.
Gateway Action	negotiation_aborted
Recommended Action	None.
Revision	1

2.14.121. max_phase1_negotiations_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.
Gateway Action	negotiation_aborted
Recommended Action	None.
Revision	2

2.14.122. 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.
Gateway Action	quick-mode_not_done
Recommended Action	None.
Revision	1

2.14.123. 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.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.14.124. 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.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.14.125. 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.
Gateway Action	certificate_not_trusted
Recommended Action	None.
Revision	1

2.14.126. 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.

Gateway Action	certificate_not_usable_if_no_valid_CRLs
Recommended Action	None.
Revision	1

2.14.127. 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.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.14.128. 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.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.14.129. 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.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.14.130. 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.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.14.131. could_not_loack_certificate (ID: 01802608)

Default Severity	WARNING
Log Message	Could not lock certificate in cache
Explanation	Could not lock certificate in cache.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.14.132. 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.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.14.133. 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.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.14.134. ike_sa_negotiation_completed (ID: 01802703)

Default Severity INFORMATIONAL

Log Message IKE SA: Local IKE peer: <local_peer> Remote IKE peer: <remote_peer> Initiator SPI: <initiator_spi> Responder SPI: <responder_spi>. Internal severity level: <int_severity>.

Explanation Ike SA sucessfully installed.

Gateway Action ike_sa_completed

Recommended Action None.

Revision 1

Parameters local_peer
remote_peer
initiator_spi
responder_spi
int_severity

2.14.135. ike_sa_negotiation_completed (ID: 01802704)

Default Severity INFORMATIONAL

Log Message IKE SA: Local IKE peer: <local_peer> Remote IKE peer: <remote_peer>. Internal severity level: <int_severity>

Explanation Ike SA sucessfully installed.

Gateway Action ike_sa_completed

Recommended Action None.

Revision 1

Parameters local_peer
remote_peer
int_severity

2.14.136. 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.

Gateway Action try_next_certificate

Recommended Action None.

Revision 1

Parameters len

2.14.137. 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.
Gateway Action	skip_dn_name
Recommended Action	None.
Revision	1
Parameters	dn_name

2.14.138. 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.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.14.139. ike_sa_destroyed (ID: 01802708)

Default Severity	INFORMATIONAL
Log Message	IKE SA destroyed: <ike_sa>
Explanation	Ike SA is destroyed.
Gateway Action	ike_sa_killed
Recommended Action	None.
Revision	1
Parameters	ike_sa

2.14.140. 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.
Gateway Action	None

Recommended Action None.

Revision 1

Parameters cfgmode
msg
int_severity

2.14.141. 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.

Gateway Action None

Recommended Action None.

Revision 1

Parameters ipaddr
[time]

2.14.142. remote_access_dns (ID: 01802711)

Default Severity INFORMATIONAL

Log Message DNS for remote access attributes: <dns_server>

Explanation DNS for remote access attributes.

Gateway Action None

Recommended Action None.

Revision 1

Parameters dns_server

2.14.143. remote_access_wins (ID: 01802712)

Default Severity INFORMATIONAL

Log Message WINS for remote access attributes: <win>

Explanation WINS for remote access attributes.

Gateway Action None

Recommended Action None.

Revision 1

Parameters win

2.14.144. remote_access_dhcp (ID: 01802713)

Default Severity	INFORMATIONAL
Log Message	DHCP for remote access attributes: <dhcp_s>
Explanation	DHCP remote access attributes.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dhcp_s

2.14.145. remote_access_subnets (ID: 01802714)

Default Severity	INFORMATIONAL
Log Message	Subnets remote access attributes: <subnets>
Explanation	Subnets remote access attributes.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	subnets

2.14.146. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	side msg int_severity

2.14.147. 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.
Gateway Action	no_ipsec_sa_selected
Recommended Action	None.
Revision	2
Parameters	reason int_severity

2.14.148. certificate_search_failed (ID: 01802718)

Default Severity	WARNING
Log Message	Certificate manager search failure: <reason>. Internal severity level: <int_severity>
Explanation	Search for matching certificate failed.
Gateway Action	certificate_failure
Recommended Action	None.
Revision	1
Parameters	reason int_severity

2.14.149. ipsec_sa_event (ID: 01802730)

Default Severity	WARNING
Log Message	IPsec SA negotiation event: <msg>, <local_proxy>, <remote_proxy>. Internal severity level: <int_severity>
Explanation	Event occured for IPsec SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	msg local_proxy remote_proxy int_severity

2.14.150. ipsec_sa_event (ID: 01802731)

Default Severity	WARNING
Log Message	IPsec SA negotiation event: <msg>. Internal severity level:

	<int_severity>
Explanation	Event occured for IPsec SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	msg int_severity

2.14.151. ipsec_sa_destroyed (ID: 01802732)

Default Severity	INFORMATIONAL
Log Message	IPsec SA destroyed: Inbound SPI: <spiin> | Outbound SPI: <spiout>
Explanation	IPsec SA have been destroyed.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	spiin spiout

2.14.152. (ID: 01802735)

Default Severity	INFORMATIONAL
Log Message	L2TP <side> negotiation event: <msg>. <local_peer>, <remote_peer>. Internal severity level: <int_severity>
Explanation	L2TP negotiation event.
Gateway Action	l2tp_negotiation_event
Recommended Action	None.
Revision	1
Parameters	side msg local_peer remote_peer int_severity

2.14.153. (ID: 01802736)

Default Severity	INFORMATIONAL
Log Message	L2TP <side> negotiation event: <msg>. <local_id>, <remote_id>. Internal severity level: <int_severity>

Explanation	L2TP negotiation event.
Gateway Action	l2tp_negotiation_event
Recommended Action	None.
Revision	1
Parameters	side msg local_id remote_id int_severity

2.14.154. 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.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.155. init_rulelooklup_failed (ID: 01802903)

Default Severity	CRITICAL
Log Message	Initialization of rule lookup failed
Explanation	Initialization of rule lookup failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.156. init_rule_looklup_failed (ID: 01802904)

Default Severity	CRITICAL
Log Message	Allocating default drop rule failed!
Explanation	Allocating default drop rule failed!.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.157. init_rule_looklup_failed (ID: 01802905)

Default Severity	CRITICAL
Log Message	allocating default pass rule failed!
Explanation	Allocating default pass rule failed!.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.158. init_mutexes_failed (ID: 01802906)

Default Severity	CRITICAL
Log Message	Allocating mutexes failed
Explanation	Allocating mutexes failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.159. init_interface_table_failed (ID: 01802907)

Default Severity	CRITICAL
Log Message	Initialization of interface table failed
Explanation	Initialization of interface table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.160. init_flow_id_table_failed (ID: 01802908)

Default Severity	CRITICAL
Log Message	Allocation of flow id hash tables failed
Explanation	Allocation of flow id hash tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.161. init_flow_table_failed (ID: 01802909)

Default Severity	CRITICAL
Log Message	Allocation of flow table failed (size <size>)
Explanation	Allocation of flow table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1
Parameters	size

2.14.162. init_next_hop_table_failed (ID: 01802910)

Default Severity	CRITICAL
Log Message	Allocation of next hop table failed
Explanation	Allocation of next hop table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.163. init_transform_table_failed (ID: 01802911)

Default Severity	CRITICAL
Log Message	Allocation of transform table failed (size <size>)
Explanation	Allocation of transform table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1
Parameters	size

2.14.164. init_peer_hash_failed (ID: 01802912)

Default Severity	CRITICAL
Log Message	Allocation of peer hash table failed
Explanation	Allocation of peer hash table failed.
Gateway Action	ipsec_disabled

Recommended Action	None.
Revision	1

2.14.165. init_peer_id_hash_failed (ID: 01802913)

Default Severity	CRITICAL
Log Message	Allocation of peer id hash table failed
Explanation	Allocation of peer id hash table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.166. init_rule_table_failed (ID: 01802914)

Default Severity	CRITICAL
Log Message	Allocation of rule table failed
Explanation	Allocation of rule table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.167. init_inbound_spi_hash_failed (ID: 01802915)

Default Severity	CRITICAL
Log Message	Allocation of inbound spi hash table failed
Explanation	Allocation of inbound spi hash table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.168. init_transform_context_hash_failed (ID: 01802916)

Default Severity	CRITICAL
Log Message	Allocation of transform context hash table failed
Explanation	Allocation of transform context hash table failed.

Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.169. init_packet_context_cache_failed (ID: 01802917)

Default Severity	CRITICAL
Log Message	Allocation of packet context cache failed
Explanation	Allocation of packet context cache failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.170. init_transform_context_table_failed (ID: 01802918)

Default Severity	CRITICAL
Log Message	Allocation of transform context table failed
Explanation	Allocation of transform context table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.171. init_nat_table_failed (ID: 01802919)

Default Severity	CRITICAL
Log Message	Allocation of NAT tables failed
Explanation	Allocation of NAT tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.172. init_frag_table_failed (ID: 01802920)

Default Severity	CRITICAL
Log Message	Allocation of fragmentation tables failed

Explanation	Allocation of fragmentation tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.173. init_engine_tables_failed (ID: 01802921)

Default Severity	CRITICAL
Log Message	Allocation of engine tables failed
Explanation	Allocation of engine tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.174. init_interceptor_failed (ID: 01802922)

Default Severity	CRITICAL
Log Message	Opening the interceptor failed
Explanation	Opening the interceptor failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.14.175. malformed_ike_sa_proposal (ID: 01803000)

Default Severity	WARNING
Log Message	Malformed IKE SA proposal: <reason>
Explanation	Received a malformed IKE SA proposal.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.14.176. failed_to_select_policy_rule (ID: 01803001)

Default Severity	INFORMATIONAL

Log Message	Could not select policy rule
Explanation	Could not select policy rule.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.177. failed_to_select_ike_sa (ID: 01803002)

Default Severity	INFORMATIONAL
Log Message	Could not select SA from IKE SA proposal
Explanation	Could not select SA from IKE SA proposal.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.178. ike_phase1_notification (ID: 01803003)

Default Severity	WARNING
Log Message	<status> Phase-1 notification from <remote_peer> for protocol <proto>, SPI <spi>: <msg> (<type>) (<size> bytes)
Explanation	Received a IKE Phase-2 notification.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	status remote_peer proto spi msg type size

2.14.179. ipsec_sa_failed (ID: 01803020)

Default Severity	WARNING
Log Message	IPsec SA negotiation failed: <statusmsg>
Explanation	Negotiation of IPsec SA failed.
Gateway Action	no_ipsec_sa

Recommended Action None.

Revision 1

Parameters statusmsg

2.14.180. ipsec_sa_statistics (ID: 01803021)

Default Severity INFORMATIONAL

Log Message IPsec SA negotiations: <done> done, <success> successful, <failed> failed

Explanation IPsec SA statistics.

Gateway Action None

Recommended Action None.

Revision 1

Parameters done
success
failed

2.14.181. config_mode_exchange_event (ID: 01803022)

Default Severity INFORMATIONAL

Log Message Config Mode exchange event: <msg>. <reason>.

Explanation A Config Mode exchange event occured.

Gateway Action None

Recommended Action None.

Revision 1

Parameters msg
reason

2.14.182. config_mode_exchange_event (ID: 01803023)

Default Severity INFORMATIONAL

Log Message Config Mode exchange event: <msg>.

Explanation A Config Mode exchange event occured.

Gateway Action None

Recommended Action None.

Revision 1

Parameters msg

2.14.183. xauth_exchange_done (ID: 01803024)

Default Severity	INFORMATIONAL
Log Message	XAuth exchange done: <statusmsg>
Explanation	Information about the result of a completed XAuth exchange.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	statusmsg

2.14.184. config_mode_exchange_event (ID: 01803025)

Default Severity	INFORMATIONAL
Log Message	Config Mode exchange event: <msg>. <reason>.
Explanation	A Config Mode exchange event occured.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg reason

2.14.185. config_mode_exchange_event (ID: 01803026)

Default Severity	INFORMATIONAL
Log Message	Config Mode exchange event: <msg>.
Explanation	A Config Mode exchange event occured.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg

2.14.186. rejecting_ipsec_sa_delete (ID: 01803027)

Default Severity	WARNING
Log Message	Rejecting IPsec SA delete notification from <remote_peer> since it was for protocol <proto>

Explanation	Rejected IPsec SA delete notification due to protocol mismatch.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remote_peer proto

2.14.187. rejecting_ipsec_sa_delete (ID: 01803028)

Default Severity	WARNING
Log Message	Rejecting IPsec SA delete notification from <remote_peer> since the SPI size <spi_size> does not match the expected value 4
Explanation	Rejected IPsec SA delete notification because the SPI size did not match the expected value 4.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remote_peer spi_size

2.14.188. ike_phase2_notification (ID: 01803029)

Default Severity	WARNING
Log Message	<status> Phase-2 notification from <remote_peer> for protocol <proto>, SPI <spi>: <msg> (<type>) (<size> bytes)
Explanation	Received a IKE Phase-2 notification.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	status remote_peer proto spi msg type size

2.14.189. ike_qm_notification (ID: 01803030)

Default Severity	WARNING

Log Message	Quick-Mode notification from <remote_peer> for protocol <proto>, SPI <spi>: <msg> (<type>) (<size> bytes)
Explanation	Received a IKE Quick-Mode notification.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remote_peer proto spi msg type size

2.14.190. failed_to_verify_peer_identity (ID: 01803040)

Default Severity	INFORMATIONAL
Log Message	Could not verify remote peer's identity
Explanation	Could not verify remote peer's identity.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.191. malformed_ipsec_sa_proposal (ID: 01803050)

Default Severity	WARNING
Log Message	Malformed IPsec SA proposal: <reason>
Explanation	Received a malformed IPsec SA proposal.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.14.192. malformed_ipsec_esp_proposal (ID: 01803051)

Default Severity	WARNING
Log Message	Malformed IPsec ESP proposal: <reason>
Explanation	Received a malformed IPsec ESP proposal.
Gateway Action	None

Recommended Action	None.
Revision	1
Parameters	reason

2.14.193. malformed_ipsec_ah_proposal (ID: 01803052)

Default Severity	WARNING
Log Message	Malformed IPsec AH proposal: <reason>
Explanation	Received a malformed IPsec AH proposal.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.14.194. failed_to_select_ipsec_proposal (ID: 01803053)

Default Severity	WARNING
Log Message	Could not select proposal for IPsec SA <sa_index>
Explanation	Could not select proposal for IPsec SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	sa_index

2.14.195. failed_to_select_ipsec_sa (ID: 01803054)

Default Severity	INFORMATIONAL
Log Message	Could not select SA from IPsec SA proposal
Explanation	Could not select SA from IPsec SA proposal.
Gateway Action	None
Recommended Action	None.
Revision	1

2.14.196. ike_responder_mode_not_available (ID: 01803101)

Default Severity	NOTICE
Log Message	Negotiation aborted due to license restrictions: IKE responder mode not available.
Explanation	A negotiation was aborted because it was not initiated by the correct side in accordance with license restrictions.
Gateway Action	ike_negotiation_aborted
Recommended Action	None.
Revision	1

2.14.197. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg int_severity

2.14.198. ipsec_hwaccel_failed (ID: 01803410)

Default Severity	WARNING
Log Message	Failed to create a hardware acceleration context for IPsec SA (<dir> SPI <spi>). <error_msg> Packets will be processed in software.
Explanation	Hardware acceleration of the IPsec SA couldn't be done. All packets belonging to the specified SA will be processed in software.
Gateway Action	None
Recommended Action	Verify that the crypto suites are supported by the hardware accelerator. Contact support and report this issue if a supported crypto suite is configured.
Revision	1
Parameters	dir spi error_msg

2.15. IP_ERROR

These log messages refer to the **IP_ERROR (Packet discarded due to IP header error(s))** category.

2.15.1. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.2. disallwed_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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipver
Context Parameters	Rule Name Packet Buffer

2.15.3. 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.
Gateway Action	drop
Recommended Action	None.

Revision	1
Parameters	iptotlen iphdrlen
Context Parameters	Rule Name Packet Buffer

2.15.4. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	iptotlen recvlen
Context Parameters	Rule Name Packet Buffer

2.15.5. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	recvchksum compchksum
Context Parameters	Rule Name Packet Buffer

2.16. IP_FLAG

These log messages refer to the **IP_FLAG (Events concerning the IP header flags)** category.

2.16.1. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	ttl ttlmin
Context Parameters	Rule Name Packet Buffer

2.16.2. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.16.3. 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.
Gateway Action	strip_flag
Recommended Action	None.
Revision	1

Context Parameters	Rule Name Packet Buffer

2.17. IP_OPT

These log messages refer to the **IP_OPT (Events concerning the IP header options)** category.

2.17.1. source_route (ID: 01700001)

Default Severity	NOTICE
Log Message	Packet has a source route
Explanation	The packet has a source route. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.17.2. timestamp (ID: 01700002)

Default Severity	NOTICE
Log Message	Packet has a timestamp IP Option
Explanation	The packet contains a timestamp IP Option. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.17.3. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.17.4. ipopt_present (ID: 01700004)

Default Severity	NOTICE
Log Message	IP Option <ipopt>(<optname>) is present
Explanation	The packet contains an IP Option. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	ipopt optname
Context Parameters	Rule Name Packet Buffer

2.17.5. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt minoptlen avail
Context Parameters	Rule Name Packet Buffer

2.17.6. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen

	avail
Context Parameters	Rule Name Packet Buffer

2.17.7. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.17.8. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen route
Context Parameters	Rule Name Packet Buffer

2.17.9. 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.
Gateway Action	drop

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

2.17.10. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.17.11. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.17.12. 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.
Gateway Action	drop
Recommended Action	None.

Revision	1
Parameters	ipopt optlen
Context Parameters	Rule Name Packet Buffer

2.17.13. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt tsptr
Context Parameters	Rule Name Packet Buffer

2.17.14. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt tsptr oflo
Context Parameters	Rule Name Packet Buffer

2.17.15. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.17.16. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters ipopt
optlen

Context Parameters Rule Name
Packet Buffer

2.17.17. 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.

Gateway Action drop

Recommended Action None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.17.18. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optname
Context Parameters	Rule Name Packet Buffer

2.18. IP_PROTO

These log messages refer to the **IP_PROTO (IP Protocol verification events)** category.

2.18.1. multicast_ethernet_ip_address_missmatch (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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ip_multicast_addr eth_multicast_addr
Context Parameters	Rule Name Packet Buffer

2.18.2. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	totlen
Context Parameters	Rule Name Packet Buffer

2.18.3. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.18.4. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ttl ttlmin
Context Parameters	Rule Name Packet Buffer

2.18.5. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.18.6. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.7. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen tcphdrlen
Context Parameters	Rule Name Packet Buffer

2.18.8. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.9. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen udptotlen
Context Parameters	Rule Name Packet Buffer

2.18.10. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.11. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen icmpminlen
Context Parameters	Rule Name Packet Buffer

2.18.12. multicast_ethernet_ip_address_missmatch (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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	ip_multicast_addr eth_multicast_addr
Context Parameters	Rule Name Packet Buffer

2.18.13. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.14. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.

Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.15. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.16. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.17. 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.
Gateway Action	drop

Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.18. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.19. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.20. 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.

Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.21. 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.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.18.22. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.18.23. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpiphdrminlen
Context Parameters	Rule Name Packet Buffer

2.18.24. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipver
Context Parameters	Rule Name Packet Buffer

2.18.25. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmphdrlen
Context Parameters	Rule Name Packet Buffer

2.18.26. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipdatalen icmpipdataminlen
Context Parameters	Rule Name Packet Buffer

2.18.27. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipdatalen paramprobptr
Context Parameters	Rule Name Packet Buffer

2.19. L2TP

These log messages refer to the **L2TP (L2TP tunnel events)** category.

2.19.1. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.19.2. 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.
Gateway 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

2.19.3. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	iface remotegw

2.19.4. 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.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule tunnelid sessionid

2.19.5. 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.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule tunnelid sessionid

2.19.6. 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.
Gateway Action	drop

Recommended Action
Make sure no manually configured routes to the L2TP server interface exists in the configuration.

Revision
1

Parameters
iface

2.19.7. 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.

Gateway Action
None

Recommended Action
None.

Revision
1

Parameters
iface
sessionid
tunnelid

2.19.8. 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.

Gateway Action
None

Recommended Action
None.

Revision
1

Parameters
iface
tunnelid

2.19.9. 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.

Gateway Action
None

Recommended Action
Make sure the peer is capable of MPPE encryption, or disable the MPPE requirement.

Revision	1
Parameters	iface sessionid remotegw

2.19.10. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid

2.19.11. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid sessionid auth mppe

2.19.12. 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.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1

Parameters	tunnelid sessionid

2.19.13. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid

2.19.14. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid sessionid user auth mppe assigned_ip

2.19.15. 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.
Gateway Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.
Revision	1

2.19.16. l2tpclient_tunnel_up (ID: 02800018)

Default Severity	NOTICE
Log Message	L2TP tunnel to <remotegw> is up. Tunnel ID: <tunnelid>
Explanation	L2TP tunnel negotiated successfully.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid iface remotegw

2.19.17. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw error_code

2.19.18. 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.
Gateway 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

2.20. LICUPDATE

These log messages refer to the **LICUPDATE (License update)** category.

2.20.1. license_update_failure (ID: 05500001)

Default Severity	ALERT
Log Message	License update failed, because of <reason>
Explanation	The unit tried to update the license, but failed. The reason for this is specified in the "reason" parameter.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.20.2. license_downloaded (ID: 05500002)

Default Severity	NOTICE
Log Message	New license downloaded
Explanation	An updated license has been downloaded, which will now be used.
Gateway Action	using_new_license
Recommended Action	None.
Revision	1

2.20.3. license_already_up_to_date (ID: 05500003)

Default Severity	NOTICE
Log Message	License is up-to-date
Explanation	The current license is up-to-date, and does not need to be updated.
Gateway Action	None
Recommended Action	None.
Revision	1

2.21. PPP

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

2.21.1. 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.
Gateway 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

2.21.2. 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.
Gateway Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.21.3. 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.
Gateway Action	ppp_terminated
Recommended Action	None.

Revision 1

Parameters tunnel_type

2.21.4. 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.

Gateway Action ppp_terminated

Recommended Action None.

Revision 1

Parameters tunnel_type

2.21.5. 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.

Gateway Action ppp_terminated

Recommended Action None.

Revision 1

Parameters tunnel_type

2.21.6. 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.

Gateway Action ppp_terminated

Recommended Action None.

Revision 1

Parameters	tunnel_type

2.21.7. 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.
Gateway 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

2.21.8. 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.
Gateway 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

2.21.9. 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.
Gateway 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

2.21.10. 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.
Gateway Action	ppp_terminated
Recommended Action	Upgrade your license to allow more simultaneous PPP tunnels.
Revision	1
Parameters	tunnel_type limit

2.21.11. authentication_failed (ID: 02500101)

Default Severity	WARNING
Log Message	Authentication failed. PPP terminated
Explanation	Authentication failed. PPP terminated.
Gateway Action	ppp_terminated
Recommended Action	Make sure that the right username and password is used.
Revision	1
Parameters	tunnel_type user

2.21.12. 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.
Gateway Action	chap_response_value_truncated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.21.13. 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.
Gateway Action	chap_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.21.14. 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.
Gateway Action	mschapv1_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.21.15. 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.
Gateway Action	mschapv2_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.21.16. 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.

Gateway Action	pap_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.21.17. 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.
Gateway Action	pap_password_truncated
Recommended Action	Reconfigure the endpoints to use a shorter password.
Revision	1
Parameters	tunnel_type

2.21.18. unsupported_auth_server (ID: 02500500)

Default Severity	ERROR
Log Message	Unsupported authentication server. PPP Authentication terminated
Explanation	Unsupported authentication server. PPP Authentication terminated.
Gateway Action	authentication_terminated
Recommended Action	Review the authentication server configuration.
Revision	1
Parameters	tunnel_type

2.21.19. 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.
Gateway Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.21.20. 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.
Gateway Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.21.21. 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.
Gateway Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.21.22. 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.
Gateway 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

2.22. PPPOE

These log messages refer to the **PPPOE (PPPoE tunnel events)** category.

2.22.1. 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. .
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface pppoeserver auth ifaceip downtime

2.22.2. 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. .
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface pppoeserver uptime

2.23. PPTP

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

2.23.1. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.23.2. 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.
Gateway 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

2.23.3. 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.
Gateway Action	pptp_connection_closed
Recommended Action	Make sure the userauth rules are configured correctly.

Revision 1

Parameters rule
remotegw
callid

2.23.4. 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.

Gateway Action pptp_connection_closed

Recommended Action Make sure the userauth rules are configured correctly.

Revision 1

Parameters rule
remotegw
callid

2.23.5. 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.

Gateway Action None

Recommended Action None.

Revision 2

Parameters user
callid
remotegw

2.23.6. 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.
Gateway 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

2.23.7. 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.
Gateway 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

2.23.8. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw callid

2.23.9. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remotegw

2.23.10. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	iface type callid remotegw

2.23.11. 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.
Gateway Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.
Revision	1
Parameters	callid remotegw iface

2.23.12. 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.

Gateway Action None

Recommended Action None.

Revision 1

Parameters callid
iface
remotegw
user
auth
mppe
assigned_ip

2.23.13. 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.

Gateway Action None

Recommended Action None.

Revision 1

Parameters callid
iface
remotegw
auth
mppe

2.23.14. 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.

Gateway Action close_tunnel

Recommended Action None.

Revision 1

Parameters	iface remotegw

2.23.15. 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.
Gateway Action	close_session
Recommended Action	None.
Revision	1
Parameters	iface remotegw callid

2.23.16. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.23.17. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.23.18. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.23.19. 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.
Gateway 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

2.23.20. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.23.21. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.23.22. 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.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule iface remotegw

2.23.23. 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.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule iface remotegw

2.23.24. 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.

Gateway Action None

Recommended Action Make sure the userauth rules are configured correctly.

Revision 1

Parameters iface
remotegw

2.23.25. 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.

Gateway Action None

Recommended Action None.

Revision 1

Parameters iface
remotegw
error_code

2.23.26. 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.

Gateway 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

2.24. REASSEMBLY

These log messages refer to the **REASSEMBLY (Events concerning data reassembly)** category.

2.24.1. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Connection

2.24.2. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Connection

2.24.3. 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.
Gateway Action	correct the data
Recommended Action	Research the source of this errornous traffic.
Revision	1

Context Parameters	Connection

2.24.4. memory_allocation_failure (ID: 04800005)

Default Severity	ERROR
Log Message	Can't allocate memory to keep track of a packet
Explanation	The gateway is unable to allocate memory to keep track of packet that was received. The packet will be dropped.
Gateway Action	drop
Recommended Action	Review configuration to reduce memory consumption.
Revision	1

2.24.5. drop_due_to_buffer_starvation (ID: 04800007)

Default Severity	ERROR
Log Message	Can't allocate resources to process a packet
Explanation	The gateway 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.
Gateway Action	drop
Recommended Action	Check buffer consumption.
Revision	1

2.24.6. failed_to_send_ack (ID: 04800008)

Default Severity	ERROR
Log Message	Failed to send TCP ACK in response to a segment
Explanation	The gateway 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 gateway failed to allocate resources to send such an acknoledgement segment.
Gateway Action	none
Recommended Action	Check buffer consumption.
Revision	1

2.24.7. 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.
Gateway Action	drop
Recommended Action	Consider increasing the setting Reassembly_MaxProcessingMem.
Revision	1

2.24.8. 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.
Gateway Action	none
Recommended Action	Consider increasing the setting Reassembly_MaxConnections.
Revision	1
Context Parameters	Connection

2.24.9. 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.
Gateway Action	none
Recommended Action	Review configuration to reduce memory consumption.
Revision	1
Context Parameters	Connection

2.25. RULE

These log messages refer to the **RULE (Events triggered by rules)** category.

2.25.1. 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.
Gateway Action	fwdfast
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.25.2. ip_verified_access (ID: 06000005)

Default Severity	NOTICE
Log Message	IP address verfied according to ACCESS section
Explanation	The IP address was verified according to the ACCESS section.
Gateway Action	access_allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.3. 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.
Gateway Action	GOTO
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Rule Information

Packet Buffer

2.25.4. 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.

Gateway Action RETURN

Recommended Action None.

Revision 1

Context Parameters Rule Name
Rule Information
Packet Buffer

2.25.5. 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.

Gateway Action drop

Recommended Action Investigate why this traffic had the 0.* net as the destination.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.25.6. 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.

Gateway 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

2.25.7. 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.

Gateway Action drop

Recommended Action Investigate why this traffic had the 127.* net as the destination.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.25.8. 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.

Gateway 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

2.25.9. 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.

Gateway Action forward

Recommended Action None.

Revision 1

Context Parameters Rule Name

2.25.10. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.25.11. unknown_vlanid (ID: 06000040)

Default Severity	WARNING
Log Message	Received VLAN packet with unknown tag <vlanid>. Dropping
Explanation	The unit received a VLAN packet with an unknown tag, and the packet is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	2
Parameters	vlanid
Context Parameters	Rule Name Packet Buffer

2.25.12. 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.
Gateway Action	reject
Recommended Action	If this is not the indended behaviour, modify the rule-set.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.25.13. 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.
Gateway Action	drop
Recommended Action	If this is not the indended behaviour, modify the rule-set.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.25.14. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.26. SESMGR

These log messages refer to the **SESMGR (Session Manager events)** category.

2.26.1. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.26.2. 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.
Gateway Action	remove_session
Recommended Action	Check settings for users.
Revision	1
Parameters	user database ip type

2.26.3. 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.
Gateway Action	none
Recommended Action	None.

Revision	1
Parameters	user database ip type

2.26.4. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user access database ip type

2.26.5. 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.
Gateway Action	remove_session
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.26.6. 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.

Gateway Action	deny_upload
Recommended Action	Terminate administrator session and try again.
Revision	1
Parameters	user ip type

2.26.7. 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.
Gateway Action	remove_session
Recommended Action	Check maximum number of sessions and consoles.
Revision	1
Parameters	user database ip type

2.26.8. sesmgr_session_maximum_reached (ID: 04900008)

Default Severity	WARNING
Log Message	Maximum number of sessions reached
Explanation	Maximum number of sessions reached.
Gateway Action	deny_new_session
Recommended Action	Remove inactive sessions or increase maximum number of allowed sessions.
Revision	1

2.26.9. 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.
Gateway Action	none
Recommended Action	Check memory.

Revision	1

2.26.10. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.26.11. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.26.12. sesmgr_console_denied_init (ID: 04900012)

Default Severity	ALERT
Log Message	Could not create new console at initialization of Security Gateway for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Could not create new console at initialization of Security Gateway.
Gateway Action	remove_session
Recommended Action	Check maximum number of sessions and consoles.
Revision	1

Parameters	user database ip type

2.26.13. 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.
Gateway Action	deny_session
Recommended Action	Check user settings.
Revision	1
Parameters	user database ip type

2.26.14. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.26.15. sesmgr_file_error (ID: 04900017)

Default Severity	ALERT
Log Message	Error accessing files.
Explanation	Error occured when accessing files for reading/writing.
Gateway Action	file_error
Recommended Action	Check available memory.

Revision	1

2.26.16. sesmgr_techsupport (ID: 04900018)

Default Severity	NOTICE
Log Message	Sending technical support file.
Explanation	Technical support file created and is being sent to user.
Gateway Action	techsupport_created
Recommended Action	None.
Revision	1

2.27. SMTPLOG

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

2.27.1. 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.
Gateway Action	abort_sending
Recommended Action	Verify that a SMTP server is running at the address specified.
Revision	1
Parameters	smtp_server

2.27.2. 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.
Gateway Action	abort_sending
Recommended Action	Verify that a SMTP server is running at the address specified.
Revision	1
Parameters	smtp_server

2.27.3. 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.
Gateway Action	abort_sending
Recommended Action	None.
Revision	1
Parameters	smtp_server

2.27.4. 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.
Gateway Action	abort_sending
Recommended Action	None.
Revision	1
Parameters	smtp_server

2.27.5. 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.
Gateway Action	abort_sending
Recommended Action	Verify that a SMTP Server is configured to accept connections from the unit.
Revision	1
Parameters	smtp_server

2.27.6. 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.
Gateway Action	None
Recommended Action	If problems arise, verify that the SMTP server is properly configured.
Revision	1
Parameters	smtp_server

2.27.7. 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.
Gateway Action	abort_sending
Recommended Action	Verify that the SMTP server is configured to accept this sender.
Revision	1
Parameters	smtp_server sender

2.27.8. 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.
Gateway Action	None
Recommended Action	Verify that the SMTP server is configured to accept this recipient.
Revision	1
Parameters	smtp_server recipient

2.27.9. 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.
Gateway Action	None
Recommended Action	Verify that the SMTP server is configured to accept these recipients.
Revision	1
Parameters	smtp_server

2.27.10. 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.
Gateway Action	None

Recommended Action	Verify that the SMTP server is properly configured.
Revision	1
Parameters	smtp_server

2.27.11. 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.
Gateway Action	None
Recommended Action	Verify that the SMTP server is properly configured.
Revision	1
Parameters	smtp_server

2.28. SYSTEM

These log messages refer to the **SYSTEM (System-wide events: startup, shutdown, etc..)** category.

2.28.1. demo_expired (ID: 03200020)

Default Severity	EMERGENCY
Log Message	The DEMO period for this copy of D-Link DFL-160 has expired. Please install license and re-run D-Link DFL-160, or restart the firewall to initiate another evaluation session
Explanation	The unit will no longer operate, as the demo period has expired. Install a license in order to avoid this.
Gateway Action	shutdown
Recommended Action	Install a license.
Revision	1
Parameters	shutdown

2.28.2. demo_mode (ID: 03200021)

Default Severity	ALERT
Log Message	This copy of D-Link DFL-160 is in DEMO mode. Firewall core will halt in <time> seconds
Explanation	The unit is running in DEMO mode, and will eventually expire. Install a license in order to avoid this.
Gateway Action	shutdown_soon
Recommended Action	Install a license.
Revision	1
Parameters	shutdown time

2.28.3. 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.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters oldtime
newtime
user

2.28.4. reset_clock (ID: 03200101)

Default Severity	NOTICE
Log Message	The clock at <oldtime> was manually reset to <newtime>
Explanation	The clock has manually been reset.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	oldtime newtime

2.28.5. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.28.6. nitrox2_watchdog_triggered (ID: 03200207)

Default Severity	ERROR
Log Message	Nitrox II watchdog triggered.
Explanation	Nitrox II watchdog triggered.
Gateway Action	Reboot
Recommended Action	None.
Revision	1

2.28.7. nitrox2_restarted (ID: 03200208)

Default Severity	ERROR
Log Message	NITROX II interfaces restarted.
Explanation	NITROX II interfaces restarted.
Gateway Action	None
Recommended Action	None.
Revision	1

2.28.8. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	hardware_watchdog_chip watchdog_timeout

2.28.9. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason localip destip

2.28.10. 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.

Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason localip destip port_base port_end

2.28.11. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	localip destip

2.28.12. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	localip destip

2.28.13. 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.
Gateway 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

2.28.14. 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.
Gateway 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

2.28.15. ssl_encryption_failed (ID: 03200450)

Default Severity	ERROR
Log Message	Encryption failed.
Explanation	Encryption failed due to error. Connection closed.
Gateway Action	None
Recommended Action	None.
Revision	1

2.28.16. 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.
Gateway 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

2.28.17. disk_cannot_remove_file (ID: 03200601)

Default Severity	CRITICAL
Log Message	Failed to remove <file>, bi-directional communication will now probably be impossible
Explanation	The unit failed to remove the new, faulty, configuration file. It will still try to revert to the previous configuration file.
Gateway Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	file

2.28.18. 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.
Gateway Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	new_cfg

2.28.19. 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.
Gateway Action	None
Recommended Action	Verfiy that the disk media is intact, and that the file is not write protected.
Revision	1

Parameters	old_cfg

2.28.20. 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.
Gateway Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	cfg_new cfg_real

2.28.21. 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.
Gateway Action	None
Recommended Action	Consult the recommended action in the previous log message, which contained a more detailed error description.
Revision	1

2.28.22. 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.
Gateway Action	None
Recommended Action	Consult the recommended action in the previous log message, which contained a more detailed error description.
Revision	1

2.28.23. 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.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	localcfgver remotecfgver

2.28.24. shutdown (ID: 03201000)

Default Severity	NOTICE
Log Message	Shutdown <shutdown>. Active in <time> seconds. Reason: <reason>
Explanation	The unit is shutting down.
Gateway Action	shutdown
Recommended Action	None.
Revision	1
Parameters	shutdown time reason

2.28.25. shutdown (ID: 03201010)

Default Severity	NOTICE
Log Message	Reconfiguration aborted. Configuration files are missing
Explanation	The unit was issued a reconfigure command, but no configuration file is seen. The reconfiguration process is aborted.
Gateway Action	reconfigure_gateway_aborted
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	reason

2.28.26. 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.
Gateway Action	shutdown_gateway_aborted
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	shutdown reason core

2.28.27. config_activation (ID: 03201020)

Default Severity	NOTICE
Log Message	Reconfiguration requested by <username> from <config_system> <client_ip>.
Explanation	Reconfiguration requested.
Gateway Action	reconfiguration
Recommended Action	None.
Revision	1
Parameters	username userdb" client_ip config_system

2.28.28. 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.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	change_count

2.28.29. startup_normal (ID: 03202000)

Default Severity	NOTICE
Log Message	Security gateway starting. Core: <corever>. Build: <build>. Current uptime: <uptime>. Using configuration file <cfgfile>, version

<localcfgver> <remotecfgver>. Previous shutdown: <previous_shutdown>

Explanation The Security Gateway is starting up.

Gateway Action None

Recommended Action None.

Revision 2

Parameters corever
build
uptime
cfgfile
localcfgver
remotecfgver
previous_shutdown

2.28.30. startup_echo (ID: 03202001)

Default Severity NOTICE

Log Message Security gateway starting echo (<delay> seconds). Core: <corever>. Build: <build>. Current uptime: <uptime>. Using configuration file <cfgfile>, localcfgver <localcfgver>, remotecfgver <remotecfgver>. Previous shutdown: <previous_shutdown>

Explanation The Security Gateway is starting up, echo.

Gateway Action None

Recommended Action None.

Revision 2

Parameters delay
corever
build
uptime
cfgfile
localcfgver
remotecfgver
previous_shutdown

2.28.31. shutdown (ID: 03202500)

Default Severity NOTICE

Log Message Shutdown <shutdown>

Explanation The Security Gateway is shutting down.

Gateway Action shutdown

Recommended Action None.

Revision 1

Parameters	shutdown

2.28.32. admin_login (ID: 03203000)

Default Severity	NOTICE
Log Message	Administrative user <username> logged in via <authsystem>. Access level: <access_level>
Explanation	An adminsitrative user has logged in to the configuration system.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	authsystem username access_level [userdb] [server_ip] [server_port] [client_ip] [client_port]

2.28.33. admin_logout (ID: 03203001)

Default Severity	NOTICE
Log Message	Administrative user <username> logged out, via <authsystem>. Access level: <access_level>
Explanation	An adminsitrative user has logged out from the configuration system.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	authsystem username access_level [userdb] [client_ip]

2.28.34. 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 adminsitrative user failed to log in to configuration system. This is most likely due to an invalid entered username or password.

Gateway Action	disallow_admin_access
Recommended Action	None.
Revision	1
Parameters	authsystem username [server_ip] [server_port] [client_ip] [client_port]

2.28.35. 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.
Gateway 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

2.28.36. 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.
Gateway Action	using_new_config
Recommended Action	None.
Revision	1
Parameters	username userdb" client_ip config_system

2.28.37. 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.
Gateway Action	reconfiguration_using_old_config
Recommended Action	None.
Revision	1
Parameters	username userdb" client_ip config_system

2.28.38. 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.
Gateway Action	using_new_date_time
Recommended Action	None.
Revision	2
Parameters	authsystem user pre_change_date_time post_change_date_time

2.28.39. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	authsystem username userdb client_ip access_level

2.28.40. 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.

Gateway Action disallow_admin_access

Recommended Action None.

Revision 1

Parameters authsystem
username
server_ip
server_port
client_ip
client_port

2.28.41. 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.

Gateway Action disallow_admin_access

Recommended Action Please contact the support and report this issue.

Revision 1

Parameters authsystem
username
server_ip
server_port
client_ip
client_port

2.29. TCP_FLAG

These log messages refer to the **TCP_FLAG (Events concerning the TCP header flags)** category.

2.29.1. 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.
Gateway 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

2.29.2. 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.
Gateway 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

2.29.3. 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.

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

2.29.4. 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.
Gateway Action	strip_flag
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.29.5. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.29.6. 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.
Gateway 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

2.29.7. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.29.8. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	flags endpoint state
Context Parameters	Rule Name Connection Packet Buffer

2.29.9. mismatched_syn_resent (ID: 03300011)

Default Severity	WARNING
Log Message	Mismatched syn "resent" with seq <seqno>, expected <origseqno>. Dropping
Explanation	Mismatching sequence numbers. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno origseqno
Context Parameters	Rule Name Connection Packet Buffer

2.29.10. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno expectseqno
Context Parameters	Rule Name Connection Packet Buffer

2.29.11. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno expectseqno

Context Parameters	Rule Name Connection Packet Buffer

2.29.12. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno winstart winend
Context Parameters	Rule Name Connection Packet Buffer

2.29.13. 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.
Gateway Action	drop
Recommended Action	None.
Revision	2
Parameters	seqno accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.29.14. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ack accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.29.15. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.29.16. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno accstart accend

Context Parameters

Rule Name
Connection
Packet Buffer

2.29.17. 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.

Gateway 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]

2.29.18. 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.

Gateway 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]

2.29.19. 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.

Gateway Action	None
Recommended Action	None.
Revision	1

2.29.20. 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.
Gateway Action	drop
Recommended Action	None.
Revision	2
Parameters	seqno accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.30. TCP_OPT

These log messages refer to the **TCP_OPT (Events concerning the TCP header options)** category.

2.30.1. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.30.2. 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.
Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.30.3. 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.
Gateway Action	None

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

2.30.4. 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.
Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.30.5. 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.
Gateway Action	log
Recommended Action	None.
Revision	1
Parameters	tcpopt mss mssloglevel
Context Parameters	Rule Name Packet Buffer

2.30.6. 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.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.30.7. 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.
Gateway Action	strip
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.30.8. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt minoptlen avail
Context Parameters	Rule Name Packet Buffer

2.30.9. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt len avail
Context Parameters	Rule Name Packet Buffer

2.30.10. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt optlen expectlen
Context Parameters	Rule Name Packet Buffer

2.30.11. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1

Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.30.12. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.30.13. 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.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.30.14. tcp_null_flags (ID: 03400016)

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.
Gateway Action	drop

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

2.30.15. 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.
Gateway Action	strip
Recommended Action	None.
Revision	1
Context Parameters	Connection Packet Buffer

2.30.16. 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.
Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	shift_cnt
Context Parameters	Connection Packet Buffer

2.30.17. 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.

Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	old new effective
Context Parameters	Connection Packet Buffer

2.31. TIMESYNC

These log messages refer to the **TIMESYNC (Firewall time synchronization events)** category.

2.31.1. 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.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	oldtime newtime clockdrift timeserver

2.31.2. 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.
Gateway Action	clock_not_synced
Recommended Action	Verify that the time sync server is running.
Revision	1

2.31.3. 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.
Gateway Action	clock_not_synced
Recommended Action	If the correction interval is too narrow, it can be changed in the Advanced Settings section.

Revision	1
Parameters	clockdrift timeserver interval

2.32. TRANSPARENCY

These log messages refer to the **TRANSPARENCY (Events concerning the Transparent Mode feature)** category.

2.32.1. 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.
Gateway 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

2.32.2. 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.
Gateway Action	accept
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.32.3. 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.
Gateway Action	rewrite
Recommended Action	None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.32.4. 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.

Gateway 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

2.32.5. 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.

Gateway Action accept

Recommended Action None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.32.6. 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.

Gateway Action rewrite

Recommended Action None.

Revision 1

Context Parameters Rule Name
Packet Buffer

2.32.7. 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.

Gateway 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

2.32.8. relay_stp_frame (ID: 04400417)

Default Severity INFORMATIONAL

Log Message Relaying STP frame from <recvif> to switched interfaces

Explanation An incomming STP frame has been relayed to all switched interfaces in the same switch route as [recif].

Gateway Action allow

Recommended Action None.

Revision 1

Parameters recvif

2.32.9. dropped_stp_frame (ID: 04400418)

Default Severity INFORMATIONAL

Log Message Dropping STP frame from <recvif>

Explanation An incomming STP frame has been dropped.

Gateway Action drop

Recommended Action None.

Revision 1

Parameters recvif

2.32.10. invalid_stp_frame (ID: 04400419)

Default Severity	WARNING
Log Message	Incomming STP frame from <recvif> dropped. Reason: <reason>
Explanation	An incomming 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+.
Gateway Action	drop
Recommended Action	If the frame format is invalid, locate the unit which is sending the malformed frame.
Revision	1
Parameters	recvif reason

2.32.11. relay_mpls_frame (ID: 04400420)

Default Severity	INFORMATIONAL
Log Message	Forwarding MPLS packet from <recvif>.
Explanation	An incomming MPLS packet has been forwarded through the gateway. [destif] indicates if it was forwarded to an ultimate destination or if it was broadcasted to over all interfaces in the switch group.
Gateway Action	allow
Recommended Action	None.
Revision	1
Parameters	recvif destif

2.32.12. dropped_mpls_packet (ID: 04400421)

Default Severity	INFORMATIONAL
Log Message	Dropping MPLS packet from <recvif>
Explanation	An incomming MPLS packet has been dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	recvif

2.32.13. invalid_mpls_packet (ID: 04400422)

Default Severity	WARNING
Log Message	Incomming MPLS packet on <recvif> dropped. Reason: <reason>
Explanation	An incomming MPLS packet has been dropped since it was malformed.
Gateway Action	drop
Recommended Action	If the packet format is invalid, locate the unit which is sending the malformed packet.
Revision	1
Parameters	recvif reason

2.33. USERAUTH

These log messages refer to the **USERAUTH (User authentication (e.g. RADIUS) events)** category.

2.33.1. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.2. 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.
Gateway Action	ignore_packet
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.3. 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.
Gateway Action	accounting_disabled

Recommended Action Verify that the RADIUS Accounting server daemon is running on the Accounting Server.

Revision 1

Context Parameters User Authentication

2.33.4. 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.

Gateway Action accounting_disabled

Recommended Action Verify that the RADIUS Accounting server is properly configured.

Revision 1

Context Parameters User Authentication

2.33.5. 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.

Gateway Action logout_user

Recommended Action Verify that the RADIUS Accounting server daemon is running on the Accounting Server.

Revision 1

Context Parameters User Authentication

2.33.6. 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.

Gateway Action logout_user

Recommended Action Verify that the RADIUS Accounting server is properly configured.

Revision 1

Context Parameters User Authentication

2.33.7. 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.

Gateway Action None

Recommended Action None.

Revision 1

Context Parameters User Authentication

2.33.8. 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.

Gateway Action None

Recommended Action None.

Revision 1

Parameters
bytessent
bytesrecv
packetssent
packetsrecv
gigawrapsent
gigawraprecv
sestime

Context Parameters User Authentication

2.33.9. 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.
Gateway Action	ignore_packet
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.10. 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.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.33.11. 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.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server is properly configured.

Revision	1
Context Parameters	User Authentication

2.33.12. 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.
Gateway Action	accounting_disabled
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.13. 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.
Gateway 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	1
Context Parameters	User Authentication

2.33.14. 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.
Gateway 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	1
Context Parameters	User Authentication

2.33.15. 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.
Gateway Action	user_removed
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.16. user_timeout_removed_delayed_user (ID: 03700021)

Default Severity	NOTICE
Log Message	Delayed user timeout expired, user is removed
Explanation	User did not receive any Accounting Start Response from Radius.
Gateway Action	delayed_user_removed
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.17. 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.
Gateway Action	truncating_group_list
Recommended Action	Lower the number of groups that this user belongs to.

Revision	1
Parameters	username

2.33.18. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	bytessent bytesrecv packetssent packetsrecv gigawrapsent gigawraprecv sestime
Context Parameters	User Authentication

2.33.19. 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.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.33.20. 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.

Gateway Action None

Recommended Action Verify that the RADIUS Accounting server daemon is running on the Accounting Server.

Revision 1

Context Parameters User Authentication

2.33.21. 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.

Gateway Action None

Recommended Action Verify that the RADIUS Accounting server is properly configured.

Revision 1

Context Parameters User Authentication

2.33.22. 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.

Gateway Action ignore_packet

Recommended Action None.

Revision 1

Context Parameters	User Authentication

2.33.23. 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.
Gateway Action	logout_current_user
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.24. 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 .
Gateway Action	disallowed_login
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.25. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	idle_timeout session_timeout [groups]

Context Parameters	User Authentication

2.33.26. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.27. 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.
Gateway Action	None
Recommended Action	Verify that the RADIUS Authentication server daemon is running on the Authenication Server.
Revision	1
Context Parameters	User Authentication

2.33.28. manual_logout (ID: 03700106)

Default Severity	NOTICE
Log Message	User manually logged out
Explanation	A user manually logged out, and is no longer authenticated.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.29. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.30. challenges_not_supported (ID: 03700108)

Default Severity	NOTICE
Log Message	Challenges are not supported for this authentication system
Explanation	The XAuth authentication system does not support the challenge-and-response method.
Gateway Action	None
Recommended Action	Disable the challange-and-response feature, and use password verification instead.
Revision	1
Context Parameters	User Authentication

2.33.31. 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.
Gateway Action	None
Recommended Action	Verify that the LDAP Authentication server daemon is running on the Authenication Server.
Revision	1
Context Parameters	User Authentication

2.33.32. user_logout (ID: 03700110)

Default Severity	NOTICE
Log Message	User logged out

Explanation	A user logged out, and is no longer authenticated.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.33.33. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.33.34. 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.
Gateway Action	authentication_failed
Recommended Action	Check LDAP context to work.
Revision	1

2.33.35. ldap_user_authentication_successful (ID: 03700403)

Default Severity	NOTICE
Log Message	LDAP Authentication successful for <user>
Explanation	Authentication attempt successful.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	user

2.33.36. ldap_user_authentication_failed (ID: 03700404)

Default Severity	NOTICE
Log Message	LDAP Authentication failed for <user>
Explanation	Authentication attempt failed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	user

2.33.37. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.33.38. 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.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.33.39. 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.
Gateway Action	database connection disabled
Recommended Action	Check configuration.
Revision	1
Parameters	database

2.33.40. 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.
Gateway Action	authentication_failed
Recommended Action	Verify connecting client username and password.
Revision	1

2.33.41. 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.
Gateway Action	user authentication failed
Recommended Action	Check configuration for password attribute.
Revision	1
Parameters	database

2.33.42. 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.
Gateway Action	ssl_close
Recommended Action	Make sure that the client and unit share atleast one cipher.
Revision	1

Parameters	client_ip

2.33.43. 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.
Gateway 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

2.33.44. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.33.45. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1

Parameters	client_ip

2.33.46. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.33.47. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.33.48. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.33.49. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.33.50. 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.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.33.51. negotiated_cipher_does_not_permit_the_chosen_certificate_ (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.
Gateway Action	ssl_close
Recommended Action	Change ciphers and/or certificate.
Revision	1
Parameters	client_ip

2.33.52. 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.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	client_ip level description

2.33.53. 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.
Gateway Action	close
Recommended Action	Consult the "description" parameter, which contains the reason for this.
Revision	1
Parameters	client_ip level description