Fireware v12.3

Log Message Catalog

Copyright, Trademark, and Patent Information

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

Introduction to the Log Catalog

You can use the tools available in WatchGuard Dimension, WatchGuard System Manager (WSM), and Fireware Web UI to review the log messages and events that occur on your WatchGuard Firebox devices, to examine the activity on your network. Log messages give you important information about the flow of traffic through your network, and are a key component to help you troubleshoot problems on your network.

The *Fireware Log Catalog* describes many of the types of log messages that your Firebox can generate. It includes examples of log messages for Firebox devices that run Fireware OS, grouped by the product area.

All log messages included in the *Log Catalog* are first organized into topics by product area and then separated into sections in each topic by the log message type:

- ALARM — *Alarm* log messages
- DIAG — *Debug (Diagnostics)* log messages
- EVENT — *Event* log messages
- STAT — *Statistics* log messages
- TRAFFIC — *Traffic* log messages

For more information about log message types, see *About Log Messages*.

> Only log messages that are assigned a message ID number are included in the *Log Catalog*.

To review the log messages that are defined in the *Log Catalog*, you can expand the **Log Messages** section and select a topic for a product area, expand the section for a log message type, and review the log message lists to find a specific log message.

- To expand a single section, click ⊕.
- To collapse a single section, click ⊖.
- To expand all the sections in a topic, at the top of the topic window, click ▤.
- To collapse all the sections in a topic, at the top of the topic window, click ▤.

You can also search the *Log Catalog* for the specific details included in a log message.

For more information about options to search the *Log Catalog*, see Search the Log Catalog.

About Log Messages

Your Firebox can send log messages to an instance of Dimension, a WSM Log Server, or a syslog server. You can also configure your Firebox to store log messages locally on the Firebox. You can use Traffic Monitor in Fireware Web UI or Firebox System Manager (FSM) to review log messages in real-time. If you send log messages to Dimension, you can use the Dimension Log Manager to review the log messages from your Firebox devices. If you send log messages to a WSM Log Server, you can use Log Manager in WatchGuard WebCenter to review log messages after they are generated and processed by the Log Server.

Types of Log Messages

Firebox devices can send several types of log messages for events that occur on the Firebox. Each message includes the message type in the text of the message. The log messages types are:

- Traffic
- Alarm
- Event
- Debug (Diagnostic)
- Statistic

Traffic and event log messages, and some alarm log messages, automatically appear in Traffic Monitor by default; you do not have to enable any settings on your Firebox to generate them. The majority of the other log message types must be enabled in the device configuration file before they appear in Traffic Monitor or Log Manager.

Traffic Log Messages

Most of the log messages that appear in Traffic Monitor are traffic log messages. Traffic Monitor shows all of the log messages that are generated by your Firebox and are recorded in your log file. Traffic log messages show the traffic that moves through your Firebox and how the packet filter and proxy policies were applied. A traffic log message can include details that show how NAT (network address translation) was handled for a packet.

The traffic log messages for traffic managed by packet filter policies contain a set number of fields. The information for the same traffic log message will look different in Traffic Monitor than in Log Manager.

For a traffic log message generated by traffic managed by a proxy policy, your Firebox generates more than one log message. The first entry shows the same information as a packet filter log message, but includes this additional information:

proxy_act

> The name of the proxy action that handles this packet. A proxy action is a set of rules for a proxy that can be applied to more than one policy.

rule_name

> The name of the specific proxy rule that handles this packet.

content_type

> The type of content in the packet that is filtered by the proxy rule.

Other proxy log messages include a variable number of fields.

Alarm Log Messages

Alarm log messages are sent when an event occurs that triggers the Firebox to run a command. When the alarm condition is matched, the Firebox generates an alarm log message that you can see in Traffic Monitor, sends the log message to your Dimension server, WSM Log Server, or syslog server, and then it completes the specified action for the event.

You can configure your Firebox to send alarm log messages for specific events that occur on your device. For example, you can configure an alarm to occur when a specified value matches or exceeds a threshold. Other alarm log messages are set by the Firebox OS, with values that you cannot change. For example, the Firebox sends an alarm log message when a network connection on one of the Firebox interfaces fails, or when a Denial of Service attack occurs.

There are eight categories of alarm log messages:

- System
- IPS
- AV

- Policy
- Proxy
- Counter
- Denial of Service
- Traffic

The Firebox does not send more than 10 alarms in 15 minutes for the same conditions.

Event Log Messages

Event log messages are generated for activity on your Firebox that is related to actions by the Firebox and users. Actions that can cause the Firebox to send an event log message include:

- Firebox start up and shut down
- Firebox and VPN authentication
- Process start up and shut down
- Problems with Firebox hardware components
- Any task completed by a device administrator

Debug (Diagnostic) Log Messages

Debug log messages include detailed diagnostic information that you can use to help troubleshoot problems on your Firebox . There are 27 different product components that can send debug log messages. When you configure the logging settings on your Firebox you can specify the level of diagnostic logging to see for each different product component enabled on your Firebox. The available levels are:

- Off
- Error
- Warning
- Information
- Debug

Statistic Log Messages

Statistic log messages include information about the performance of your Firebox. You can configure your Firebox to generate log messages about external interface performance, VPN bandwidth statistics, and Security Services statistics. You can review these log messages to determine what changes are necessary in your Firebox settings to improve performance. To see these log messages, performance statistic logging must be enabled on the Firebox.

Read a Log Message

Each log message generated by your Firebox includes a string of data about the traffic on your Firebox. If you review the log messages in Traffic Monitor, the details in the data have different colors applied to them to help visually distinguish each detail.

Here is an example of one traffic log message from Traffic Monitor:

```
2014-07-02 17:38:43 Member2 Allow 192.168.228.202 10.0.1.1 webcache/tcp
42973 8080 3-Trusted 1-WCI Allowed 60 63 (Outgoing-proxy-00) proc_
id="firewall" rc="100" src_ip_nat="69.164.168.163" tcp_info="offset 10
S 2982213793 win 2105" msg_id="3000-0148"
```

When you read log messages, you can see details about when the connection for the traffic occurred, the source and destination of the traffic, as well as the disposition of the connection, and other details.

Each log message includes these details:

Time Stamp

The log message line begins with a time stamp that includes the time and date that the log message was created. The time stamp uses the time zone and current time from the Firebox.

This is the time stamp from the example log message above:

```
2014-07-02 17:38:43
```

FireCluster Member Information

If the log message is from a Firebox that is a member of a FireCluster, the log message includes the cluster member number for the Firebox.

This is the FireCluster member information from the example log message above:

```
Member2
```

Disposition

Each log message indicates the disposition of the traffic: Allow or Deny. If the log message is for traffic that was managed by a proxy policy instead of a packet filter policy, the traffic may be marked Allow even though the packet body was stripped or altered by the proxy action.

This is the disposition from the example log message above:

```
Allow
```

Source and Destination Addresses

After the disposition, the log message shows the actual source and destination IP addresses of the traffic. If NAT was applied to the traffic, the NAT addresses appear later in the log message.

These are the source and destination addresses from the example log message above:

```
192.168.228.202 and 10.0.1.1
```

Service and Protocol

The next entries in the log message are the service and protocol that managed the traffic. The service is specified based on the protocol and port the traffic used, not the name of the policy that managed the traffic. If the service cannot be determined, the port number appears instead.

These are the service and protocol from the example log message above:

```
webcache/tcp
```

Source and Destination Ports

The next details in the log message are the source and destination ports. The source port identifies the return traffic. The destination port determines the service used for the traffic.

These are the source and destination ports from the example log message above:

`42973` and `8080`

Source and Destination Interfaces

The source and destination interfaces appear after the destination port. These are the physical or virtual interfaces that handle the connection for this traffic.

These are the source and destination interfaces from the example log message above:

`3-Trusted` and `1-WCI`

Connection Action

This is the action applied to the traffic connection. For proxy actions, this indicates whether the contents of the packet are allowed, dropped, or stripped.

This is the connection action from the example log message above:

`Allowed`

Packet Length

The two packet length numbers indicate the packet length (in bytes) and the TTL (Time To Live) value. TTL is a metric used to prevent network congestion by only allowing the packet to pass through a specific number of routing devices before it is discarded.

These are the packet length numbers from the example log message above:

`60` (packet length) and `63` (TTL)

Policy Name

This is the name of the policy on your Firebox that handles the traffic. The number (-00) is automatically appended to policy names, and is part of the internal reference system on the Firebox.

This is the policy name from the example log message above:

`(Outgoing-proxy-00)`

Process

This section of the log message shows the process that handles the traffic.

This is the process from the example log message above:

`proc_id="firewall"`

Return Code

This is the return code for the packet, which is used in reports.

This is the return code from the example log message above:

`rc="100"`

NAT Address

This is the IP address that appears in place of the actual source IP address of the traffic after it leaves the Firebox interface and the NAT rules have been applied. A destination NAT IP address can also be included.

This is the NAT address from the example log message above:

`src_ip_nat="69.164.168.163"`

Packet Size

The tcp_info detail includes values for the offset, sequence, and window size for the packet that initiates the connection. The packet size details that are included depend on the protocol type.

This is the packet size from the example log message above:

`tcp_info="offset 10 S 2982213793 win 2105"`

Message Identification Number

Each type of log message includes a unique message identification number. When you review a log message in Traffic Monitor, the message ID number can appear as the value for either the `msg_id=` detail or the `id=` detail. In Log Manager, the message ID number appears as the value for the `id=` detail.

Some log messages do not include a message ID number. Only log messages that are assigned a message ID number are included in the *Log Catalog*.

The is the message ID number from the example log message above:

`msg_id="3000-0148"`

The message ID numbers included in the *Log Catalog* do not include the hyphens that appear in the message ID number in Traffic Monitor and Log Manager. To make sure you can locate the message ID number in the *Log Catalog*, when you search the *Log Catalog* for the message ID, remove the hyphen from the message ID number.

For example, to search for information about message ID number *3000-0148*, in the **Search Log Catalog** text box, type `300000148`.

Firewall Log Messages

Firewall log messages are generated by your Firebox for events that occur on the Firebox and for traffic managed by some packet filter policies. In addition to normal traffic, this can include messages related to feature keys, subscription services, server load balancing, and other features configured on your Firebox.

Alarm

Firewall log messages of the *Alarm* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
30000152	INFO	Firewall / Packet Filter	IPv4 source route attack	IPv4 source route attack from 10.0.1.34 detected.	IPv4 source route attack was detected.	IPv4 source route attack from %s detected.	IPv4 source route from ${src} detected.
30000153	INFO	Firewall / Packet Filter	IPv4 SYN flood attack	SYN flood attack against 10.0.1.51 from 216.3.21.4 detected.	IPv4 SYN flood attack was detected.	SYN flood attack against %s from %s detected.	SYN flood attack against ${dst} from ${src} detected.
30000154	INFO	Firewall / Packet Filter	IPv4 ICMP flood attack	ICMP flood attack against 10.0.1.51 from 216.3.21.4 detected.	IPv4 ICMP flood attack was detected.	ICMP flood attack against $dst from $src detected.	ICMP flood attack against ${dst} from ${src} detected.
30000155	INFO	Firewall / Packet Filter	IPv4 UDP flood attack	UDP flood attack against 32.21.56.8 from 12.34.23.67 detected.	IPv4 UDP flood attack was detected.	UDP flood attack against %s from %s detected.	UDP flood attack against ${dst} from ${src} detected.
30000156	INFO	Firewall / Packet Filter	IPv4 IPSEC flood attack	IPSEC flood attack against 32.21.56.8 from 12.34.23.67 detected.	IPv4 IPSEC flood attack was detected.	IPSEC flood attack against %s from %s detected.	IPSEC flood attack against $dst from $src detected.
30000157	INFO	Firewall	IPv4 IKE	IKE flood attack against 32.21.56.8 from 12.34.23.67 detected.	IPv4 IKE flood attack was detected	IKE flood attack against %s from %s detected.	IKE flood attack against ${dst} from ${src} detected.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		/ Packet Filter	flood attack				
30000158	INFO	Firewall / Packet Filter	IPv4 scan attack	IP scan attack against 32.21.56.8 from 12.34.23.67 detected.	IPv4 scan attack was detected.	IP scan attack against %s from %s detected.	IP scan attack against ${dst} from ${src} detected.
30000159	INFO	Firewall / Packet Filter	IPv4 port scan attack	PORT scan attack against 32.21.56.8 from 12.34.23.67 detected.	IPv4 port scan attack was detected.	PORT scan attack against %s from %s detected.	Port scan attack against ${dst} from ${src} detected.
30000160	INFO	Firewall / Packet Filter	IPv4 DDOS against server	DDOS against server 10.0.1.34 detected.	IPv4 DDOS attack against a server was detected.	DDOS against server %s detected.	DDOS against server ${dst} detected.
30000161	INFO	Firewall / Packet Filter	IPv4 DDOS attack from client	DDOS from client 10.0.1.34 detected.	IPv4 DDOS attack from a client was detected.	DDOS from client $src detected.	DDOS from client ${src} detected.
30000162	INFO	Firewall / Packet Filter	IPv6 SYN flood attack	SYN flood attack against 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 from FF01::101 detected.	IPv6 SYN flood attack was detected.	SYN flood attack against %s from %s detected.	SYN flood attack against ${dst} from ${src} detected.
30000163	INFO	Firewall / Packet Filter	IPv6 ICMP flood attack	ICMP flood attack against 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 from FF01::101 detected.	IPv6 ICMP flood attack was detected.	ICMP flood attack against %s from %s detected.	ICMP flood attack against ${dst} from ${src} detected.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
30000164	INFO	Firewall / Packet Filter	IPv6 UDP flood attack	UDP flood attack against 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 from FF01::101 detected.	IPv6 UDP flood attack was detected.	UDP flood attack against %s from %s detected.	UDP flood attack against ${dst} from ${src} detected.
30000165	INFO	Firewall / Packet Filter	IPv6 IPSEC flood attack	IPSEC flood attack against 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 from FF01::101 detected.	IPv6 IPSEC flood attack was detected.	IPSEC flood attack against %s from %s detected.	IPSEC flood attack against ${dst} from ${src} detected.
30000166	INFO	Firewall / Packet Filter	IPv6 IKE flood attack	IKE flood attack against 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 from FF01::101 detected.	IPv6 IKE flood attack was detected.	IKE flood attack against %s from %s detected.	IKE flood attack against ${dst} from ${src} detected.
30000167	INFO	Firewall / Packet Filter	Alarm Traffic matched policy	Policy Name: HTTP-00 Source IP Address: 10.0.1.20 Source Port: 4107 Destination IP Address: 61.135.169.125 Destination Port: 80	An alarm log message was sent for traffic that matched the specified policy.	Policy Name: %s Source IP Address: %s Source Port: %d Destination IP Address: %s Destination Port: %d	Policy Name: ${pcy_name} Source IP Address: ${src_ip} Source Port: ${src_port} Destination IP Address: ${dst_ip} Destination Port: ${dst_port}
30000168	INFO	Firewall / Packet Filter	Blocked site	Blocked site: Traffic detected from 10.0.1.2 to 61.231.45.165.	Traffic was detected to or from a blocked site.	Blocked site: Traffic detected from %src to %dst.	Blocked site: Traffic detected from ${src} to ${dst}.
30000169	INFO	Firewall / Packet Filter	IP spoofing	IP spoofing: Traffic detected from 10.0.1.2 to 43.123.12.26.	IP spoofing was detected from the IP address specified in the log message.	IP spoofing: Traffic detected from %src to %dst.	IP spoofing: Traffic detected from ${src} to ${dst}.
30000169	INFO	Firewall / Packet Filter	IP spoofing	IP spoofing: Traffic detected from 10.0.1.2 to 43.123.12.26.	IP spoofing was detected from the IP address specified in the log message.	IP spoofing: Traffic detected from %src to %dst.	IP spoofing: Traffic detected from ${src} to ${dst}.
30000170	INFO	Firewall	Connection	The total number of current sessions (1024)	The total number of current	The total number of current	The total number of current sessions

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		/ Packet Filter	table high water mark	has reached the high water mark (1024).	sessions reached the high water mark (80%) of the maximum connection table.	sessions (%u) has reached the high water mark (%d).	(${value1}) has reached the high water mark (${value2}).
30000170	INFO	Firewall / Packet Filter	Connection table high water mark	The total number of current sessions (1024) has reached the high water mark (1024).	The total number of current sessions reached the high water mark (80%) of the maximum connection table.	The total number of current sessions (%u) has reached the high water mark (%d).	The total number of current sessions (${value1}) has reached the high water mark (${value2}).
30000171	INFO	Firewall / Packet Filter	Conntrack table is full	The number of connections (2048) has reached the configured limit (2048).	The conntrack table is full. The number of connections has reached the configured limit.	The number of connections (%u) has reached the configured limit (%d).	The number of connections (${value1}) has reached the configured limit (${value2}).
30000172	INFO	Firewall / Packet Filter	Blocked port	Blocked port: Traffic detected from 10.0.1.2 to 61.231.45.165 on port 513.	Traffic was detected on a blocked port.	Blocked port: Traffic detected from %src to %dst on port %port.	Blocked port: Traffic detected from ${src} to ${dst} on port ${port}.

Diagnostic

Firewall log messages of the *Debug (Diagnostic)* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3000003A	ERROR	Firewall / Packet Filter	Unable to read feature keys	Unable to read the feature keys, some features may be unavailable	Unable to read feature keys file or fail to parse feature keys file. Features that require a correct feature key will not function.	Unable to read the feature keys, some features may be unavailable	—
3000003C	ERROR	Firewall / Packet Filter	No route to HTTP redirect host	Route look up on HTTP redirect host 192.168.111.10 for policy "FTP-00" failed, local redirect may not work	Route look up on HTTP redirect host for the specified policy failed, and local HTTP redirect may not work.	Route look up on HTTP redirect host %u.%u.%u.%u for policy "%s" failed, local redirect may not work	—
3000012E	ERROR	Firewall / Packet Filter	Possible loop or ARP spoofing detected	Cannot relearn system MAC address, possible loop or MAC spoofing, ip=192.168.111.10, mac=00:50:da:c7:90:5d, interface=5	The appliance received an ARP packet sent from one of its own MAC addresses. It is possibly a network or cabling loop, or another device is faking this device's MAC address.	Cannot relearn system MAC address, possible loop or MAC spoofing, ip=%hu.%hu.%hu.%hu, mac=%02x:%02x:%02x:%02x:%02x:%02x, interface=%u	Cannot relearn system MAC address, possible loop or another device is faking this device's MAC address, ip=${ip}, mac=${mac}, interface=${interface}
30000006	INFO	Firewall / Packet Filter	Feature settings updated	Application control settings updated	Firewall settings for the feature specified in the message have been updated	%s settings updated	—
30000027	INFO	Firewall / Packet Filter	Firewall is starting up	Firewall is starting up	—	Firewall is starting up	—
30000028	INFO	Firewall / Packet Filter	Firewall is shutting down	Firewall is shutting down	—	Firewall is shutting down	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
30000029	INFO	Firewall / Packet Filter	Address exempted from blocked sites	IP address 192.168.111.254 will not be added to the blocked sites list because it is exempt	The particular IP address is an exemption and will not be added to the blocked sites list	IP address %s will not be added to the blocked sites list because it is exempt	IP address ${ip} will not be added to the blocked sites list because it is exempt
30000040	INFO	Firewall / Packet Filter	Blocked site idle timeout	Idle timeout has occurred for blocked site 192.168.111.10	Idle timeout has occurred for the specified blocked site, and it will be removed from the blocked sites list.	Idle timeout has occurred for blocked site %s	—
3000002A	INFO	Firewall / Packet Filter	Address already blocked	IP address 192.168.111.10 will not be added to the blocked sites list because it already exists.	—	IP address %s will not be added to the blocked sites list because it already exists.	IP address ${ip} will not be added to the blocked sites list because it already exists.
3000012D	INFO	Firewall / Packet Filter	Verify ARP entry	Verify ARP entry for host at 192.168.111.10	The appliance sent an ARP request to verify learned ARP entry for a given host.	Verify ARP entry for host at %hu.%hu.%hu.%hu	—

Event

Firewall log messages of the *Event* log type.

ID	Level	Area	Name	Log Messag Example	Description	Format	Message Variables
3000012C	ERROR	Firewall / Packet Filter	ARP spoofing attack	ARP spoofing attack detected, ip=192.168.111.10, mac=00:50:da:c7:90:5d, interface=5	Detected an ARP spoofing attack. The log message specifies the source IP address, MAC address, and incoming interface of the ARP packet.	ARP spoofing attack detected, ip=%u.%u.%u.%u, mac=%02x:%02x:%02x:%02x:%02x:%02x, interface=%u	ARP spoofing attack detected, ip=${ip}, mac=${mac}, interface=${interface}
30000004	INFO	Firewall / Packet Filter	Application Control feature expired	The Application Control feature has expired.	The feature key for your Application Control subscription has expired.	The Application Control feature has expired.	—
30000005	INFO	Firewall / Packet Filter	IPS feature expired	The IPS feature has expired.	The feature key for your Intrusion Prevention Services subscription has expired.	The IPS feature has expired.	—
3000002F	INFO	Firewall / Packet Filter	Feature not supported by feature key	Feature key does not support the feature Policy based routing.	The device feature key does not support the specified feature.	Feature key does not support the feature %s.	No valid ${feature name} feature

ID	Level	Area	Name	Log Messag Example	Description	Format	Message Variables
300000C9	INFO	Firewall / Packet Filter	Load Balance Server (TCP Probe)	TCP probe packets timeout, Load Balance Server 10.10.10.100 port 3030 is offline.	Load Balance Server status update due to response or lack of response to a TCP Probe packet. The log message specifies the server IP address and port.	%s %s , Load Balance Server %hu.%hu.%hu.%hu port %d is %s.	${probe method} ${reason}, Load Balance Server ${ip} port ${port} is ${status}
300000CB	INFO	Firewall / Packet Filter	Load Balance Server (ICMP Probe)	ICMP probe packets timeout, Load Balance Server 10.10.10.100 is offline.	Update to status of Load Balance Server due to success or failure of ICMP Probe packet. The log message specifies the server IP and status.	%s %s , Load Balance Server %u.%u.%u.%u is %s.	${probe method} ${reason}, Load Balance Server ${ip} is ${status}

Traffic

Firewall log messages of the *Traffic* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
30000148	INFO	Firewall / Packet Filter	Normal traffic	Allow Firebox 0-External 52 tcp 20 127 10.0.1.2 206.190.60.138 62443 80 offset 8 S 832026162 win 8192 (HTTP-00)	Details of normal traffic either allowed or denied by the firewall policy specified in the log message.	%s %s %s %d %s %d %s %s %d %d offset %d %s %d %s %d(%s)	${disposition} ${inif} ${outif} ${ip_pkt_len} ${protocol} ${iph_len} ${TTL} {${src_ip}|${src_user}} {${dst_ip|${dst_user}} [${tcp_info}] [${udp_info}] [${icmp_info}] [${route_type}] ${policy_name}
30000149	INFO	Firewall / Packet Filter	Application Control Traffic identified	Allow 1-Trusted 0-External 40 tcp 20 127 10.0.1.2 206.190.60.138 53008 80 offset 5 AF 3212213617 win 257 app_name="World Wide Web HTTP" cat_name="Network Protocols" app_beh_name="connect" app_id="63" app_cat_id="18" app_ctl_disp="2" msg="Application identified" (HTTP-00)	Application Control identified traffic for an application.	%s %s %s %d %s %d %s %s %d %d offset %d %s %d %s %d app_name=\"%s\" cat_name=\"%s\" app_beh_name=\"%s\" appid=\"%d\" app_cat_id=\"%d\" app_ctl_disp=\"%d\" msg=\"%s\" (%s)	${disposition} ${inif} ${outif} ${ip_pkt_len} ${protocol} ${iph_len} ${TTL} {${src_ip}|${src_user}} {${dst_ip|${dst_user}} [${tcp_info}] [${udp_info}] app_name=${app_name} cat_name=${cat_name} app_beh_name=${app_beh_name} appid=${appid} app_cat_id=${app_cat_id} app_ctl_disp=${app_ctl_disp} msg=${msg} [${route_type}] ${policy_name}
30000150	INFO	Firewall / Packet Filter	IPS Traffic detected	Deny 1-Trusted 0-External 1440 tcp 20 61 10.0.1.2 192.168.130.126 55810 80 offset 5 A 447868619 win 54 signature_name="EXPLOIT Apple QuickTime FLIC Animation file buffer overflow -1-2" signature_cat="Misc" signature_id="1112464" severity="4" msg="IPS detected" (HTTP-00)	IPS detected traffic that matches an IPS signature.	%s %s %s %d %s %d %s %s %d %d offset %d %s %d %s %d signature_name=\"%s\" signature_cat=\"%s\" signature_id=\"%s\" severity=\"%d\" msg=\"%s\" (%s)	${disposition} ${inif} ${outif} ${ip_pkt_len} ${protocol} ${iph_len} ${TTL} {${src_ip}|${src_user}} {${dst_ip|${dst_user}} [${tcp_info}] [${udp_info}] signature_name=${signature_name} signature_cat=${signature_cat} signature_id=${signature_id} severity=${severity} msg=${msg} [${route_type}] ${policy_name}
30000151	INFO	Firewall / Packet Filter	Traffic connection terminated	Allow 1-Trusted 0-External tcp 10.0.1.2 220.181.90.24 53018 80 app_id="63" app_cat_id="18" app_ctl_disp="2" duration="80" sent_bytes="652" rcvd_bytes="423" (HTTP-00)	Record for a terminated connection	%s %s %s %d %s %d %s %s %d %d offset %d %s %d %s %d appid=\"%d\" app_cat_id=\"%d\" app_ctl_disp=\"%d\" duration=\"%d\" sent_	${disposition} ${inif} ${outif} ${ip_pkt_len} ${protocol} ${iph_len} ${TTL} {${src_ip}|${src_user}} {${dst_ip|${dst_user}} [${tcp_info}] [${udp_info}] appid=${appid} app_cat_id=${app_cat_id} app_ctl_disp=${app_ctl_disp} duration=${duration} sent_

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						bytes=\"%d\" rcvd_bytes=\"%d\" (%s)	bytes=${sent_bytes} rcvd_bytes=${rcvd_bytes} ${policy_name}
30000173	INFO	Firewall / Packet Filter	Hostile traffic	Deny 0-External Firebox 52 tcp 20 127 206.190.60.138 10.0.0.1 62443 80 offset 8 S 832026162 win 8192 blocked sites (Internal Policy)	Details of hostile traffic denied by the firewall internal policy.	%s %s %s %d %s %d %s %s %d %d offset %d %s %d %s %d(%s)	${inif} ${outif} ${ip_pkt_len} ${protocol} ${iph_len} ${TTL} {${src_ip}|${src_user}} {${dst_ip|${dst_user}} [${tcp_info}] [${udp_info}] [${icmp_info}]

Networking Log Messages

Networking log messages are generated for traffic related to the connections through your Firebox. This can include events related to interface activity, dynamic routing, PPPoE connections, DHCP server requests, FireCluster management, link monitoring, and wireless connections.

Diagnostic

Networking log messages of the *Debug (Diagnostic)* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
09000001	ERROR	Networking / PPPoE	Duplicate PPPoE Instance Error	Another instance of PPPoE is running	Another instance of the PPPoE process is already active in the system.	Another instance of PPPoE is running	—
09000002	ERROR	Networking / PPPoE	Invalid PPPoE automatic restart settings	PPPoE automatic restart settings are invalid, automatic restart will not be used	Automatic restart of PPPoE is disabled due to invalid settings.	PPPoE automatic restart settings are invalid, automatic restart will not be used	—
09000006	INFO	Networking / PPPoE	Initiate PPPoE automatic restart	Initiating PPPoE automatic restart	PPPoE instance will restart automatically.	Initiating PPPoE automatic restart	—
09000007	WARN	Networking / PPPoE	Skip PPPoE automatic restart	Skipped PPPoE automatic restart because the link was not up	PPPoE instance will not restart automatically due to no link.	Skipped PPPoE automatic restart because the link was not up	—
31000003	INFO	Networking / Network Management	Initiate gratuitous ARP	Initiating GARP for eth0	Initiate gratuitous ARP for the specified interface.	Initiating GARP for %s	Initiating GARP for ${dev_name}
31000004	INFO	Networking /	Initiate	Initiating GARP for all interfaces	Initiate gratuitous	Initiating GARP for all interfaces	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		Network Management	gratuitous ARP		ARP for all the interfaces.		
31000030	INFO	Networking / Network Management	Send interface logical link status event	[eth0] Sending interface status event, logical=up link=up ip=10.0.0.1 mask=255.255.255.0	Interface status event is sent for logical link status change.	[%s] Sending interface status event%s, logical=%s link=%s ip=%u.%u.%u.%u mask=%u.%u.%u.%u	[${dev_name}] Sending interface status event, logical=${logical} link=${link} ip=${ip} mask=${mask}
31000030	INFO	Networking / Network Management	Send interface logical link status event	[eth0] Sending interface status event, logical=up link=up ip=10.0.0.1 mask=255.255.255.0	Interface status event is sent for logical link status change.	[%s] Sending interface status event%s, logical=%s link=%s ip=%u.%u.%u.%u mask=%u.%u.%u.%u	[${dev_name}] Sending interface status event, logical=${logical} link=${link} ip=${ip} mask=${mask}
31000030	INFO	Networking / Network Management	Send interface logical link status event	[eth0] Sending interface status event, logical=up link=up ip=10.0.0.1 mask=255.255.255.0	Interface status event is sent for logical link status change.	[%s] Sending interface status event%s, logical=%s link=%s ip=%u.%u.%u.%u mask=%u.%u.%u.%u	[${dev_name}] Sending interface status event, logical=${logical} link=${link} ip=${ip} mask=${mask}
31000030	INFO	Networking / Network Management	Send interface logical link status event	[eth0] Sending interface status event, logical=up link=up ip=10.0.0.1 mask=255.255.255.0	Interface status event is sent for logical link status change.	[%s] Sending interface status event%s, logical=%s link=%s ip=%u.%u.%u.%u mask=%u.%u.%u.%u	[${dev_name}] Sending interface status event, logical=${logical} link=${link} ip=${ip} mask=${mask}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
31000030	INFO	Networking / Network Management	Send interface logical link status event	[eth0] Sending interface status event, logical=up link=up ip=10.0.0.1 mask=255.255.255.0	Interface status event is sent for logical link status change.	[%s] Sending interface status event%s, logical=%s link=%s ip=%u.%u.%u.%u mask=%u.%u.%u.%u	[${dev_name}] Sending interface status event, logical=${logical} link=${link} ip=${ip} mask=${mask}
31000031	INFO	Networking / Network Management	Send interface link status event	[eth0] Sending interface status event for link up	Interface status event is sent for link change.	[%s] Sending interface status event%s for link %s	[${dev_name}] Sending interface status event for link ${link}
31000031	INFO	Networking / Network Management	Send interface link status event	[eth0] Sending interface status event for link up	Interface status event is sent for link change.	[%s] Sending interface status event%s for link %s	[${dev_name}] Sending interface status event for link ${link}
31000034	INFO	Networking / Network Management	A change was made to the IP address of the external interface	[eth0 (External)] External Interface set IP address	Handle IP address for the specified external interface.	[%s (%s)] External Interface %s IP address	[${dev_name} (${if_name})] External Interface ${operation} IP address
31000034	INFO	Networking / Network Management	A change was made to the IP address of the external interface	[eth0 (External)] External Interface set IP address	Handle IP address for the specified external interface.	[%s (%s)] External Interface %s IP address	[${dev_name} (${if_name})] External Interface ${operation} IP address
31000034	INFO	Networking / Network Management	A change was made to the IP address of the external	[eth0 (External)] External Interface set IP address	Handle IP address for the specified external interface.	[%s (%s)] External Interface %s IP address	[${dev_name} (${if_name})] External Interface ${operation} IP address

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			interface				
31000035	ERROR	Networking / Network Management	Ignore unknown address operation	[eth0 (External)] Ignoring unknown address operation sss	Ignore unknown address operation on the specified interface.	[%s (%s)] Ignoring unknown address operation %s	[${dev_name} (${if_name})] Ignoring unknown address operation ${operation}
31000035	ERROR	Networking / Network Management	Ignore unknown address operation	[eth0 (External)] Ignoring unknown address operation sss	Ignore unknown address operation on the specified interface.	[%s (%s)] Ignoring unknown address operation %s	[${dev_name} (${if_name})] Ignoring unknown address operation ${operation}
31000035	ERROR	Networking / Network Management	Ignore unknown address operation	[eth0 (External)] Ignoring unknown address operation sss	Ignore unknown address operation on the specified interface.	[%s (%s)] Ignoring unknown address operation %s	[${dev_name} (${if_name})] Ignoring unknown address operation ${operation}
31000036	INFO	Networking / Network Management	Layer 2 traffic gate is closed	[Cluster] The traffic gate of layer2 is closed due to cluster role backup	Layer 2 traffic gate is closed due to the specified reason.	[Cluster] The traffic gate of layer2 is closed due to cluster role %s	[Cluster] The traffic gate of layer2 is closed due to cluster role ${role}
31000037	INFO	Networking / Network Management	Layer 2 traffic gate is opened	[Cluster] The traffic gate of layer2 is opened due to cluster role master	Layer 2 traffic gate is opened due to the specified reason.	[Cluster] The traffic gate of layer2 is opened due to cluster role %s	[Cluster] The traffic gate of layer2 is opened due to cluster role ${role}
31000038	INFO	Networking / Network Management	Traffic signal changed	[Cluster] Traffic signal become green	Traffic signal is changed to the specified status.	[Cluster] Traffic signal become %s	[Cluster] Traffic signal become ${status}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
31000050	INFO	Networking / Network Management	Starting wireless AP	Starting wireless AP ath1	Starting specified wireless AP.	Starting wireless AP %s	—
31000051	INFO	Networking / Network Management	Stopping wireless AP	Stopping wireless AP ath1	Stopping the specified wireless Access Point.	Stopping wireless AP %s	—
31000057	INFO	Networking / Network Management	Start processing configuration	Starts processing a configuration setting	Started to process configuration settings.	Starts processing a configuration setting	—
31000058	INFO	Networking / Network Management	Update bridge mode settings	Updating global bridge mode setting	Update global bridge mode settings.	Updating global bridge mode setting	—
31000059	INFO	Networking / Network Management	Update drop-in mode settings	Updating global drop-in mode setting	Update global drop-in mode settings.	Updating global drop-in mode setting	—
31000070	INFO	Networking / Network Management	Clean up stale connections	[Cluster] Clean up stale IP connections with expired address 192.168.1.22 for PPPoE interface eth0	Clean up stale connections for the expired IP address on dynamic interface.	[Cluster] Clean up stale IP connections with expired address %s for %s interface %s	[Cluster] Clean up stale IP connections with expired address ${ip} for dynamic interface ${dev_name}
31000070	INFO	Networking / Network Management	Clean up stale connections	[Cluster] Clean up stale IP connections with expired address 192.168.1.22 for PPPoE interface eth0	Clean up stale connections for the expired IP address on dynamic interface.	[Cluster] Clean up stale IP connections with expired address %s for %s interface %s	[Cluster] Clean up stale IP connections with expired address ${ip} for dynamic interface ${dev_name}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
31000075	ERROR	Networking / Network Management	DNSWatch servers should not be in use	DNSWatch is expired or was disabled. Your Firebox does not have a configured DNS server. To make sure your Firebox does not use the DNSWatch servers, you must specify a DNS server in the network DNS/WINS settings.	DNSWatch servers should not be in use but the Firebox does not have an alternative DNS server it can use.	DNSWatch is expired or was disabled. Your Firebox does not have a configured DNS server. To make sure your Firebox does not use the DNSWatch servers, you must specify a DNS server in the network DNS/WINS settings.	—
31130001	ERROR	Networking / Network Management	Capture stopped	Capture stopped, insufficient space	Capture stopped due to the specified reason.	Capture stopped, %s	Capture stopped, ${reason}
45000001	ERROR	Networking / Modem	Duplicate modem instance running	Another instance of Modem is running	System loaded Modem process, but another instance is already active.	Another instance of Modem is running	—
3100000F	INFO	Networking / Network Management	Add bridge interface	Adding bridge tbr0	Add bridge interface in bridge mode.	Adding bridge %s	Adding bridge ${dev_name}
3100003D	INFO	Networking / Network Management	Update ARP rules	[Cluster] Update arp rules for cluster role backup	Update ARP rules for the specified cluster role.	[Cluster] Update arp rules for cluster role %s	[Cluster] Update arp rules for cluster role ${role}
3100004F	INFO	Networking / Network Management	Fix up multipath gateways	[ECMP] Fixup 2 multipath gateway successfully	Fix up multipath gateways of the specified number successfully.	[ECMP] Fixup %d multipath gateway successfully	[ECMP] Fixup ${num} multipath gateway successfully
3100005A	INFO	Networking / Network Management	Update wireless settings	Updating wireless setting	Update wireless settings	Updating wireless setting	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3100005B	INFO	Networking / Network Management	Update secondary IP settings	Updating Trust-1 secondary IP(s) setting	Update secondary IP address settings for the specified interface.	Updating %s secondary IP(s) setting	Updating ${if_name} secondary IP (s) setting
3100005C	INFO	Networking / Network Management	Update route settings	Updating route setting	Update route settings.	Updating route setting	—
3100005D	INFO	Networking / Network Management	Update 1to1 NAT settings	Updating 1to1 NAT setting	Update 1-to-1 NAT settings.	Updating 1to1 NAT setting	—
3100005E	INFO	Networking / Network Management	Update DNS settings	Updating DNS setting	Update DNS settings.	Updating DNS setting	—
5A000001	INFO	Networking / Dynamic DNS	Response from Dynamic DNS server	Response from server: update succeeded with no change, abusive warning (1)	Receive the specified response from the dynamic DNS server.	Response from server: %s (%d)	Response from server: ${response} (${ret_code})
5A000001	INFO	Networking / Dynamic DNS	Response from Dynamic DNS server	Response from server: update succeeded with no change, abusive warning (1)	Receive the specified response from the dynamic DNS server.	Response from server: %s (%d)	Response from server: ${response} (${ret_code})
5A000002	INFO	Networking / Dynamic DNS	Dynamic DNS Domain Name Resolved	Resolved domain members.dyndns.org to 204.13.248.111	Dynamic DNS server domain name successfully resolved to an IP address.	Resolved domain %s to %s	Resolved domain ${domain} to ${ip}
5A000002	INFO	Networking / Dynamic DNS	Dynamic DNS Domain	Resolved domain members.dyndns.org to 204.13.248.111	Dynamic DNS server domain name successfully	Resolved domain %s to %s	Resolved domain ${domain} to ${ip}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			Name Resolved		resolved to an IP address.		
5A000003	INFO	Networking / Dynamic DNS	Connected to the server	Connected to: members.dyndns.org / 204.13.248.111	Connected to the specified dynamic DNS server.	Connected to: %s / %s	Connected to: ${server_name} / ${server_ip}
5A000003	INFO	Networking / Dynamic DNS	Connected to the server	Connected to: members.dyndns.org / 204.13.248.111	Connected to the specified dynamic DNS server.	Connected to: %s / %s	Connected to: ${server_name} / ${server_ip}
5A000004	INFO	Networking / Dynamic DNS	Connecting to the server	Connecting to: members.dyndns.com / 204.13.248.111	Connecting to the specified dynamic DNS server.	Connecting to: %s / %s	Connecting to: ${server_name} / ${server_ip}
5A000004	INFO	Networking / Dynamic DNS	Connecting to the server	Connecting to: members.dyndns.com / 204.13.248.111	Connecting to the specified dynamic DNS server.	Connecting to: %s / %s	Connecting to: ${server_name} / ${server_ip}
5A000005	INFO	Networking / Dynamic DNS	Activate dynamic DNS	Activating DynDNS on interface: External	Activate dynamic DNS on the specified interface.	Activating DynDNS on interface: %s	Activating DynDNS on interface: ${if_name}
5A000006	DEBUG	Networking / Dynamic DNS	Received reply from the server	Received reply: HTTP/1.1 200 OK Date: Tue, 27 Nov 2012 17:14:57 GMT Server: Apache Content-Type: text/plain Connection: close good 192.168.53.88	Received the specified reply from the dynamic DNS server.	Received reply: %s	Received reply: ${reply}
5A000007	ERROR	Networking / Dynamic DNS	Unable to resolve domain name	Could not resolve server: members.dyndns.org	Could not resolve domain for dynamic DNS server.	Could not resolve server: %s	Could not resolve server: ${server}
5A000008	ERROR	Networking / Dynamic DNS	Failed to connect to the server	Could not connect to members.dyndns.org / 204.13.248.111, connection refused	Could not connect to the dynamic DNS server due to specified reason.	Could not connect to %s / %s, %m	Could not connect to ${server_name} / ${server_ip}, ${reason}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
5A000008	ERROR	Networking / Dynamic DNS	Failed to connect to the server	Could not connect to members.dyndns.org / 204.13.248.111, connection refused	Could not connect to the dynamic DNS server due to specified reason.	Could not connect to %s / %s, %m	Could not connect to ${server_name} / ${server_ip}, ${reason}
5A000008	ERROR	Networking / Dynamic DNS	Failed to connect to the server	Could not connect to members.dyndns.org / 204.13.248.111, connection refused	Could not connect to the dynamic DNS server due to specified reason.	Could not connect to %s / %s, %m	Could not connect to ${server_name} / ${server_ip}, ${reason}
5A000009	ERROR	Networking / Dynamic DNS	Unable to connect to server	Unable to connect to server: members.dyndns.org / 204.13.248.111	Unable to connect to the specified dynamic DNS server.	Unable to connect to server: %s / %s	Unable to connect to server: ${server_name} / ${server_ip}
5A000009	ERROR	Networking / Dynamic DNS	Unable to connect to server	Unable to connect to server: members.dyndns.org / 204.13.248.111	Unable to connect to the specified dynamic DNS server.	Unable to connect to server: %s / %s	Unable to connect to server: ${server_name} / ${server_ip}
5A00000A	ERROR	Networking / Dynamic DNS	No response from server	No response from server members.dyndns.org / 204.13.248.111	Not able to get response from specified dynamic DNS server.	No response from server %s / %s	No response from server ${server_name} / ${server_ip}
5A00000A	ERROR	Networking / Dynamic DNS	No response from server	No response from server members.dyndns.org / 204.13.248.111	Not able to get response from specified dynamic DNS server.	No response from server %s / %s	No response from server ${server_name} / ${server_ip}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
5A00000B	ERROR	Networking / Dynamic DNS	Invalid response from server	Invalid response from server (-2)	The dynamic DNS server returned an invalid response code. The log message specifies that code.	Invalid response from server (%d)	Invalid response from server (${ret_code})
5A00000C	INFO	Networking / Dynamic DNS	The time for next update	Next update is on Tue, 27 Nov 2012 17:14:57	The log message specifies the next update time for dynamic DNS.	Next update is on %s	Next update is on ${time}
5A00000D	DEBUG	Networking / Dynamic DNS	Send update request	Sending update request (138 bytes): GET /nic/update?system=dyndns	Sending dynamic DNS update request. The log message specifies the size and content of the request.	Sending update request (%zu bytes): %s	Sending update request (${size} bytes): ${content}
5A00000D	DEBUG	Networking / Dynamic DNS	Send update request	Sending update request (138 bytes): GET /nic/update?system=dyndns	Sending dynamic DNS update request. The log message specifies the size and content of the request.	Sending update request (%zu bytes): %s	Sending update request (${size} bytes): ${content}

Event

Networking log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
09000004	ERROR	Networking / PPPoE	Authentication failure	PPPoE authentication failed	The Firebox or XTM device failed to authenticate for PPPoE.	PPPoE authentication failed	—
09000005	ERROR	Networking / PPPoE	PPPoE stopped	PPPoE stopped unexpectedly (unknown error)	PPPoE stopped unexpectedly due to an unknown error.	PPPoE stopped unexpectedly (unknown error)	—
09000008	INFO	Networking / PPPoE	Enforce static IP address	[eth2 (External)] Enforced PPPoE static IP address: 192.168.3.48 is replaced with 192.168.3.29	Replaced the assigned PPPoE IP address with the configured static IP address. The assigned IP address is retained as a secondary IP address for the interface.	[%s (%s)] Enforced PPPoE static IP address: %s is replaced with %s	[${dev_name} (${if_name})] Enforced PPPoE static IP address: ${nego_ip} is replaced with ${static_ip}
09000008	INFO	Networking / PPPoE	Enforce static IP address	[eth2 (External)] Enforced PPPoE static IP address: 192.168.3.48 is replaced with 192.168.3.29	Replaced the assigned PPPoE IP address with the configured static IP address. The assigned IP address is retained as a secondary IP address for the interface.	[%s (%s)] Enforced PPPoE static IP address: %s is replaced with %s	[${dev_name} (${if_name})] Enforced PPPoE static IP address: ${nego_ip} is replaced with ${static_ip}
09000008	INFO	Networking / PPPoE	Enforce static IP address	[eth2 (External)] Enforced PPPoE static IP address: 192.168.3.48 is replaced with 192.168.3.29	Replaced the assigned PPPoE IP address with the configured static IP address. The assigned IP address is retained as a secondary IP address for the interface.	[%s (%s)] Enforced PPPoE static IP address: %s is replaced with %s	[${dev_name} (${if_name})] Enforced PPPoE static IP address: ${nego_ip} is replaced with ${static_ip}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
09000008	INFO	Networking / PPPoE	Enforce static IP address	[eth2 (External)] Enforced PPPoE static IP address: 192.168.3.48 is replaced with 192.168.3.29	Replaced the assigned PPPoE IP address with the configured static IP address. The assigned IP address is retained as a secondary IP address for the interface.	[%s (%s)] Enforced PPPoE static IP address: %s is replaced with %s	[${dev_name} (${if_name})] Enforced PPPoE static IP address: ${nego_ip} is replaced with ${static_ip}
09000009	INFO	Networking / PPPoE	Session established	[eth0 (External)] PPPoE session [11] is established, acquired IP address 192.168.3.48, peer 192.168.3.254	The specified interface established a PPPoE session. The log message also specifies the session ID, acquired IP address, and peer IP address.	[%s (%s)] PPPoE session[%d] is established, acquired IP address %s, peer %s	[${physical_name} (${ifname})] PPPoE session[${session_id}] is established, acquired IP address ${ipaddr}, peer ${peer_addr}
09000009	INFO	Networking / PPPoE	Session established	[eth0 (External)] PPPoE session [11] is established, acquired IP address 192.168.3.48, peer 192.168.3.254	The specified interface established a PPPoE session. The log message also specifies the session ID, acquired IP address, and peer IP address.	[%s (%s)] PPPoE session[%d] is established, acquired IP address %s, peer %s	[${physical_name} (${ifname})] PPPoE session[${session_id}] is established, acquired IP address ${ipaddr}, peer ${peer_addr}
09000009	INFO	Networking / PPPoE	Session established	[eth0 (External)] PPPoE session [11] is established, acquired IP address 192.168.3.48, peer 192.168.3.254	The specified interface established a PPPoE session. The log message also specifies the session ID, acquired IP address, and peer IP address.	[%s (%s)] PPPoE session[%d] is established, acquired IP address %s, peer %s	[${physical_name} (${ifname})] PPPoE session[${session_id}] is established, acquired IP address ${ipaddr}, peer ${peer_addr}
09000009	INFO	Networking / PPPoE	Session established	[eth0 (External)] PPPoE session [11] is established, acquired IP address 192.168.3.48, peer 192.168.3.254	The specified interface established a PPPoE session. The log message also specifies the session ID, acquired IP address, and peer IP address.	[%s (%s)] PPPoE session[%d] is established, acquired IP address %s, peer %s	[${physical_name} (${ifname})] PPPoE session[${session_id}] is established, acquired IP address ${ipaddr}, peer ${peer_addr}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
09000009	INFO	Networking / PPPoE	Session established	[eth0 (External)] PPPoE session [11] is established, acquired IP address 192.168.3.48, peer 192.168.3.254	The specified interface established a PPPoE session. The log message also specifies the session ID, acquired IP address, and peer IP address.	[%s (%s)] PPPoE session[%d] is established, acquired IP address %s, peer %s	[${physical_name} (${ifname})] PPPoE session[${session_id}] is established, acquired IP address ${ipaddr}, peer ${peer_addr}
16000001	ERROR	Networking / DHCP Server	DHCP discover	DHCPDISCOVER from 00:50:04:ce:c6:3d via eth1: network 192.168.111.0/24: no free leases	Received DHCP discover from the client, but there are no free leases available.	%s	—
16000002	INFO	Networking / DHCP Server	DHCP offer	DHCPOFFER on 192.168.111.20 to 84:2b:2b:a6:02:3f (client) via eth1	The DHCP server offered an IP address to the specified client device.	%s	—
16000003	INFO	Networking / DHCP Server	DHCP request	DHCPREQUEST for 192.168.111.20 from 84:2b:2b:a6:02:3f (client) via eth1	Received DHCP request for specified IP address from the specified client.	%s	—
31000009	INFO	Networking / Network Management	Interface initializing	[eth1 (Trusted)] Interface initializing	Initializing the specified interface.	[%s (%s)] Interface initializing	[${dev_name} (${if_name})] Interface initializing
31000009	INFO	Networking / Network Management	Interface initializing	[eth1 (Trusted)] Interface initializing	Initializing the specified interface.	[%s (%s)] Interface initializing	[${dev_name} (${if_name})] Interface initializing
31000010	ERROR	Networking / Network Management	Failed to add bridge	Failed to add bridge tbr0 VLAN ID 1	Failed to add bridge	Failed to add bridge %s VLAN ID %d	—
31000029	ERROR	Networking / Network	Failed to add interface IP	[eth1 (Trusted)] Failed to add address 198.51.100.0	Failed to add the specified IP address to the specified	[%s (%s)] Failed to %s address %s	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		Management	address		interface.		
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000039	INFO	Networking / Network Management	Cluster management interface change	[Cluster] Management interface setting is changed: interface from eth1 to eth2, IPv4 address from 10.0.1.3 to 10.0.2.3, IPv4 mask from 24 to 24, IPv6 CIDR from 2000::1/64 to 2001::2/64	The configuration for the cluster management interface changed. The log message specifies changes to the interface, IP address, mask and IPv6 address.	[Cluster] Management interface setting is changed: interface from %s to %s, IPv4 address from %u.%u.%u.%u to %u.%u.%u.%u IPv4 mask from %d to %d IPv6 CIDR from %s to %s%s	[Cluster] Management interface setting is changed: interface from ${pre_if} to ${new_if}, IPv4 address from ${pre_ip} to ${new_ip} IPv4 mask from ${pre_mask} to ${new_mask} IPv6 CIDR from ${pre_ipv6} to %{new_ipv6}%s
31000046	INFO	Networking / Network Management	Activating external interface	[eth0 (External)] Activating external interface	Activating specified external interface.	[%s (%s)] Activating external interface	[${dev_name} (${if_name})] Activating external interface

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
31000046	INFO	Networking / Network Management	Activating external interface	[eth0 (External)] Activating external interface	Activating specified external interface.	[%s (%s)] Activating external interface	[${dev_name} (${if_name})] Activating external interface
31000047	INFO	Networking / Network Management	Deactivating external interface	[eth0 (External)] Deactivating external interface	Deactivating the specified external interface.	[%s (%s)] Deactivating external interface	[${dev_name} (${if_name})] Deactivating external interface
31000047	INFO	Networking / Network Management	Deactivating external interface	[eth0 (External)] Deactivating external interface	Deactivating the specified external interface.	[%s (%s)] Deactivating external interface	[${dev_name} (${if_name})] Deactivating external interface
31000052	INFO	Networking / Network Management	Starting wireless AP service	Starting wireless AP service	Starting wireless AP service.	Starting wireless AP service	—
31000054	INFO	Networking / Network Management	Detect rogue wireless AP	Starting the scan for rogue wireless AP detection	Starting rogue wireless AP detection scan.	Starting the scan for rogue wireless AP detection	—
31000055	INFO	Networking / Network Management	Stop detecting rogue wireless AP	Stopping the scan for rogue wireless AP detection	Stopping rogue wireless AP detection scan.	Stopping the scan for rogue wireless AP detection	—
31000056	INFO	Networking / Network Management	Restart detecting rogue wireless AP	Restart the scan for rogue wireless AP detection	Restart rogue wireless AP detection scan.	Restart the scan for rogue wireless AP detection	—
31000069	INFO	Networking / Network Management	IPv6 interface activated.	[eth0 (External)] IPv6 interface is activated.	An IPv6 interface was activated. The log message specifies the interface.	[%s (%s)] IPv6 interface is activated.	—
31000071	INFO	Networking / Network Management	PPPoE IP address change during	[eth0 (External)] PPPoE IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the PPPoE IP address changed.	[%s (%s)] PPPoE IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] PPPoE IP address changes during cluster failover, from ${pre_ip} to ${new_ip}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			cluster failover				
31000071	INFO	Networking / Network Management	PPPoE IP address change during cluster failover	[eth0 (External)] PPPoE IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the PPPoE IP address changed.	[%s (%s)] PPPoE IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] PPPoE IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
31000071	INFO	Networking / Network Management	PPPoE IP address change during cluster failover	[eth0 (External)] PPPoE IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the PPPoE IP address changed.	[%s (%s)] PPPoE IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] PPPoE IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
31000071	INFO	Networking / Network Management	PPPoE IP address change during cluster failover	[eth0 (External)] PPPoE IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the PPPoE IP address changed.	[%s (%s)] PPPoE IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] PPPoE IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
31000072	INFO	Networking / Network Management	No change for PPPoE IP address during cluster failover	[eth0 (External)] PPPoE IP address 192.168.1.22 did not change during cluster failover	PPPoE IP address did not change during cluster failover.	[%s (%s)] PPPoE IP address %u.%u.%u.%u did not change during cluster failover	—
31000073	INFO	Networking / Network Management	DHCP IP address change during cluster failover	[eth0 (External)] DHCP IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the DHCP IP address changed.	[%s (%s)] DHCP IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] DHCP IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
31000073	INFO	Networking / Network Management	DHCP IP address change during	[eth0 (External)] DHCP IP address changed during cluster failover, from 192.168.1.22 to	The cluster completed a failover. During the failover, the DHCP IP address	[%s (%s)] DHCP IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] DHCP IP address changes during cluster failover, from ${pre_ip} to ${new_ip}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			cluster failover	192.168.1.23	changed.		
31000073	INFO	Networking / Network Management	DHCP IP address change during cluster failover	[eth0 (External)] DHCP IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the DHCP IP address changed.	[%s (%s)] DHCP IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] DHCP IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
31000073	INFO	Networking / Network Management	DHCP IP address change during cluster failover	[eth0 (External)] DHCP IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the DHCP IP address changed.	[%s (%s)] DHCP IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] DHCP IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
31000074	INFO	Networking / Network Management	No change for DHCP IP address during cluster failover	[eth0 (External)] DHCP IP address 192.168.1.22 did not change during cluster failover	DHCP IP address did not change during cluster failover.	[%s (%s)] DHCP IP address %u.%u.%u.%u did not change during cluster failover	—
45000003	INFO	Networking / Modem	Modem disconnected	modem0 disconnected	Specified modem is disconnected.	%s disconnected	—
45000004	ERROR	Networking / Modem	Modem authentication failed	Modem authentication failed, check your modem configuration	Modem authentication failed.	Modem authentication failed, check your modem configuration	—
49000001	ERROR	Networking / Link Monitoring	Multi-WAN Domain Name Resolution Failed	[Link Monitor] External unable to resolve domain name www.example.com	Specified interface failed to resolve specified domain name for ping or TCP test for failover.	[Link Monitor] %s unable to resolve domain name %s	—
49000002	WARN	Networking / Link Monitoring	Multi-Wan Probe Failed	[Link Monitor] No response received on External from TCP host 192.168.1.218 port 9999	Specified interface did not receive a response to Probe for failover.	[Link Monitor] No response received on %s from %s	[Link Monitor] No response received on ${if_name} from ${target}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
49000002	WARN	Networking / Link Monitoring	Multi-Wan Probe Failed	[Link Monitor] No response received on External from TCP host 192.168.1.218 port 9999	Specified interface did not receive a response to Probe for failover.	[Link Monitor] No response received on %s from %s	[Link Monitor] No response received on ${if_name} from ${target}
49000003	ERROR	Networking / Link Monitoring	Probe failure	[Link Monitor] External interface failed because a probe to the target host failed	Specified interface marked as Failed due to no response from ping or TCP host.	[Link Monitor] %s interface failed because a probe to the target host failed	—
68000001	INFO	Networking / Discovery	Network scan completed	On demand scan completed	Specified type of scan completed	%s scan completed	${scan_type} scan completed
68000002	INFO	Networking / Discovery	Network scan started	On demand scan— stage 2 started	Specified type and stage of scan started	%s scan%s started	${scan_type} scan${scan_stage} started
68000002	INFO	Networking / Discovery	Network scan started	On demand scan— stage 2 started	Specified type and stage of scan started	%s scan%s started	${scan_type} scan${scan_stage} started
68000003	INFO	Networking / Discovery	On demand scan— stage 1 completed	On demand scan— stage 1 completed	On demand scan— stage 1 completed	On demand scan— stage 1 completed	On demand scan— stage 1 completed
0900000A	INFO	Networking / PPPoE	Disconnect	[eth0 (External)] PPPoE session [11] is disconnected.	The PPPoE session for the specified interface is disconnected.	[%s (%s)]PPPoE session[%d] is disconnected.	—
3100000A	INFO	Networking / Network Management	Interface shutting down	[eth1 (Trusted)] Interface shutting down	Shutting down the specified interface.	[%s (%s)] Interface shutting down	[${dev_name} (${if_name})] Interface shutting down
3100000A	INFO	Networking / Network Management	Interface shutting down	[eth1 (Trusted)] Interface shutting down	Shutting down the specified interface.	[%s (%s)] Interface shutting down	[${dev_name} (${if_name})] Interface shutting down

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3100000B	INFO	Networking / Network Management	Multi-WAN interface activated.	[eth1 (Trusted)] Interface is activated due to link-monitor success.	Interface is activated due to link-monitor success. The log message specifies the interface.	[%s (%s)] Interface is activated due to link-monitor success.	—
3100000D	WARN	Networking / Network Management	Multi-WAN interface deactivated	[eth1 (Trusted)] Interface is deactivated due to link-monitor failure.	Interface is deactivated due to link-monitor failure. The log message specifies the interface.	[%s (%s)] Interface is deactivated due to link-monitor failure.	—
3100002B	ERROR	Networking / Network Management	Interface is disabled	[eth1 (Trusted)] Interface is disabled because it does not exist	Specified interface does not exist, The interface status is set to disabled.	[%s (%s)] Interface is disabled because it does not exist	[${dev_name} (${if_name})] Interface is disabled because it does not exist
3100002B	ERROR	Networking / Network Management	Interface is disabled	[eth1 (Trusted)] Interface is disabled because it does not exist	Specified interface does not exist, The interface status is set to disabled.	[%s (%s)] Interface is disabled because it does not exist	[${dev_name} (${if_name})] Interface is disabled because it does not exist
3100002C	WARN	Networking / Network Management	Interface link status changed	[eth1 (Trusted)] Interface link status changed to UP	The interface link status has changed. The log message specifies the new status.	[%s (%s)] Interface link status changed to %s	—
3100003A	WARN	Networking / Network Management	Cluster is enabled	Cluster is enabled and is forming	Cluster is enabled and is forming.	Cluster is enabled and is forming	—
3100003B	WARN	Networking / Network Management	Cluster setting changed to disabled	Cluster setting changed from enabled to disabled	The cluster setting was changed from enabled to disabled.	Cluster setting changed from enabled to disabled	—
3100003E	INFO	Networking / Network Management	Cluster A/P role changed	[Cluster] Cluster A/P role successfully changed from master to idle.	The role of this device in the active/passive (A/P) cluster changed. The log message specifies the old and new roles.	[Cluster] Cluster A/P role successfully changed from %s to %s.	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3100003F	INFO	Networking / Network Management	Cluster A/A role changed	[Cluster] Cluster A/A role successfully changed from master to idle.	The Cluster active/active (A/A) role changed. The log message specifies the old and new roles.	[Cluster] Cluster A/A role successfully changed from %s to %s.	—
3100006A	WARN	Networking / Network Management	IPv6 interface deactivated.	[eth0 (External)] IPv6 interface is deactivated.	IPv6 interface was deactivated. The log message specifies the interface.	[%s (%s)] IPv6 interface is deactivated.	—
3100006C	INFO	Networking / Network Management	IPv6 interface shutting down	[eth0 (External)] IPv6 interface shutting down	Shutting down specified IPv6 interface.	[%s (%s)] IPv6 interface shutting down	[${dev_name} (${if_name})] IPv6 interface shutting down
3100006C	INFO	Networking / Network Management	IPv6 interface shutting down	[eth0 (External)] IPv6 interface shutting down	Shutting down specified IPv6 interface.	[%s (%s)] IPv6 interface shutting down	[${dev_name} (${if_name})] IPv6 interface shutting down
3100006D	INFO	Networking / Network Management	IPv6 interface initializing	[eth0 (External)] IPv6 interface initializing	Initializing specified IPv6 interface.	[%s (%s)] IPv6 interface initializing	[${dev_name} (${if_name})] IPv6 interface initializing
3100006D	INFO	Networking / Network Management	IPv6 interface initializing	[eth0 (External)] IPv6 interface initializing	Initializing specified IPv6 interface.	[%s (%s)] IPv6 interface initializing	[${dev_name} (${if_name})] IPv6 interface initializing

Proxy Policy Log Messages

Proxy policy log messages are generated for traffic managed by the proxy policies configured on your Firebox. This can include events related to traffic through the proxy, proxy actions, authentication, Subscription Services, and Security Services. For information about log messages from Security Services processes, see *Security Services Log Messages* on page 93.

Event

Proxy Policy log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
0F000001	INFO	Proxy / Connection Framework Manager	HTTPS content inspection list imported	HTTPS content inspection exception list imported	When a pre-defined HTTPS exception list is imported, this event log is generated to inform the user.	HTTPS content inspection exception list imported	—
0F010015	WARN	Proxy / Connection Framework Manager	APT threat notified	APT threat notified. Details='Policy Name: HTTPS-proxy-00 Reason: high APT threat detected Task_UUID: d09445005c3f4a9a9bb78c8cb34edc2a Source IP: 10.0.1.2 Source Port: 43130 Destination IP: 67.228.175.200 Destination Port: 443 Proxy Type: HTTP Proxy Host: analysis.lastline.com Path: /docs/lastline-demo-sample.exe'	When APT server analysis result returned and identified as certain level threat, this event log will be generated to inform that the APT notification has been sent with detailed information.	APT threat notified. Details='%s'	—
0F010016	INFO	Proxy / Connection Framework Manager	APT safe result from file submission. Details='%s'	Cannot get the rule from ruleset 'request/download'	—	APT safe result from file submission. Details='Policy Name: HTTP-OUT-00 Reason: clean Message: APT safe object Task_UUID: 7a1e1500e92a410fa44d907f96b9209e MD5: d2723ba60dc88ec1ea449be9eee601cc Source IP: 10.0.1.2 Source Port: 50293 Destination IP: 100.100.100.3 Destination Port: 80 Proxy Type: HTTP Proxy Host: 100.100.100.3 Path: /test.exe'	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
1C0200CD	ERROR	Proxy / FTP	Ruleset lookup failed	Ruleset 'envelope/greeting' lookup failed	FTP proxy -- Failed to check the specified ruleset	Cannot get the rule from ruleset '%s'	—
1B0400CE	ERROR	Proxy / SMTP	Ruleset lookup failed	Ruleset 'envelope/greeting' lookup failed	SMTP proxy -- Failed to check the specified ruleset	Ruleset '%s' lookup failed	—

Traffic

Proxy Policy log messages of the *Traffic* log type.

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1DFF0000	INFO	Proxy / DNS	DNS invalid number of questions	Invalid number of questions	The traffic was blocked because the message included an invalid number of questions.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56701 53 msg="ProxyDeny: DNS invalid number of questions" (DNS-proxy-00)	—
1DFF0001	INFO	Proxy / DNS	DNS oversized query name	Query name oversized	The DNS query was blocked because the DNS query name exceeded the allowed buffer size, which varies from 0 kilobytes to 64 kilobytes.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56702 53 msg="ProxyDeny: DNS oversized query name" (DNS-proxy-00)	—
1DFF0002	INFO	Proxy / DNS	DNS compressed query name	Query name compressed	The DNS query was blocked because the domain name was compressed.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56703 53 msg="ProxyDeny: DNS compressed query name" (DNS-proxy-00)	—
1DFF0003	INFO	Proxy / DNS	DNS Parse error	Parse error	The DNS request was blocked because the proxy failed to parse the domain name.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56704 53 msg="ProxyDeny: DNS parse error" (DNS-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1DFF0004	INFO	Proxy / DNS	DNS Not Internet CLASS	Not Internet CLASS	The DNS query was not Internet CLASS. The log message specifies the action taken and the CLASS.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 46828 53 msg="ProxyDeny: DNS Not Internet CLASS" proxy_act="DNS-Outgoing.1" query_class="ANY" (DNS-proxy-00)	—
1DFF0005	INFO	Proxy / DNS	DNS OpCode match	OPcode match	The OpCode matched a configured rule, or the default rule of no match. The log message specifies the action taken, the rule, and the OpCode.	Deny 1-Trusted 0-External udp 10.0.1.3 192.168.130.81 36755 53 msg="ProxyDeny: DNS OpCode match" proxy_act="DNS-Outgoing.1" rule_name="Query" query_opcode="QUERY" (DNS-proxy-00)	—
1DFF0006	INFO	Proxy / DNS	DNS query type match	Query type match	The query type matched a configured rule, or the default rule of no match. The log message specifies the action taken, the rule matched, and the query type.	Deny 2-Optional-1 0-External udp 10.0.2.2 192.168.130.245 53710 53 msg="ProxyDeny: DNS query type match" proxy_act="DNS-Outgoing.1" rule_name="PTR record" query_type="PTR" (DNS-proxy-00)	—
1DFF0007	INFO	Proxy / DNS	DNS undersized question	Question undersized	The DNS query was blocked because the query size was less than the minimum valid size of 17 bytes.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56704 53 msg="ProxyDeny: DNS undersized question" (DNS-proxy-00)	—
1DFF0008	INFO	Proxy / DNS	DNS oversized question	Question oversized	The DNS query was blocked because the query size exceeds the maximum allowed size of 271 bytes.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56705 53 msg="ProxyDeny: DNS oversized question" (DNS-proxy-00)	—
1DFF0009	INFO	Proxy / DNS	DNS timeout	Timeout	The DNS connection was idle longer than the configured timeout value in the DNS policy.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 54807 53 msg="ProxyDrop: DNS timeout" (DNS-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1DFF000A	INFO	Proxy / DNS	DNS undersized answer	Response answer undersized	The DNS response was blocked because the response size was less than the minimum value of 17 bytes.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56706 53 msg="ProxyDeny: DNS undersized answer" (DNS-proxy-00)	—
1DFF000C	INFO	Proxy / DNS	DNS invalid response	Response ID Invalid	The DNS response was blocked because the response ID did not match the current or previous request ID.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56706 53 msg="ProxyDeny: DNS invalid response" (DNS-proxy-00)	—
1DFF000E	INFO	Proxy / DNS	DNS question match	Query question match	The DNS query name matched a configured rule, or the default rule of no match. The log message specifies the rule matched, action taken, and query name.	Deny 1-Trusted 0-External udp 10.0.1.3 192.168.130.81 59806 53 msg="ProxyDeny: DNS question match" proxy_act="DNS-Outgoing.1" rule_name="GStatic" query_type="A" question="ssl.gstatic.com" (DNS-proxy-00)	—
1DFF000F	INFO	Proxy / DNS	DNS request	Request	The DNS request audit log specifies the query type and name.	Allow 2-Optional-1 0-External udp 10.0.2.2 192.168.130.245 61758 53 msg="DNS request" proxy_act="DNS-Outgoing.1" query_type="PTR" question="1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa" (DNS-proxy-00)	—
1DFF0010	INFO	Proxy / DNS	DNS IPS match	IPS match	Intrusion Prevention Service (IPS) detected an intrusion threat. The log message specifies the signature ID, threat severity, signature name, and signature category.	Deny 0-External 1-Trusted udp 10.0.1.5 192.168.53.143 1024 53 msg="ProxyDrop: DNS IPS match" proxy_act="DNS-Outgoing.1" signature_id="1056125" severity="4" signature_name="EXPLOIT Tftpd32 DNS Server Buffer Overflow" signature_cat="Buffer Over Flow" (DNS-proxy-00)	—
1DFF0012	INFO	Proxy / DNS	DNS App match	Application match	Application Control identified the application type from the DNS client query and server response. The log message specifies the application name and ID, the application category name and ID, and the behavior name and ID.	Allow 1-Trusted 0-External udp 10.0.1.3 192.168.130.81 36755 53 msg="ProxyAllow: DNS App match" proxy_act="DNS-Outgoing.1" app_cat_name="Network Management" app_cat_id="9" app_name="DNS" app_id="61" app_beh_name="access" app_beh_id="6" (DNS-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1CFF0019	ERROR	Proxy / FTP	FTP Bounce Attempt	FTP Bounce Attempt	FTP proxy -- User attempted FTP bounce	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.164 37989 21 msg="ProxyBlock: FTP Bounce Attempt" proxy_act="FTP-Client.Standard" bounce ip="10.0.1.101"	—
1CFF0000	INFO	Proxy / FTP	FTP user name too long	User name too long	The user name exceeds the maximum length specified in the FTP proxy. The default is 64 characters.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 60774 21 msg="ProxyDeny: FTP user name too long" proxy_act="FTP-Client.1" user="testusertestuser1" length="17" (FTP-proxy-00)	—
1CFF0001	INFO	Proxy / FTP	FTP user password too long	Password too long	The password specified for the user exceeds the maximum length configured in the FTP proxy. The default maximum length is 32 characters.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 60776 21 msg="ProxyDeny: FTP user password too long" proxy_act="FTP-Client.1" length="17" (FTP-proxy-00)	—
1CFF0002	INFO	Proxy / FTP	FTP file or directory name too long	File or directory name too long	The file or directory name exceeds the maximum length configured in the FTP proxy. The default maximum length is 1,024 bytes.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 60782 21 msg="ProxyDeny: FTP file or directory name too long" proxy_act="FTP-Client.1" length="5" (FTP-proxy-00)	—
1CFF0003	INFO	Proxy / FTP	FTP command line too long	Command line too long	The command exceeded the maximum length configured in the FTP proxy. The default maximum length is 1,030 characters.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 60784 21 msg="ProxyDeny: FTP command line too long" proxy_act="FTP-Client.1" length="12" (FTP-proxy-00)	—
1CFF0004	INFO	Proxy / FTP	FTP exceeded maximum permitted login attempts	Exceeded maximum allowed login attempts	The user exceeded the configured maximum number of allowed failed log in attepmts per connection. The default limit is 6.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49162 21 msg="ProxyDrop: FTP exceeded maximum permitted login attempts" (FTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1CFF0005	INFO	Proxy / FTP	FTP command match	Command match	The command matched a configured rule, or the default of no match. For the FTP-server proxy action, the default is to deny any command that does not appear on the list. For the FTP-client proxy action, there is no default restriction on commands. The log message specifies the proxy action, action taken, and the command.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49196 21 msg="ProxyDeny: FTP command match" proxy_act="FTP-Client.2" rule_name="LIST" command="ls" (FTP-proxy-00)	—
1CFF0006	INFO	Proxy / FTP	FTP download match	Download match	The file type matched a configured download rule, or the default rule of no match. The log message specifies the proxy action, action taken, and file type.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49208 21 msg="ProxyDeny: FTP download match" proxy_act="FTP-Client.2" rule_name="*.zip" file_name="hostname.zip" (FTP-proxy-00)	—
1CFF0007	INFO	Proxy / FTP	FTP upload match	Upload match	The file type matched a configured upload rule, or the default rule of no match. The log message specifies the proxy action, action taken, and file type.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49228 21 msg="ProxyDeny: FTP upload match" proxy_act="FTP-Client.2" rule_name="ISO" file_name="test.iso" (FTP-proxy-00)	—
1CFF0008	INFO	Proxy / FTP	FTP timeout	Timeout	The connection exceeded the configured idle time value. The default is 180 seconds.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49561 21 msg="ProxyDrop: FTP timeout" (FTP-proxy-00)	—
1CFF0009	INFO	Proxy / FTP	FTP invalid request	Invalid request	The FTP proxy rejected the command because of a lack of required arguments, such as a user name. The log message specifies the proxy action and command.	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49579 21 msg="ProxyDeny: FTP invalid request" proxy_act="FTP-Client.2" reason="No username value provided for USER command" (FTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1CFF000C	INFO	Proxy / FTP	FTP request	Request	This log message for the FTP request transaction includes the source and destination IP addresses for the initial connections.	Allow 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49590 21 msg="FTP request" proxy_act="FTP-Client.2" ctl_src="10.0.1.49:47553" ctl_dst="11.11.11.2:5120" file="test.exe" rcvd_bytes="1084" sent_bytes="0" user="testuser" type="download" (FTP-proxy-00)	—
1CFF000D	INFO	Proxy / FTP	FTP IPS match	IPS match	Intrusion Prevention Service (IPS) detected a threat. The action configured for an IPS Match will be applied to the traffic. The log message includes the signature ID, threat severity, signature name, and signature category.	Deny 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 1024 21 msg="ProxyDrop: FTP IPS match" proxy_act="FTP-Client.3" signature_id="1110297" severity="4" signature_name="EXPLOIT FlashGet FTP PWD Command Stack buffer overflow -1" signature_cat="Buffer Over Flow" (FTP-proxy-00)	—
1CFF000E	INFO	Proxy / FTP	FTP Virus found	GAV Virus found	Gateway AntiVirus (GAV) detected a virus or malware in the attachment. The log message specifies the detected virus name and the file name of the attachment.	Deny 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 56528 msg="ProxyDrop: FTP Virus found" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" virus="EICAR_Test" file="eicar.com" (FTP-proxy-00)	—
1CFF000F	INFO	Proxy / FTP	FTP AV scanning error	GAV scan error	Gateway AntiVirus (GAV) failed to scan due to the error specified in the log message.	Deny 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 44485 msg="ProxyDrop: FTP AV scanning error" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" error="avg scanner is not created" file="eicar.com" (FTP-proxy-00)	—
1CFF0010	INFO	Proxy / FTP	FTP App match	Application match	Application Control identified an application in the FTP client request or server response. The log message specifies the proxy action, application control action, action taken, application name and ID, application category and ID, and application behavior name and	Allow 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49843 21 msg="ProxyAllow: FTP App match" proxy_act="FTP-Client.3" app_cat_name="File Transfer" app_cat_id="3" app_name="FTP Applications" app_id="1" app_beh_name="authority" app_beh_id="1" (FTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
					ID.		
1CFF0011	INFO	Proxy / FTP	FTP DLP violation found	DLP violation found	Data Loss Prevention (DLP) detected a rule violation. The log message specifies the proxy action, the DLP sensor name, DLP rule name, the authenticated user, and the file name. The log message also specifies the source and destination IP addresses and port for the control channel of the FTP session.	Deny 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 37611 msg="ProxyDrop: FTP DLP violation found" proxy_act="FTP-Client.3" ctl_src="10.0.1.49:47553" ctl_dst="11.11.11.2:5120" dlp_sensor="test" dlp_rule="SocialsecuritynumberswithqualifyingtermsUSA" authenticated_user="testuser" file="test.docx" (FTP-proxy-00)	—
1CFF0012	INFO	Proxy / FTP	FTP cannot perform DLP scan	DLP cannot perform scan	Data Loss Prevention (DLP) failed to scan because of the error specified in the log message.	Allow 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 52217 msg="ProxyAllow: FTP cannot perform DLP scan" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" error="Error: DLP not initialized" file="ssn.docx" (FTP-proxy-00)	—
1CFF0013	INFO	Proxy / FTP	FTP DLP object unscannable	DLP cannot scan object	Data Loss Prevention (DLP) could not scan and analyze the attachment because it is encrypted. The log message specifies the DLP sensor name, error message, the authenticated user, and the file name.	Allow 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 43974 msg="ProxyAllow: FTP DLP object unscannable" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" dlp_sensor="test" error="unscannable object (File was encrypted)" authenticated_user="testuser" file="test.zip" (FTP-proxy-00)	—
1CFF0014	INFO	Proxy / FTP	FTP DLP object too large	DLP object too large	Data Loss Prevention (DLP) could not analyze the attachment because the file was larger than the configured limit. The limit varies by platform, from one to five MB. The log message specifies the DLP sensor name and error message.	Allow 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 43813 msg="ProxyAllow: FTP DLP object too large" proxy_act="FTP-Client.3" error="DLP scan limit (5242880) exceeded" (FTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1CFF0015	INFO	Proxy / FTP	FTP APT detected	APT threat detected	APT Blocker identified a threat. The log message specifies the threat level, threat name, threat class, malicious activities, and file name where the threat was located.	Deny 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 58661 msg="ProxyDrop: FTP APT detected" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" md5="03e7ef270a157090e2f68079603b10fc" task_uuid="d21914d5a2bc4b618fae72da3b1c137e" threat_level="low" file="apt.txt" (FTP-proxy-00)	—
1CFF0017	INFO	Proxy / FTP	FTP File submitted to APT analysis server	File submitted to APT analysis server	File submitted to APT analysis server for deep threat analysis. A separate log message will appear when the result is retrieved from the APT analysis server.	Allow 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 43490 msg="ProxyAllow: FTP File submitted to APT analysis server" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" md5="03e7ef270a157090e2f68079603b10fc" task_uuid="d21914d5a2bc4b618fae72da3b1c137e" file="apt.txt"	—
1CFF0018	INFO	Proxy / FTP	FTP File reported safe from APT hash check	File reported safe from APT hash check	APT hash check did not report a threat from the object	Allow 0-External 1-Trusted tcp 11.11.11.2 11.11.11.5 20 43490 msg="ProxyAllow: FTP File reported safe from APT hash check" proxy_act="FTP-Client.3" ctl_src="11.11.11.2:5120" ctl_dst="10.0.1.49:47553" md5="03e7ef270a157090e2f68079603b10fc" task_uuid="d21914d5a2bc4b618fae72da3b1c137e" file="apt.txt"	—
2AFF0000	INFO	Proxy / H.323	H323 timeout	Timeout	The connection was idle longer than the configured timeout value. The default value is 180 seconds.	Deny 1-Trusted 0-External tcp 10.0.1.5 192.168.53.143 1720 1720 msg="ProxyDrop: H323 timeout" (H323-ALG-00)	—
2AFF0001	INFO	Proxy / H.323	H323 request	Request	This log message specifies the IP addresses for the completed H323 call.	Allow 1-Trusted 0-External tcp 10.0.1.2 192.168.53.167 3233 1720 msg="H323 request" proxy_act="H.323-Client.1" call_from="10.0.1.2" call_to="192.168.53.167" rcvd_bytes="171444" sent_bytes="256488" (H323-ALG-00)	—
2AFF0002	INFO	Proxy / H.323	H323 codec	Codec	The media codec is denied because it matched a configured Denied Codec. The log message specifies the codec.	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.167 3230 1720 msg="ProxyDeny: H323 codec" proxy_act="H.323-Client.1" codec="(unknown)" (H323-ALG-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
2AFF0003	INFO	Proxy / H.323	H323 Access control	Access control	The header address is allowed or denied because it matches an Access Control rule configured in the H323 policy. The log message specifies the address.	Allow 1-Trusted 0-External tcp 10.0.1.2 192.168.53.167 3232 1720 msg="ProxyAllow: H323 Access control" proxy_act="H.323-Client.1" From-header="10.0.1.2" (H323-ALG-00)	—
2AFF0006	INFO	Proxy / H.323	H323 IPS match	IPS match	Intrusion Prevention Service (IPS) detected an intrusion threat. The log message specifies the signature ID, threat severity, signature name, signature category, destination host name, and URI path.	Deny 0-External 1-Trusted tcp 10.0.1.5 192.168.53.143 3234 3230 msg="ProxyDrop: H323 IPS match" proxy_act="H.323-Client.1" signature_id="1112506" severity="4" signature_name="EXPLOIT Digium Asterisk Invalid RTP Payload Type Number Memory Corruption" signature_cat="Access Control" (H323-ALG-00)	—
2AFF0007	INFO	Proxy / H.323	H323 App match	Application match	Application Control detected an application type from the transaction. The log message specifies the action taken, the application name and ID, application category name and ID, and the application behavior name and ID.	Deny 1-Trusted 0-External tcp 10.0.1.6 192.168.53.167 3234 3230 msg="ProxyDrop: H323 App match" proxy_act="H.323-Client.1" app_cat_name="Voice over IP" app_cat_id="6" app_name="H.323" app_id="2" app_beh_name="access" app_beh_id="6" (H323-ALG-00)	—
1AFF0001	INFO	Proxy / HTTP	HTTP server response timeout	Session timeout with server idle	The HTTP session has timed out because no traffic has been received from the server for the specified amount of time. (Default: 10 minutes)	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 192.168.53.82 60654 80 msg="ProxyDeny: HTTP server response timeout" (HTTP-proxy-00)	—
1AFF0002	INFO	Proxy / HTTP	HTTP client request timeout	Session timeout with client idle	The HTTP session has timed out because no traffic has been received from the client for the specified amount of time. (Default: 10 minutes)	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 23.3.105.139 60680 80 msg="ProxyDeny: HTTP client request timeout" (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF0003	INFO	Proxy / HTTP	HTTP close complete timeout	Session timeout with close complete command timeout	The Close HTTP Session command timed out because no response to the FIN packet was received within the response time limit (3 minutes).	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 182.168.53.82 60654 80 msg="ProxyDeny: HTTP close complete timeout" (HTTP-proxy-00)	—
1AFF0004	INFO	Proxy / HTTP	HTTP Start-Line oversize	Oversize Start-Line	The first line of the client request or server response is longer than the configured maximum line length. The default maximum length is 4,096 bytes.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 134.170.188.84 52662 80 msg="ProxyDeny: HTTP Start-Line oversize" (HTTP-proxy-00)	—
1AFF0005	INFO	Proxy / HTTP	HTTP Invalid Request-Line Format	Invalid Request-Line format	The request line from the client does not match the standard format of [Method][SP][Request-URI][SP][HTTP/Version]. The incorrect status-line is specified in the log message.	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.92 52668 80 msg="ProxyDeny: HTTP invalid Request-Line Format" proxy_act="HTTP-Client.5" line="\x03\x03\x0d\x0a" (HTTP-proxy-00)	—
1AFF0006	INFO	Proxy / HTTP	HTTP invalid Status-Line format	Invalid Status-Line format	The status line from the server does not match the standard format of [HTTP/Version][SP][Status Code][SP][Reason]. The incorrect status-line is specified in the log message.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 194.219.221.195 64610 80 msg="ProxyDeny: HTTP invalid Status-Line format" proxy_act="HTTP-Client.2" line="\x03\x00\x00Kh\x80\x00\x07\x02,\x97\x02\xcc\x18M\xe4\xbe\xff\xa8\x87_a\x07\xb1\xa3d\x9f\x82\xc2\xea\xa2\xe17\x9f\xc8@+\xde\x7f\x7f\x0a" (HTTP-proxy-00)	—
1AFF0007	INFO	Proxy / HTTP	HTTP header line oversize	Header line oversize	A single client request or server response line is longer than the configured maximum line length. The default maximum length is 4,096 bytes.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 74.125.25.105 64152 80 msg="ProxyDeny: HTTP header line oversize" proxy_act="HTTP-Client.4" line="X-Frame-Options: " (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF0008	INFO	Proxy / HTTP	HTTP header block oversize	Header block oversize	The client request or server response header block length is longer than the configured limit. If maximum total length is enabled, the default limit is 16,384 bytes.	Deny 1-Trusted 0-External tcp 10.0.1.2 77.237.248.69 50019 80 msg="ProxyDeny: HTTP header block oversize" proxy_act="HTTP-Client.1" line="Date: Fri, 30 May 2014 16:50:51 GMT\x0d\x0a" (HTTP-proxy-00)	—
1AFF0009	INFO	Proxy / HTTP	HTTP header block parse error	Header block parse error	The HTTP proxy cannot process the header line because the format is incorrect. The required format is [Name]:[Value].	Deny 1-Trusted 0-External tcp 10.0.1.2 54.230.68.99 58900 80 msg="ProxyDeny: header block parse error" (HTTP-proxy-00)	—
1AFF000A	INFO	Proxy / HTTP	HTTP request URL path missing	Request missing URL path	The HTTP proxy cannot complete the URL because the host or URI value is missing. The HTTP request is denied.	Deny 1-Trusted 0-External tcp 10.0.1.2 54.230.68.99 58900 80 msg="ProxyDeny: HTTP request URL path missing" proxy_act="HTTP-Client.1" line="Date: Fri, 30 May 2014 18:50:51 GMT\x0d\x0a"	—
1AFF000B	INFO	Proxy / HTTP	HTTP request URL match	Request URL match	The requested URL matched a configured URL path in the HTTP proxy. By default, all URL paths are allowed.	Allow 1-Trusted 0-External tcp 10.0.1.2 173.194.33.185 60351 80 msg="ProxyAllow: HTTP request URL match" proxy_act="HTTP-Client.1" rule_name="Default" dstname="pagead2.googlesyndication.com" arg="/pagead/osd.js" (HTTP-proxy-00)	—
1AFF000C	INFO	Proxy / HTTP	HTTP chunk size line oversize	Chunk size line oversize	The HTTP chunk size line does not terminate correctly with a carriage return and line-feed (CRLF). The invalid line is specified in the log message.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40656 80 msg="ProxyDeny: HTTP chunk size line oversize" proxy_act="HTTP-Client.2" line="\x03\x00\x00Kh\x80\x00\x07\x02,\x97\x02\xcc\x18M\xe4\xbe\xff\xa8\x87_a\x07\xb1\xa3d\x9f\x82\xc2\xea\xa2\xe17\x9f\xc8@+\xde\x7f\x7f\x0a" (HTTP-proxy-00)	—
1AFF000D	INFO	Proxy / HTTP	HTTP chunk size invalid	Chunk size line invalid	The HTTP chunk size line has an invalid hexadecimal value. The invalid line is specified in the log message.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40722 80 msg="ProxyDeny: HTTP chunk size invalid" proxy_act="HTTP-Client.2" line="k7\x0d\x0a" (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF000E	INFO	Proxy / HTTP	HTTP chunk CRLF tail missing	Chunk no CRLF tail	The HTTP chunk does not close with a carriage return and line feed (CRLF) because the chunk block is missing the closing characters. This is required for each chunk when chunked transfer-encoding is in use. The log message includes the invalid chunk tail line.	Deny 1-Trusted 0-External tcp 10.0.1.2 77.237.248.69 50019 80 msg="ProxyDeny: HTTP chunk CRLF tail missing" proxy_act="HTTP-Client.1" line="This string missing the Carriage Return in the terminating CF-LF pair\x0a" (HTTP-proxy-00)	—
1AFF000F	INFO	Proxy / HTTP	HTTP footer line oversize	Footer line oversize	One line of the HTTP footer, an additional header sent at the end of a message is larger than the configured line limit. The default line limit is 4,096 bytes.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40662 80 msg="ProxyDeny: HTTP footer line oversize" proxy_act="HTTP-Client.2" line="\x03\x00\x00Kh\x80\x00\x07\x02,\x97\x02\xcc\x18M\xe4\xbe\xff\xa8\x87_a\x07\xb1\xa3d\x9f\x82\xc2\xea\xa2\xe17\x9f\xc8@+\xde\x7f\x7f\x0a" (HTTP-proxy-00)	—
1AFF0010	INFO	Proxy / HTTP	HTTP footer block oversize	Footer block oversize	The HTTP footer includes additional header information that is larger than the configured block limit size. The default total message limit, if enabled, is 16,384 bytes. The log message includes information about the invalid line.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40688 80 msg="ProxyDeny: HTTP footer block oversize" proxy_act="HTTP-Client.2" line="\x03\x00\x00Kh\x80\x00\x07\x02,\x97\x02\xcc\x18M\xe4\xbe\xff\xa8\x87_a\x07\xb1\xa3d\x9f\x82\xc2\xea\xa2\xe17\x9f\xc8@+\xde\x7f\x7f\x0a" (HTTP-proxy-00)	—
1AFF0011	INFO	Proxy / HTTP	HTTP footer block parse error	Footer block parse error	The HTTP footer includes an additional header field with syntax that violates the header format restrictions.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40705 80 msg="ProxyDeny: HTTP footer block parse error" (HTTP-proxy-00)	—
1AFF0012	INFO	Proxy / HTTP	HTTP Body Content Type match	Body content type match	The HTTP content either matches a configured Body Content Type or no Body Content Type is defined (only the default rule is in use).	Allow 1-Trusted 0-External tcp 10.0.1.2 192.168.53.92 52089 80 msg="ProxyAllow: HTTP Body Content Type match" proxy_act="HTTP-Client.1" rule_name="Default" (HTTP-proxy-00)	—
1AFF0013	INFO	Proxy / HTTP	HTTP header	Header content	The HTTP header line does not	Allow 1-Trusted 0-External tcp 10.0.1.2 192.168.53.92 41048 80 msg="ProxyStrip: HTTP header malformed" proxy_act="393296"	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
			malformed	malformed	follow the correct syntax for a client request or server response header. The log message contains the header line with the syntax error.	header="WWW-Authenticate: \x0d\x0a"	
1AFF0016	INFO	Proxy / HTTP	HTTP header transfer encoding match	Header Transfer-Encoding match	The Transfer-Encoding in the HTTP header matches a configured rule, or the default rule of no match. The log message specifies the matching rule name and header value.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40719 80 msg="ProxyAllow: HTTP header Transfer-Encoding match" proxy_act="HTTP-Client.2" rule_name="chunked" encoding="chunked" (HTTP-proxy-00)	—
1AFF0018	INFO	Proxy / HTTP	HTTP header Content Type match	Header content type match	The HTTP header Content Type matches a configured rule, or the default rule of no match. The log message specifies the matching rule name and header value.	Allow 1-Trusted 0-External tcp 10.0.1.2 198.252.206.140 52047 80 msg="ProxyAllow: HTTP header Content Type match" proxy_act="HTTP-Client.1" rule_name="text/*" content_type="text/html" (HTTP-proxy-00)	—
1AFF0019	INFO	Proxy / HTTP	HTTP request version match	Request version match	The HTTP version specified in the HTTP request line matches a configured rule, or the default rule of no match. The log specifies the matched rule name and the request line.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40627 80 msg="ProxyDeny: HTTP request version match" proxy_act="HTTP-Client.2" rule_name="Default" line="GET /index.html HTTP/1.8\x0d\x0a" (HTTP-proxy-00)	—
1AFF001A	INFO	Proxy / HTTP	HTTP request method match	Request method match	The HTTP request method specified in the Request-Line matches a configured rule, or the default rule of no match. The log message specifies the matched rule name and the method.	Allow 1-Trusted 0-External tcp 10.0.1.2 50.16.229.215 52301 80 msg="ProxyAllow: HTTP request method match" proxy_act="HTTP-Client.1" rule_name="GET" method="GET" (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF001B	INFO	Proxy / HTTP	HTTP header match	Header match	The HTTP header line matches a configured rule, or the default rule of no match. The log message specifies the matched rule name and header line.	Allow 1-Trusted 0-External tcp 10.0.1.2 50.16.229.215 52301 80 msg="ProxyAllow: HTTP header match" proxy_act="HTTP-Client.1" rule_name="Default" header="Host: www.walkscore.com\x0d\x0a" (HTTP-proxy-00)	—
1AFF001C	INFO	Proxy / HTTP	HTTP header cookie domain match	Header cookie domain match	The cookie domain header matches a configured rule, or the default rule of no match. The log message includes the matched rule name and the cookie domain.	Deny 1-Trusted 0-External tcp 10.0.1.2 50.16.229.215 52466 80 msg="ProxyDeny: HTTP header cookie domain match" proxy_act="HTTP-Client.1" rule_name="DoubleClick.com" domain=".doubleclick.com" (HTTP-proxy-00)	—
1AFF001D	INFO	Proxy / HTTP	HTTP request host missing	Request host missing	The HTTP request header is missing the host value.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 192.168.53.82 60654 80 msg="ProxyDeny: HTTP request host missing" (HTTP-proxy-00)	—
1AFF001E	INFO	Proxy / HTTP	HTTP header auth scheme match	Header authentication scheme match	The authentication scheme in the HTTP header server response matches one of the configured rules, or the default rule of no match. The log message specifies the matched rule name and the authentication scheme.	Allow 1-Trusted 6-Ext-access tcp 10.0.1.2 192.168.53.92 4910 80 msg="ProxyAllow: HTTP Header auth scheme match" proxy_act="HTTP-Client.1" rule_name="Basic" scheme="Basic" (HTTP-proxy-00)	—
1AFF001F	INFO	Proxy / HTTP	HTTP request method unsupported	Request method not supported	The HTTP request method does not match a configured rule. The log message specifies the method in use.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 192.168.53.92 64152 80 msg="ProxyDeny: HTTP request method unsupported" proxy_act="HTTP-Client.1" method="OPTIONS" (HTTP-proxy-00)	—
1AFF0020	INFO	Proxy / HTTP	HTTP request port mismatch	Request port mismatch	Relative-URI is in use and the port specified in the HTTP request host header does not match the port used for the connection.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 192.168.53.92 64152 80 msg="ProxyDeny: HTTP request port mismatch" proxy_act="HTTP-Client.1" (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF0021	INFO	Proxy / HTTP	HTTP Request categories	Request categories	The HTTP request is sent to a web address that matched a selected WebBlocker category. The log message specifies the action taken by the proxy, the URL, and the category matched.	Allow 1-Trusted 0-External tcp 10.0.1.2 50.16.210.117 50790 80 msg="ProxyAllow: HTTP Request categories" proxy_act="HTTP-Client.2" cats="Reference Materials" op="GET" dstname="www.walkscore.com" arg="/" (HTTP-proxy-00)	—
1AFF0022	INFO	Proxy / HTTP	HTTP service unavailable	Service unavailable	WebBlocker categorization failed because the configured WebBlocker server is not available. The log message specifies the profile name and a more detailed error message.	Deny 2-Internal-traffic 4-External-traffic tcp 192.168.2.23 23.21.224.150 60921 80 msg="ProxyDeny: HTTP service unavailable" proxy_act="HTTP-Client.1" service="WebBlocker.1" details="Webblocker server is not available" (HTTP-proxy-00)	—
1AFF0023	INFO	Proxy / HTTP	HTTP request URL path oversize	Request URL path oversize	The URI in the HTTP Request-Line is longer than the configured limit. The default limit is 2,048 bytes. The log message specifies the oversize URI.	Deny 1-Trusted 6-Ext-access tcp 10.0.1.2 173.194.33.167 64279 80 msg="ProxyDeny: HTTP request URL path oversize" proxy_act="HTTP-Client.1" path="/crx/blobs/QwAAAHF3InbmK-wFIemaY3I3BCMqOfjjbz3ZPr0OdvcXp8cUu10k48t_h-qsRfYvKPciETPh6ZMAQTV8WL-Rx-lfADpBbs0T0xmHzDv3tYNK4R4eAMZSmuX1YAUWVQIL6kSI-xpS-vSmdvbuQg/extension_0_1_0_12919.crx" (HTTP-proxy-00)	—
1AFF0024	INFO	Proxy / HTTP	HTTP request	Request	A detailed summary of the last HTTP proxy transaction.	Allow 1-Trusted 6-Ext-access tcp 10.0.1.2 192.168.53.92 64425 80 msg="HTTP request" proxy_act="HTTP-Client.1" op="GET" dstname="192.168.53.92" arg="/" sent_bytes="339" rcvd_bytes="2" elapsed_time="5.037750 sec(s)" (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF0025	INFO	Proxy / HTTP	HTTP header IPS match	Header IPS rule match	Intrusion Prevention Service (IPS) detected an intrusion in the client request or server response header. The log message specifies the action taken, signature ID, threat severity, signature name, signature category, destination host name, and URI path.	Deny 1-Trusted 0-External tcp 10.0.1.2 107.20.162.187 55531 80 msg="ProxyDeny: HTTP header IPS match" proxy_act="HTTP-Client.1" signature_id="1055396" severity="5" signature_name="WEB Cross-site Scripting -9" signature_cat="Web Attack" host="intext.nav-links.com" path="/util/intexteval.pl?action=startup" (HTTP-proxy-00)	—
1AFF0026	INFO	Proxy / HTTP	HTTP body IPS match	Body IPS rule match	Intrusion Prevention Service (IPS) detected an intrusion in the client request or server response content body. The log message specifies the action taken, signature ID, threat severity, signature name, signature category, destination host name, and URI path.	Deny 4-Trusted-1 0-External tcp 192.168.53.92 188.40.238.252 45617 443 msg="ProxyDeny: HTTP body IPS match" proxy_act="HTTP-Client.4" signature_id="1051723" severity="5" signature_name="Virus Eicar test string" signature_cat="Virus/Worm" host="secure.eicar.org" path="/eicar.com.txt" src_user="testuser@test.net" (HTTPS-proxy-00)	—
1AFF0028	INFO	Proxy / HTTP	HTTP Virus found	GAV Virus found	Gateway AntiVirus (GAV) detected a virus or malware. The log message specifies the virus name, destination host name, and URI path.	Deny 2-Internal-traffic 4-External-traffic tcp 10.0.1.8 192.168.53.92 57525 80 msg="ProxyDrop: HTTP Virus found" proxy_act="HTTP-Client.1" virus="EICAR_Test" host="192.168.53.92" path="/viruses/eicar.com" (HTTP-proxy-00)	—
1AFF0029	INFO	Proxy / HTTP	HTTP AV scanning error	GAV scan error	Gateway AntiVirus (GAV) failed to scan because of an error. The log message specifies the error message, the destination host name, and URI path.	Allow 1-Trusted 0-External tcp 10.0.1.2 8.25.35.115 51859 80 msg="ProxyAllow: HTTP AV scanning error" proxy_act="HTTP-Client.3" error="avg scanner is not created" host="api.yontoo.com" path="/LoadJS.ashx" (HTTP-proxy-00)	—
1AFF002B	INFO	Proxy / HTTP	HTTP Trusted host	Trusted host	The destination host name matches a proxy exception configured in the HTTP proxy.	Allow 1-Trusted 0-External tcp 10.0.1.2 134.170.51.254 51941 80 msg="ProxyAllow: HTTP Trusted host" proxy_act="HTTP-Client.3" rule_name="*.windowsupdate.com" (HTTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF002C	INFO	Proxy / HTTP	HTTP bad reputation	Bad reputation	The HTTP proxy blocked access to the destination address because of a bad reputation score for the URL.	Deny 1-Trusted 0-External tcp 172.16.1.101 188.40.238.250 36834 80 msg="ProxyDeny: HTTP bad reputation" proxy_act="HTTP-ACT-OUT" reputation="100" host="www.eicar.org" path="/download/eicar_com.zip" (HTTP-OUT-00)	—
1AFF002D	INFO	Proxy / HTTP	HTTP good reputation	Good reputation	The HTTP proxy did not complete a Gateway AntiVirus (GAV) scan for traffic to the destination address because the URL received a good reputation score.	Allow 4-Trusted-1 0-External tcp 192.168.53.92 198.35.26.96 45365 80 msg="ProxyAllow: HTTP good reputation" proxy_act="HTTP-Client.4" reputation="1" host="en.wikipedia.org" path="/favicon.ico" src_user="user@test.net" (HTTP-00)	—
1AFF002E	INFO	Proxy / HTTP	HTTP App match	Application match	Application Control identified the application type from the HTTP client request or server response stream.	Allow 4-Trusted-1 0-External tcp 192.168.53.92 198.35.26.96 45365 80 msg="ProxyAllow: HTTP App match" proxy_act="HTTP-Client.4" app_cat_name="Web" app_cat_id="13" app_name="Mozilla Firefox" app_id="12" app_beh_name="access" app_beh_id="6" src_user="test@test.net" (HTTP-00)	—
1AFF002F	INFO	Proxy / HTTP	HTTP DLP violation found	DLP violation found	Data Loss Prevention (DLP) detected a violation of DLP rules. The log message only includes information about the first rule matched.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.3 59568 80 msg="ProxyAllow: HTTP DLP violation found" proxy_act="HTTP-Client.1" dlp_sensor="sample_dlp_test" dlp_rule="BankaccountdetailsnearpersonallyidentifiableinformationUSA" host="100.100.100.3" path="/cgi-bin/upload.cgi" (HTTP-OUT.1-00)	—
1AFF0030	INFO	Proxy / HTTP	HTTP cannot perform DLP Scan	DLP cannot perform scan	Data Loss Prevention (DLP) failed to scan the traffic because of the error specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 62398 80 msg="ProxyAllow: HTTP cannot perform DLP scan" proxy_act="HTTP-Client.1" dlp_sensor="sample_dlp_test" error="Cannot Perform DLP scanning" (HTTP-proxy-00)	—
1AFF0031	INFO	Proxy / HTTP	HTTP DLP object unscannable	DLP object unscannable	Data Loss Prevention (DLP) cannot extract data from an object because it is encrypted.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40608 80 msg="ProxyAllow: HTTP DLP object unscannable" proxy_act="HTTP-Client.2" dlp_sensor="PCI Audit Sensor.1" error="unscannable object (File was encrypted)" host="100.100.100.11" path="/password-protected.zip" (HTTP-proxy-00)	—
1AFF0032	INFO	Proxy / HTTP	HTTP DLP object too	HTTP object too large	Data Loss Prevention (DLP) cannot scan the object because it	Allow 2-optional 0-External tcp 192.168.53.92 172.16.10.14 8902 80 msg="ProxyAllow: HTTP DLP object too large" proxy_act="HTTP-Client.1" dlp_	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
			large		is larger than the configured limit. The default value varies by device type and ranges between 1 and 5 MB.	sensor="DLPSensor.1" error="DLP scan limit exceeded" (HTTP-proxy-00)	
1AFF0033	INFO	Proxy / HTTP	HTTP Range header	Range header	This is the configured action (allow or strip) for the HTTP proxy Range header. The default action is strip. The HTTP proxy Range header can allow partial file transfers that impact content scans because the full content is not presented.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.15 40535 80 msg="ProxyStrip: HTTP Range header" proxy_act="HTTP-Client.1" header="Accept-Ranges: bytes\x0d\x0a" (HTTP-proxy-00)	—
1AFF0034	INFO	Proxy / HTTP	HTTP APT detected	APT threat detected	APT Blocker detected a threat. The log message specifies the the threat level, threat name, threat class, malicious activities, destination host name, and URI path.	Deny 2-Internal-traffic 4-External-traffic tcp 192.168.2.20 192.168.3.30 48120 80 msg="ProxyDrop: HTTP APT detected" proxy_act="HTTP-Client.1" host="192.168.3.30" path="/apt_sample.exe" md5="2e77cadb722944a3979571b444ed5183"	—
1AFF0036	INFO	Proxy / HTTP	HTTP File submitted to APT analysis server	File submitted to APT analysis server	File submitted to APT analysis server for deep threat analysis. The analysis result will be notified when the analysis result is fetched from APT analysis server.	Allow 2-Internal-traffic 4-External-traffic tcp 192.168.2.20 192.168.3.30 34063 80 msg="ProxyAllow: HTTP File submitted to APT analysis server" proxy_act="HTTP-Client.1" host="192.168.3.30" path="/test/sample.exe" md5="dd0af53fec2267757cd90d633acd549a" task_uuid="35c8ac1aaeee4e5186d584318deb397b" (HTTP-proxy-00)	—
1AFF0037	INFO	Proxy / HTTP	HTTP connect tunnel port match	Connect tunnel port match	The HTTP CONNECT tunnel request port matches a configured rule, or the default rule of no match. The log message specifies the matched rule name and port.	Allow 1-Trusted Firebox tcp 10.0.1.3 100.100.100.16 53531 3128 msg="ProxyReplace: HTTP connect tunnel port match" proxy_act="Explicit-Web.Standard.1" rule_name="Redirect-HTTPS" port="443" (Explicit-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1AFF0038	INFO	Proxy / HTTP	HTTP webproxy redirect	Webproxy redirect	The HTTP Webproxy connection was redirected to a different proxy action because of the configuration setting in explicit proxy. The log message specifies the new proxy action used.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.16 53532 3128 msg="ProxyReplace: HTTP webproxy redirect" proxy_act="Explicit-Web.Standard.1" redirect_action="HTTPS-Client.Standard" (Explicit-proxy-00)	—
1AFF0039	INFO	Proxy / HTTP	HTTP File reported safe from APT hash check	File reported safe from APT hash check	APT hash check did not report a threat from the object	Allow 2-Internal-traffic 4-External-traffic tcp 192.168.2.20 192.168.3.30 34063 80 msg="ProxyAllow: HTTP File reported safe from APT hash check" proxy_act="HTTP-Client.1" host="192.168.3.30" path="/test/sample.exe" md5="dd0af53fec2267757cd90d633acd549a" task_uuid="35c8ac1aaeee4e5186d584318deb397b" (HTTP-proxy-00)	—
1AFF003A	INFO	Proxy / HTTP	HTTP Content redirect	Content redirect	The HTTP content action connection was redirected to a different proxy action because of the configuration. The log message specifies the new proxy action used as well as the current ssl status.	Allow 0-External 3-Optional-2 tcp 203.0.113.2 203.0.113.3 50560 80 msg="ProxyReplace: HTTP Content Action redirect" proxy_act="HTTP-Content.Standard.1" redirect_action="HTTP-Server.Standard.2" srv_ip="10.0.2.8" srv_port="80" ssl_offload="0" client_ssl="NONE" server_ssl="NONE" (HTTP-proxy-00)	—
1AFF003B	INFO	Proxy / HTTP	HTTP Request content match	Request Content match	The request contained content which matched a configured content rule in the HTTP proxy. The log message specifies the content which matched the rule as well as rule details.	Allow 0-External 1-Trusted tcp 203.0.113.2 203.0.113.2 50428 80 msg="ProxyReplace: HTTP Request content match" proxy_act="HTTP-Content.Standard.1" rule_name="forums" content_type="URN" dstname="203.0.113.2" arg="/forums/index.html" srv_ip="10.0.2.8" srv_port="80" ssl_offload="1" redirect_action="HTTP-Server.Standard.1" (HTTP-proxy-00)	—
2CFF0000	INFO	Proxy / HTTPS	HTTPS Request	Request	HTTPS transaction log includes server name, certificate details and action taken.	Allow 1-Trusted 0-External tcp 10.0.1.2 173.194.33.184 59277 443 msg="HTTPS Request" proxy_act="HTTPS-Client.Standard.3" sni="www.gstatic.com" cn="*.google.com" cert_issuer="CN=olympus.wgti.net,OU=QA,O=WGTI,L=Seattle,ST=WA,C=US" cert_subject="CN=*.google.com,O=Google Inc,L=Mountain View,ST=California,C=US" action="allow" (HTTPS-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
2CFF0001	INFO	Proxy / HTTPS	HTTPS Request categories	WebBlocker Request categories	WebBlocker identified the category for a web request. The log message specifies the category and host name.	Allow 1-Trusted 0-External tcp 10.0.1.2 74.125.25.104 44773 443 msg="ProxyAllow: HTTPS Request categories" proxy_act="HTTPS-Client.1" service="Def" cats="Search Engines and Portals" dstname="www.google.com" (HTTPS-proxy-00)	—
2CFF0002	INFO	Proxy / HTTPS	HTTPS service unavailable	WebBlocker service unavailable	WebBlocker failed because a WebBlocker Server was not available.	Allow 1-Trusted 0-External tcp 10.0.1.2 74.125.25.147 51566 443 msg="ProxyAllow: HTTPS service unavailable" proxy_act="HTTPS-Client.1" error="Webblocker server is not available" service="Def" cats="" dstname="www.google.com" (HTTPS-proxy-00)	—
2CFF0003	INFO	Proxy / HTTPS	HTTPS domain name match	Domain name match	This rule log includes the matched rule name or default rule of no match and the patterns its been matched against.	Allow 1-Trusted 0-External tcp 10.0.1.2 173.194.33.176 59545 443 msg="ProxyAllow: HTTPS domain name match" proxy_act="HTTPS-Client.Standard.3" rule_name="*.google.com" sni="www.google.com" cn="" ipaddress="173.194.33.176" (HTTPS-proxy-00)	—
2CFF0007	INFO	Proxy / HTTPS	HTTPS invalid protocol	Protocol invalid	The HTTPS proxy detected an invalid SSL version.	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.143 41551 443 msg="ProxyDrop: HTTPS invalid protocol" proxy_act="HTTPS-Client.1" version="0x9999" length="123" data="\x16\x03\x01\x00{\x01\x00\x00w\x99\x99" (HTTPS-proxy-00)	—
2CFF0008	INFO	Proxy / HTTPS	HTTPS timeout	Timeout	The HTTPS connection was idle longer than the timeout value configured in the HTTPS policy. The default is 180 seconds.	Deny 1-Trusted 0-External tcp 10.0.1.5 192.168.53.143 54707 443 msg="ProxyDrop: HTTPS timeout" (HTTPS-proxy-00)	—
2CFF0009	INFO	Proxy / HTTPS	HTTPS content inspection	Content inspection	The HTTPS traffic was directed to a different proxy action because of the Content Inspection settings in the HTTPS proxy. The log message specifies the new proxy action used for content inspection, as well as the TLS ciphers used for the server and client.	Allow 1-Trusted 0-External tcp 10.0.1.2 173.194.33.180 59276 443 msg="ProxyInspect: HTTPS content inspection" proxy_act="HTTPS-Client.Standard.3" inspect_action="HTTP-Client.Standard" server_ssl="ECDHE-RSA-AES256-SHA384" client_ssl="ECDHE-RSA-AES256-GCM-SHA384" (HTTPS-proxy-00)	—
22FF0000	INFO	Proxy /	IMAP	Request	This audit log message specifies	Allow 1-Trusted 0-External tcp 10.0.1.70 10.148.22.60 53589 143 msg="IMAP	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
		IMAP	Request		the email message transaction result.	Request" proxy_act="IMAP-Client.Standard.1" email_len="652" action="allow" reason="" mbx="INBOX" user="wg" auth_method="plain" (IMAP-proxy-00)	
22FF0001	INFO	Proxy / IMAP	IMAP Timeout	Timeout	The connection was idle for longer than the configured timeout limit. The default limit is 1 minute.	Deny 1-Trusted 0-External tcp 10.0.1.70 10.148.22.60 53589 143 msg="IMAP Timeout" proxy_act="IMAP-Client.Standard.1" timeout="120" (IMAP-proxy-00)	—
22FF0002	INFO	Proxy / IMAP	IMAP Malformed Command	Malformed Command	The IMAP client sent malformed/unsupported command	Deny 1-Trusted 0-External tcp 10.0.1.70 10.148.22.60 53589 143 msg="IMAP Malformed Command" proxy_act="IMAP-Client.Standard.1" command="CONDSTORE" mbx="INBOX" user="wg" auth_method="plain" (IMAP-proxy-00)	—
22FF0004	INFO	Proxy / IMAP	IMAP Malformed Response	Malformed Response	The IMAP server sent malformed/unsupported response	Deny 1-Trusted 0-External tcp 10.0.1.70 10.148.22.60 53589 143 msg="IMAP Malformed Response" proxy_act="IMAP-Client.Standard.1" response="* 3597 EXISTS" mbx="INBOX" user="wg" auth_method="plain" (IMAP-proxy-00)	—
22FF0005	INFO	Proxy / IMAP	IMAP Content Type	Content Type	A MIME-type matched a configured content type rule, or the default rule of no match. The log message specifies the rule, MIME-type, and user-related information.	Allow 1-Trusted 0-External tcp 10.0.1.73 10.148.22.60 54116 143 msg="ProxyAvScan: IMAP Content Type" proxy_act="IMAP-Client.Standard.1" rule_name="All text types" content_type="text/plain" mbx="inbox" user="wg" auth_method="plain" (IMAP-proxy-00)	—
22FF0006	INFO	Proxy / IMAP	IMAP Filename	Filename	The attachment matches a configured file name rule, or the default rule of no match. The log message specifies the rule, file name, and user-related information.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 56079 143 msg="ProxyStrip: IMAP Filename" proxy_act="IMAP-Client.Standard.1" rule_name="Word documents" filename="bug92408.doc" attachment="bug92408.zip.zip" mbx="inbox" user="wg" auth_method="plain" (IMAP-proxy-00)	—
22FF0008	INFO	Proxy / IMAP	IMAP Virus Found	Virus Found	Gateway AntiVirus detected a virus or malware in the file. The log message specifies the virus name, file name, and user-related information.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 50633 143 msg="ProxyAllow: IMAP Virus Found" proxy_act="IMAP-Client.Standard.1" virus="Eicar" mbx="INBOX" user="wg" (IMAP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
22FF0009	INFO	Proxy / IMAP	IMAP Cannot Perform Gateway AV Scan	Cannot Perform Gateway AV Scan	Gateway AntiVirus (GAV) failed to scan because of the error specified in the log message	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 50633 143 msg="ProxyLock: IMAP Cannot Perform Gateway AV Scan" proxy_act="IMAP-Client.Standard.1" error="unable to scan" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF000A	INFO	Proxy / IMAP	IMAP APT detected	APT detected	APT Blocker found the threat specified in the log message in an attached file.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyStrip: IMAP APT detected" proxy_act="IMAP-Client.Standard.1" filename="lastline-demo-sample.exe" md5="7abebcf53e97b586c92a9ce5b9985cd4" task_uuid="e8a3730d1f88491c8821712e85d94929" threat_level="high" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF000C	INFO	Proxy / IMAP	IMAP File Submitted to APT analysis server	File Submitted to APT analysis server	File submitted to APT analysis server for deep threat analysis. The analysis result will be notified when the analysis result is fetched from APT analysis server.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyStrip: IMAP File submitted to APT analysis server" proxy_act="IMAP-Client.Standard.1" filename="971d3aa1c683c69f425cc6ddf66833d3d172f0fd.apk" md5="7abebcf53e97b586c92a9ce5b9985cd4" task_uuid="e8a3730d1f88491c8821712e85d94929"APT detected" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF000D	INFO	Proxy / IMAP	IMAP File reported safe from APT hash check	File reported safe from APT hash check	APT hash check did not report a threat from the object.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyStrip: IMAP File reported safe from APT hash check" proxy_act="IMAP-Client.Standard.1" filename="971d3aa1c683c69f425cc6ddf66833d3d172f0fd.apk" md5="7abebcf53e97b586c92a9ce5b9985cd4" task_uuid="e8a3730d1f88491c8821712e85d94929"APT detected" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF000E	INFO	Proxy / IMAP	IMAP Classified as confirmed SPAM	spamBlocker confirmed spam	spamBlocker classified the message as confirmed SPAM. The log message specifies the user-related information	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyReplace: IMAP Classified as confirmed SPAM" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
22FF000F	INFO	Proxy / IMAP	IMAP Classified as bulk mail	spamBlocker bulk mail	spamBlocker classified the message as bulk mail. The log message specifies the user-related information	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyReplace: IMAP Classified as bulk mail" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF0010	INFO	Proxy / IMAP	IMAP Classified as suspect SPAM	spamBlocker suspect spam	spamBlocker classified the message as suspect SPAM. The log message specifies the user-related information	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyReplace: IMAP Classified as suspect SPAM" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF0011	INFO	Proxy / IMAP	IMAP Message could not be scored	spamBlocker not scored	spamBlocker cannot score the message. The log message specifies the user-related information	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyAllow: IMAP Message could not be scored" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF0012	INFO	Proxy / IMAP	IMAP spamBlocker exception was matched	spamBlocker exception matched	The sender for the email matched a spamBlocker exception rule. The log message specifies the rule and user-related information.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyAllow: IMAP spamBlocker exception was matched" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF0013	INFO	Proxy / IMAP	IMAP Classified as not SPAM	spamBlocker not spam	spamBlocker classified the message as not SPAM. The log message specifies the user-related information.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyAllow: IMAP Classified as not SPAM" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
22FF0014	INFO	Proxy / IMAP	IMAP Message classification is unknown because an error occurred while classifying	spamBlocker not spam	spamBlocker was unable to classify the message because of the error specified in the log message. The log message specifies the user-related information.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 60275 143 msg="ProxyAllow: IMAP Message classification is unknown because an error occurred while classifying" proxy_act="IMAP-Client.Standard.1" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF0015	INFO	Proxy / IMAP	IMAP Gateway AV object too large	GAV file too large	The attachment file size exceeds the Gateway AV scan size limit.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 50698 143 msg="ProxyAllow: IMAP Gateway AV object too large" proxy_act="IMAP-Client.OUT" attachment="large_file.doc" error="File exceeding the scan size limit" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF0016	INFO	Proxy / IMAP	Gateway AV object encrypted (password-protected)	GAV file encrypted	The attachment file is encrypted or password-protected.	Allow 1-Trusted 0-External tcp 10.0.1.3 100.100.100.3 50698 143 msg="ProxyAllow: IMAP Gateway AV object enrcypted (password-protected)" proxy_act="IMAP-Client.OUT" attachment="password-protected.zip" error="Object Encrypted" mbx="INBOX" user="wg" (IMAP-proxy-00)	—
22FF1017	INFO	Proxy / IMAP	IMAP invalid TLS protocol	Protocol invalid	The IMAP proxy detected invalid TLS protocol.	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.143 41551 993 msg="ProxyDrop: IMAP invalid TLS protocol" proxy_act="IMAP-Client.1" (IMAP-proxy-00)	—
22FF1018	INFO	Proxy / IMAP	IMAP TLS content inspection	Content Inspection	The IMAP proxy decrypted a secure connection for content inspection.	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.143 41551 993 msg="ProxyInspect: IMAP TLS content inspection" proxy_act="IMAP-Client.1" server_ssl="ECDHE-RSA-AES256-SHA384" client_ssl="ECDHE-RSA-AES256-GCM-SHA384" (IMAP-proxy-00)	—
21FF0000	INFO	Proxy / POP3	POP3 CAPA	CAPA	The CAPA response contained the unknown or blocked capability that is specified in the log message.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 43924 110 msg="ProxyDeny: POP3 CAPA" keyword="VERF": (POP3-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
21FF0001	INFO	Proxy / POP3	POP3 AUTH	Authentication	The authentication type matched a rule, or the default rule of no match. The log message specifies the rule name and authentication type.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44047 110 msg="ProxyDeny: POP3 AUTH" proxy_act="POP3-Client.2" rule_name="Default" authtype="KERBOSE_V12" (POP3-proxy-00)	—
21FF0002	INFO	Proxy / POP3	POP3 command	Command	The client sent an authentication command when it was not allowed.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44225 110 msg="ProxyDeny: POP3 command" proxy_act="POP3-Client.2" keyword="AUTH KERBEROS_V12\x0d\x0a" (POP3-proxy-00)	—
21FF0005	INFO	Proxy / POP3	POP3 header	Header	A POP3 header matched a configured Header rule, or the default rule of no match. The log message specifies the rule and header.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 43909 110 msg="ProxyStrip: POP3 header" proxy_act="POP3-Client.1" rule_name="Default" header="Delivered-To: wg@localhost" (POP3-proxy-00)	—
21FF0006	INFO	Proxy / POP3	POP3 content type	Content type	A MIME-type matched a configured content type rule, or the default rule of no match. The log message specifies the rule, MIME-type, and user name.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 43909 110 msg="ProxyAllow: POP3 content type" proxy_act="POP3-Client.1" rule_name="All text types" content_type="text/plain" user="wg" (POP3-proxy-00)	—
21FF0007	INFO	Proxy / POP3	POP3 filename	File name	The attachment matches a configured file name rule, or the default rule of no match. The log message specifies the rule, file name, and user name.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44035 110 msg="ProxyAvScan: POP3 filename" proxy_act="POP3-Client.1" rule_name="Text files" file_name="high-triggerme.txt" user="wg" (POP3-proxy-00)	—
21FF0009	INFO	Proxy / POP3	POP3 timeout	Timeout	The connection was idle for longer than the configured timeout limit. The default limit is 1 minute.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44042 110 msg="ProxyDeny: POP3 timeout" proxy_act="POP3-Client.1" timeout="180" (POP3-proxy-00)	—
21FF000A	INFO	Proxy / POP3	POP3 request	Request	This audit log message specifies the bytes sent, bytes received, and user.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 43909 110 msg="POP3 request" proxy_act="POP3-Client.1" rcvd_bytes="625052" sent_bytes="1433" user="wg" (POP3-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
21FF000C	INFO	Proxy / POP3	POP3 IPS match	IPS match	Intrusion Prevention Service (IPS) detected an intrusion threat. The log message specifies the action taken, the signature ID, threat severity, signature name, and signature category.	Deny 0-External 1-Trusted tcp 172.16.180.2 172.16.181.2 1024 25 msg="ProxyDrop: POP3 IPS match" proxy_act="POP3-Incoming.1" signature_id="1110401" severity="4" signature_name="EXPLOIT IBM Lotus Notes Lotus 1-2-3 Work Sheet File Viewer Buffer Overflow (CVE-2007-6593)" signature_cat="Buffer Over Flow" (POP3-proxy-00)	—
21FF000F	INFO	Proxy / POP3	POP3 Virus found	GAV Virus found	Gateway AntiVirus detected a virus or malware in the file. The log message specifies the virus name, user, and file name.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44042 110 msg="ProxyAllow: POP3 Virus found" proxy_act="POP3-Client.1" user="wg" filename="sample.apt" virus="Generic34.EFX" (POP3-proxy-00)	—
21FF0010	INFO	Proxy / POP3	POP3 cannot perform Gateway AV	GAV cannot perform scan	Gateway AntiVirus (GAV) failed to scan because of the error specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39589 25 msg="ProxyLock: POP3 Cannot perform Gateway AV scan" proxy_act="POP3-Client.1" user="wg" filename="message.scr" error="scan request failed" (POP3-proxy-00)	—
21FF0012	INFO	Proxy / POP3	POP3 line length too long	Line length too long	A line exceeds the configured limit. The default is 1,000 bytes. The log message specifies the line length.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39457 25 msg="ProxyDeny: POP3 line length too long" proxy_act="POP3-Client.1" line_length="22121" (POP3-proxy-00)	—
21FF0014	INFO	Proxy / POP3	POP3 message format	Message format	The message is not in an allowed format. The log message specifies the error and the user.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44061 110 msg="ProxyStrip: POP3 message format" proxy_act="POP3-Client.2" file_name="sm_conns.txt" type="uuencode" (POP3-proxy-00)	—
21FF0015	INFO	Proxy / POP3	POP3 encoding error	Encoding error	The proxy was unable to decode and encode the message because of the error specified in the log message.	Allow 0-External 1-Trusted tcp 100.100.106.253 100.100.106.55 51064 110 msg="ProxyStrip: POP3 encoding error" proxy_act="POP3-Server.1" message="invalid b64 characters in input" (POP3-IN-00)	—
21FF0016	INFO	Proxy / POP3	POP3 Classified as confirmed SPAM	spamBlocker confirmed spam	spamBlocker classified the message as confirmed SPAM. The log message specifies the sender and recipients.	Allow 1-Trusted 0-External tcp 10.0.55.253 100.100.100.155 45551 110 msg="ProxyReplace: POP3 Classified as confirmed SPAM" (POP3-OUT-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
21FF0017	INFO	Proxy / POP3	POP3 Classified as suspect SPAM	spamBlocker BULK spam	spamBlocker classified the message as bulk SPAM. The log message specifies the sender and recipients.	Allow 0-External 1-Trusted tcp 100.100.106.253 100.100.106.55 46177 110 msg="ProxyReplace: POP3 Classified as suspect SPAM" (POP3-IN-00)	—
21FF0018	INFO	Proxy / POP3	POP3 Classified as suspect SPAM	spamBlocker suspect spam	spamBlocker classified the message as suspect SPAM. The log message specifies the sender and recipients.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44249 110 msg="ProxyReplace: POP3 Classified as suspect SPAM" (POP3-proxy-00)	—
21FF001A	INFO	Proxy / POP3	POP3 spamBlocker exception was matched	spamBlocker exception matched	The sender for the email matched a spamBlocker exception rule. The log message specifies the sender, recipient, and subject.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 43913 110 msg="ProxyAllow: POP3 spamBlocker exception was matched" proxy_act="POP3-Client.1" from="tester@testnet.com" to="wg@localhost" subj_tag=" (none)" (POP3-proxy-00)	—
21FF001B	INFO	Proxy / POP3	POP3 Classified as not SPAM	spamBlocker not spam	spamBlocker classified the message as not SPAM. The log message specifies the sender and recipients.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 43924 110 msg="ProxyAllow: POP3 Classified as not SPAM" (POP3-proxy-00)	—
21FF001C	INFO	Proxy / POP3	POP3 message classification is unknown because an error occurred while classifying	spamBlocker classification unknown	spamBlocker was unable to classify the message because of the error specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.55.253 100.100.100.155 53776 110 msg="ProxyAllow: POP3 message classification is unknown because an error occurred while classifying" (POP3-OUT-00)	—
21FF001D	INFO	Proxy / POP3	POP3 extra pad characters in base64 input	Extra pad characters	The POP3 proxy encountered extra pad characters in the body of a base64-encoded message.	Allow 0-External 1-Trusted tcp 100.100.106.253 100.100.106.55 46177 110 msg="ProxyStrip: POP3 Extra pad characters in base64 input" proxy_act="POP3-Server.1" pad_error="1" (POP3-IN-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
21FF001E	INFO	Proxy / POP3	POP3 App match	Application match	Application Control identified the application from the email message. The log specifies the application name and ID, application category and ID, and the application behavior name and ID.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44042 110 msg="ProxyAllow: POP3 App match" proxy_act="POP3-Client.1" app_cat_name="Mail and Collaboration" app_cat_id="5" app_name="POP3" app_id="2" app_beh_name="communicate" app_beh_id="2" (POP3-proxy-00)	—
21FF001F	INFO	Proxy / POP3	POP3 APT detected	APT threat detected	APT Blocker found the threat specified in the log message in an attached file.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.3 47193 110 msg="ProxyDrop: POP3 APT detected" proxy_act="POP3-Client.Standard.1" user="wg" filename="971d3aa1c683c69f425cc6ddf66833d3d172f0fd.apk" md5="7abebcf53e97b586c92a9ce5b9985cd4" task_uuid="e8a3730d1f88491c8821712e85d94929" threat_level="high" (POP3-proxy-00)	—
21FF0021	INFO	Proxy / POP3	POP3 File submitted to APT analysis server	File submitted to APT analysis server	File submitted to APT analysis server for deep threat analysis. The analysis result will be notified when the analysis result is fetched from APT analysis server.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.3 47187 110 msg="ProxyAllow: POP3 File submitted to APT analysis server" proxy_act="POP3-Client.Standard.1" user="wg" filename="971d3aa1c683c69f425cc6ddf66833d3d172f0fd.apk" md5="7abebcf53e97b586c92a9ce5b9985cd4" task_uuid="e8a3730d1f88491c8821712e85d94929" (POP3-proxy-00)	—
21FF0022	INFO	Proxy / POP3	POP3 File reported safe from APT hash check	File reported safe from APT hash check	APT hash check did not report a threat from the object	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.3 47187 110 msg="ProxyAllow: POP3 File reported safe from APT hash check" proxy_act="POP3-Client.Standard.1" user="wg" filename="971d3aa1c683c69f425cc6ddf66833d3d172f0fd.apk" md5="7abebcf53e97b586c92a9ce5b9985cd4" task_uuid="e8a3730d1f88491c8821712e85d94929" (POP3-proxy-00)	—
28FF0000	INFO	Proxy / SIP	SIP timeout	Timeout	The connection was idle for longer than the configured timeout value. The default value is 180 seconds.	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 5060 5060 msg="ProxyDrop: SIP timeout" (SIP-ALG-00)	—
28FF0004	INFO	Proxy / SIP	SIP request	Request	The log message specifies the source and destination of the	Allow 1-Trusted 0-External udp 10.0.1.3 192.168.53.143 5060 5060 msg="SIP request" proxy_act="SIP-Client.1" call_from="10.0.1.3" call_	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
					allowed call.	to="192.168.53.143" (SIP-ALG-00)	
28FF0005	INFO	Proxy / SIP	SIP codec	Codec	The codec is allowed or denied based on the setting for Denied Codecs in the SIP policy.	Deny 1-Trusted 0-External udp 10.0.1.3 192.168.53.143 5060 5060 msg="ProxyDeny: SIP codec" proxy_act="SIP-Client.1" codec="speex" (SIP-ALG-00)	—
28FF0006	INFO	Proxy / SIP	SIP Access control	Access control	The header address is allowed or denied based on the Access Control settings. The log message specifies the action taken, header and message ID.	Allow 1-Trusted 0-External udp 10.0.1.3 192.168.53.143 5060 5060 msg="ProxyAllow: SIP Access control" proxy_act="SIP-Client.1" To-header="zoolvb1@192.168.53.143" (SIP-ALG-00)	—
28FF0008	INFO	Proxy / SIP	SIP IPS match	IPS match	Intrusion Prevention Service (IPS) detected an intrusion threat. The log message specifies the signature ID, threat severity, signature name, signature category, destination host name and URI path.	Deny 0-External 1-Trusted udp 10.0.1.5 192.168.53.143 5060 5060 msg="ProxyDrop: SIP IPS match" proxy_act="SIP-Client.1" signature_id="1057422" severity="4" signature_name="SIP Digium Asterisk SIP SDP Header Parsing Stack Buffer Overflow -1" signature_cat="Buffer Over Flow" (SIP-ALG-00)	—
28FF0009	INFO	Proxy / SIP	SIP App match	Application match	Application Control identified an application from the transaction. The log message specifies the action taken, the application name and ID, application category name and ID, and the application behavior name and ID.	Deny 1-Trusted 0-External udp 10.0.1.4 192.168.53.143 5060 5060 msg="ProxyDrop: SIP App match" proxy_act="SIP-Client.1" signature_id="12" app_name="SIP" beh_name="communicate" app_msg="Application matched. application name: SIP; behavior name:communicate" (SIP-ALG-00)	—
1BFF0000	INFO	Proxy / SMTP	SMTP greeting	Greeting	The host name in the SMTP proxy HELO or EHLO command matched one of the Greeting Rules, or the default rule of no match.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39366 25 msg="ProxyDeny: SMTP greeting" proxy_act="SMTP-Outgoing.1" rule_name="*.test.net" hostname="testbox.test.net" (SMTP-proxy-00)	—
1BFF0001	INFO	Proxy /	SMTP	ESMTP	The EHLO response from the	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39371 25	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
		SMTP	ESMTP option	option	SMTP server includes an ESMTP option that is disabled or unknown.	msg="ProxyStrip: SMTP ESMTP option" proxy_act="SMTP-Outgoing.1" keyword="VRFY" (SMTP-proxy-00)	
1BFF0002	INFO	Proxy / SMTP	SMTP AUTH	Authentication (AUTH)	The EHLO response from the SMTP server included an authentication type that matches a configured authentication rule. The log message specifies the proxy action, the rule name, the action taken, and the authentication type.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39374 25 msg="ProxyDeny: SMTP AUTH" proxy_act="SMTP-Outgoing.1" rule_name="PLAIN" authtype="PLAIN" (SMTP-proxy-00)	—
1BFF0003	INFO	Proxy / SMTP	SMTP header	Header	A MIME header matched a configured rule, or the default rule of no match.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39379 25 msg="ProxyStrip: SMTP header" proxy_act="SMTP-Outgoing.1" rule_name="Default" header="X-MimeOLE: Produced By Microsoft Exchange V6.0.6603.0" (SMTP-proxy-00)	—
1BFF0004	INFO	Proxy / SMTP	SMTP From address	From address	The sender address matched a rule specified in the Mail From rules.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39383 25 msg="ProxyDeny: SMTP From address" proxy_act="SMTP-Outgoing.1" rule_name="jsmith@*.com->ex-employee" address="dbonn@testnet.com" (SMTP-proxy-00)	—
1BFF0005	INFO	Proxy / SMTP	SMTP To address	To address	The recipient address matched a rule specified in the Rcpt To rules.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39384 25 msg="ProxyDeny: SMTP To address" proxy_act="SMTP-Outgoing.1" rule_name="Default" address="tester@testnet.com" (SMTP-proxy-00)	—
1BFF0006	INFO	Proxy / SMTP	SMTP content type	Content type	Some of the message content matched a content filter rule.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39391 25 msg="ProxyAvScan: SMTP content type" proxy_act="SMTP-Outgoing.1" rule_name="Default" content_type="application/x-gzip" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF0007	INFO	Proxy / SMTP	SMTP filename	Filename	An email attachment matched a file name rule, or the attachment is uuencoded and the SMTP proxy allows uuencoded attachments.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39436 25 msg="ProxyStrip: SMTP filename" proxy_act="SMTP-Outgoing.1" rule_name="*.exe" file_name="app.exe" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1BFF000A	INFO	Proxy / SMTP	SMTP timeout	Timeout	The SMTP connection was idle for longer than the configured idle timeout limit. The default is 10 minutes.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39402 25 msg="ProxyDeny: SMTP timeout" proxy_act="SMTP-Outgoing.1" timeout="60" (SMTP-proxy-00)	—
1BFF000C	INFO	Proxy / SMTP	SMTP Virus found	GAV Virus found	Gateway AntiVirus (GAV) detected a virus or malware in an email attachment.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39445 25 msg="ProxyStrip: SMTP Virus found" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" virus="I-Worm/Netsky.CORRUPTED" filename="message.scr" (SMTP-proxy-00)	—
1BFF000E	INFO	Proxy / SMTP	SMTP cannot perform Gateway AV scan	GAV cannot perform scan	Gateway AntiVirus (GAV) could not complete the scan because of the error that is specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39589 25 msg="ProxyLock: SMTP cannot perform Gateway AV scan" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" error="scan request failed" filename="message.scr" (SMTP-proxy-00)	—
1BFF000F	INFO	Proxy / SMTP	SMTP request	Request	This SMTP audit log specifies the bytes sent, bytes received, the sender and recipient addresses, and the sender and recipient TLS cipher.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39398 25 msg="SMTP request" proxy_act="SMTP-Outgoing.1" rcvd_bytes="272" sent_bytes="282" sender="tester@testnet.com" recipients="wg@localhost" server_ssl="ECDHE-RSA-AES256-GCM-SHA384" client_ssl="AES128-SHA256" tls_profile="TLS-Client.Standard"(SMTP-proxy-00)	—
1BFF0010	INFO	Proxy / SMTP	SMTP message format	Message format	The email message format matched a message format rule specified in the SMTP proxy. The log message includes the error message.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39452 25 msg="ProxyDeny: SMTP message format" proxy_act="SMTP-Outgoing.1" file_name="sm_conns.txt" type="uuencode" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF0011	INFO	Proxy / SMTP	SMTP IPS match	IPS match	Intrusion Prevention Service (IPS) detected a threat. The log message specifies the signature name and ID, threat severity, and signature category.	Deny 0-External 1-Trusted tcp 172.16.180.2 172.16.181.2 1024 25 msg="ProxyDrop: SMTP IPS match" proxy_act="SMTP-Incoming.1" signature_id="1110401" severity="4" signature_name="EXPLOIT IBM Lotus Notes Lotus 1-2-3 Work Sheet File Viewer Buffer Overflow (CVE-2007-6593)" signature_cat="Buffer Over Flow" (SMTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1BFF0013	INFO	Proxy / SMTP	SMTP too many recipients	Too many recipients	The number of email recipients specified in the email message exceeds the configured limit. The default limit is 99 for inbound messages and unlimited for outbound messages. The log message specifies the proxy action and number of recipients.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39404 25 msg="ProxyDeny: too many recipients" proxy_act="SMTP-Outgoing.1" rule_name="Default" content_type="" sender="tester@testnet.com" recipients="wg1@tenet.com;wg2@testnet.com" (SMTP-proxy-00)	—
1BFF0014	INFO	Proxy / SMTP	SMTP response size too long	Response size too long	The SMTP server response exceeds the configured limit. The default limit is 10,000 KB. The log message specifies the size of the response.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39973 25 msg="ProxyDeny: SMTP response size too long" proxy_act="SMTP-Outgoing.1" response_size="5030" (SMTP-proxy-00)	—
1BFF0015	INFO	Proxy / SMTP	SMTP line length too long	Line too long	The email message contains a line that exceeds the configured limit. The default is 1,000 bytes. The log message specifies the line length.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39457 25 msg="ProxyDeny: SMTP line length too long" proxy_act="SMTP-Outgoing.1" line_length="32110" (SMTP-proxy-00)	—
1BFF0016	INFO	Proxy / SMTP	SMTP message size too long	Message too long	The SMTP message length exceeds the configured limit. The default limit is 10,000 kb.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39466 25 msg="ProxyDeny: SMTP message size too long" proxy_act="SMTP-Outgoing.1" size="16384" (SMTP-proxy-00)	—
1BFF0017	INFO	Proxy / SMTP	SMTP header size too long	Header too long	The SMTP message contains a header that exceeds the configured Maximum Header Length. The default is 20,000 bytes.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39473 25 msg="ProxyDeny: SMTP header size too long" proxy_act="SMTP-Outgoing.1" headers_size="12157" (SMTP-proxy-00)	—
1BFF0018	INFO	Proxy / SMTP	SMTP command	Command	The SMTP request contains a command that is not supported or is not valid for the email transaction. The log message specifies the proxy action, action taken, SMTP command, and the	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39474 25 msg="ProxyDeny: SMTP command" proxy_act="SMTP-Outgoing.1" keyword="VERIFY\x0d\x0a" response="500" (SMTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
					response code.		
1BFF0019	INFO	Proxy / SMTP	SMTP Classified as confirmed SPAM	spamBlocker confirmed spam	spamBlocker has classified the message as confirmed SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39446 25 msg="ProxyDeny: SMTP Classified as confirmed SPAM" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF001A	INFO	Proxy / SMTP	SMTP Classified as bulk mail	spamBlocker bulk spam	spamBlocker has classified the message as bulk SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39499 25 msg="ProxyReplace: SMTP Classified as bulk mail" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF001B	INFO	Proxy / SMTP	SMTP Classified as suspect SPAM	spamBlocker suspect spam	spamBlocker has classified the message as suspect SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39999 25 msg="ProxyAllow: SMTP Classified as suspect SPAM" proxy_act="SMTP-Outgoing.1" sender="tester@wgrd.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF001C	INFO	Proxy / SMTP	SMTP Classified as not SPAM	spamBlocker not SPAM	spamBlocker has classified the message as not SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39487 25 msg="ProxyAllow: SMTP Classified as not SPAM" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1BFF001D	INFO	Proxy / SMTP	SMTP message classification is unknown because an error occurred while classifying	spamBlocker classification unknown	spamBlocker was unable to classify the email message because of an error. The log message specifies the sender and recipient addresses.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39524 25 msg="ProxyDeny: SMTP message classification is unknown because an error occurred while classifying" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF001E	INFO	Proxy / SMTP	SMTP spamBlocker exception was matched	spamBlocker exception matched	The sender or recipient of the email message matches a spamBlocker exception specified in the SMTP proxy.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39476 25 msg="ProxyAvScan: SMTP spamBlocker exception" proxy_act="SMTP-Outgoing.1" rule_name="Default" content_type="" sender="tester@watchguard.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF001F	INFO	Proxy / SMTP	SMTP An error was found by our decoder	Decoder error	The SMTP proxy was unable to decode the email message due to the error specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.55.253 100.100.100.155 36921 25 msg="ProxyStrip: SMTP An error was found by our decoder" proxy_act="SMTP-Outgoing.1" message="invalid b64 characters in input" (SMTP-OUT-00)	—
1BFF0021	INFO	Proxy / SMTP	SMTP extra pad characters in base64 input	Extra pad characters in base64 encoding	The SMTP proxy encountered extra pad characters when the body of the base64-encoded message was processed.	Allow 1-Trusted 0-External tcp 10.0.55.253 100.100.100.155 36664 25 msg="ProxyStrip: SMTP extra pad characters in base64 input" proxy_act="SMTP-Outgoing.1" pad_error="1" (SMTP-OUT-00)	—
1BFF0022	INFO	Proxy / SMTP	SMTP Mail From address too long	Mail from address too long	A sender email address exceeded the configured maximum address length. The address length is unlimited by default.	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39497 25 msg="ProxyDeny: SMTP Mail From address too long" proxy_act="SMTP-Outgoing.1" address="senderEmailAddressIsTooLongForTheForSettings@testnet.com" length="56" response="553" (SMTP-proxy-00)	—
1BFF0023	INFO	Proxy / SMTP	SMTP App match	Application match	Application Control identified the application in the mail message that is specified in the log	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39913 25 msg="ProxyDrop: SMTP App match" proxy_act="SMTP-Outgoing.1" app_cat_name="Mail and Collaboration" app_cat_id="5" app_name="SMTP" app_id="1"	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
					message.	app_beh_name="access" app_beh_id="6" (SMTP-proxy-00)	
1BFF0024	INFO	Proxy / SMTP	SMTP DLP violation Found	DLP violation found	Data Loss Prevention (DLP) detected the rule violation that is specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39510 25 msg="ProxyAllow: SMTP DLP violation Found" proxy_act="SMTP-Outgoing.1" dlp_sensor="PCI Audit Sensor.1" dlp_rule="SocialsecuritynumbersUSA" sender="tester@testnet.com" recipients="wg@localhost" filename="ssn.docx" (SMTP-proxy-00)	—
1BFF0025	INFO	Proxy / SMTP	SMTP cannot perform DLP Scan	DLP cannot perform scan	Data Loss Prevention (DLP) is unable to scan because of the error specified in the log message.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39589 25 msg="ProxyLock: SMTP cannot perform DLP scan" proxy_act="SMTP-Outgoing.1" sender="tester@testnet.com" recipients="wg@localhost" error="scan request failed" filename="message.scr" (SMTP-proxy-00)	—
1BFF0026	INFO	Proxy / SMTP	SMTP DLP object unscannable	DLP cannot scan object	Data Loss Prevention (DLP) is unable to extract data from an object because the object is encrypted.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39900 25 msg="ProxyAllow: SMTP DLP object unscannable" proxy_act="SMTP-Outgoing.1" dlp_sensor="PCI Audit Sensor.1" error="unscannable object (File was encrypted)" sender="tester@wgrd.com" recipients="wg@localhost" (SMTP-proxy-00)	—
1BFF0027	INFO	Proxy / SMTP	SMTP DLP object too large	DLP object too large	The file requested for Data Loss Prevention (DLP) analysis is larger than the configured limit. The default value varies by platform, from one to five MB. The log specifies the DLP sensor name and error message.	May 30 06:36:45 2014 gary_xtmv local1.info smtp-proxy[2861]: msg_id="1BFF-0027" Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.3 50976 25 msg="ProxyAllow: SMTP DLP oject too large" proxy_act="SMTP-Outgoing.1" sender="ghong@watchguard.com" recipients="wg@localhost" error="DLP scan limit (524288) exceeded" filename="2M-dlp-violates-end.txt" (SMTP-proxy-00)	—
1BFF0028	INFO	Proxy / SMTP	SMTP APT detected	APT threat detected	APT Blocker found the threat specified in the log message in an attached file.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39771 25 msg="ProxyAllow: SMTP APT detected" proxy_act="SMTP-Outgoing.1" sender="tester@wgrd.com" recipients="wg@localhost" filename="ecc59a46b439bdf63b058964e29ace0c" md5="ecc59a46b439bdf63b058964e29ace0c" task_uuid="b239bc669b534fcfa61bd78e156c9b19" threat_level="high" (SMTP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
1BFF002A	INFO	Proxy / SMTP	SMTP File submitted to APT analysis server	File submitted to APT analysis server	File submitted to APT analysis server for deep threat analysis. The analysis result will be notified when the analysis result is fetched from APT analysis server.	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39965 25 msg="ProxyAllow: SMTP File submitted to APT analysis server" proxy_act="SMTP-Outgoing.1" sender="tester@wgrd.com" recipients="wg@localhost" filename="regex2.dll" md5="547c43567ab8c08eb30f6c6bacb479a3" task_uuid="b8517202826a43fc93dba00f9e8c30ed" (SMTP-proxy-00)	—
1BFF002B	INFO	Proxy / SMTP	SMTP File reported safe from APT hash check	File reported safe from APT hash check	APT hash check did not report a threat from the object	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39965 25 msg="ProxyAllow: SMTP File reported safe from APT hash check" proxy_act="SMTP-Outgoing.1" sender="tester@wgrd.com" recipients="wg@localhost" filename="regex2.dll" md5="547c43567ab8c08eb30f6c6bacb479a3" task_uuid="b8517202826a43fc93dba00f9e8c30ed" (SMTP-proxy-00)	—
1BFF002C	INFO	Proxy / SMTP	SMTP invalid TLS protocol	Protocol invalid	The SMTP proxy detected invalid TLS protocol.	Deny 1-Trusted 0-External tcp 10.0.1.2 192.168.53.143 41551 465 msg="ProxyDrop: SMTP invalid TLS protocol" proxy_act="SMTP-Outgoing.1" (SMTP-proxy-00)	—
2DFF0000	INFO	Proxy / TCP-UDP	IP Request	Request	TCP-UDP transaction log for the traffic that is configured to allow or deny.	Allow ppp0 0-External tcp 10.0.1.46 206.191.171.104 49391 80 msg="IP Request" proxy_act="TCP-UDP-Proxy.Standard.1" sent_bytes="72271" rcvd_bytes="72271" src_user="testuser@Firebox-DB" (TCP-UDP-proxy-00)	—
2DFF0001	INFO	Proxy / TCP-UDP	IP IPS match	IPS match	Intrusion Prevention Service (IPS) detected an intrusion threat in TCP-UDP proxy traffic. The log message specifies the action taken, signature ID, threat severity, signature name, and signature category.	Deny 0-External 1-Trusted udp 10.0.1.5 192.168.53.143 1025 80 msg="ProxyDrop: TCP-UDP IPS match" proxy_act="TCP-UDP-Proxy.1" signature_id="1110070" severity="4" signature_name="DOS Apache mod_ssl HTTPS Request DOS -1" signature_cat="Dos/DDoS" (TCP-UDP-proxy-00)	—

ID	Level	Area	Name	Log Message Example	Log Message Example	Description	Message Variables
2DFF0004	INFO	Proxy / TCP-UDP	IP protocol	Protocol	The TCP-UDP proxy recognized the protocol. The log message specifies the action taken, and the rule name.	Allow 1-Trusted 0-External tcp 10.0.1.2 91.189.95.36 53246 80 msg="ProxyReplace: IP protocol" proxy_act="TCP-UDP-Proxy.1" rule_name="HTTP-Client.1" new_action="HTTP-Client.1" (TCP-UDP-proxy-00)	—
2DFF0005	INFO	Proxy / TCP-UDP	IP App match	Application match	Application Control identified the application type from the TCP-UDP proxy traffic. The log message specifies the action taken, the application name and ID, the application category name and ID, and the application behavior and ID.	Allow 1-Trusted 0-External udp 10.0.1.3 4.2.2.1 63690 53 msg="ProxyAllow: IP App match" proxy_act="TCP-UDP-Proxy.1" app_cat_name="Network Management" app_cat_id="9" app_name="DNS" app_id="61" app_beh_name="access" app_beh_id="6" (TCP-UDP-proxy-00)	—

Management Log Messages

Management log messages are generated for activity on your Firebox. This includes when changes are made to the device configuration and Device Management user accounts, for user authentication to the Firebox, and actions related to LiveSecurity and system settings.

Diagnostic

Management log messages of the *Debug (Diagnostic)* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
55010010	INFO	Management / System	USB drive format	—	USB drive format operation was %s	USB drive format operation was successful	USB drive format ${result}
55010014	INFO	Management / System	Generate system diagnostic file failed	—	Generate system diagnostic file to %s failed	Generate system diagnostic file to USB drive failed	Generate system diagnostic file to ${device} failed
55010015	INFO	Management / System	Periodic support snapshot is enabled	—	System periodic support snapshot is enabled	System periodic support snapshot is enabled	—
55010017	INFO	Management / System	Generate system diagnostic successfully	—	Exported system diagnostic file to %s successfully	Exported system diagnostic file to server successfully	Generate system diagnostic file to ${device} successfully
55010018	INFO	Management / System	Reset to the default configuration failed	The default configuration settings were not restored after a system reset.	Reset to the default configuration failed when the device was rebooted.	Reset to the default configuration failed when the device was rebooted.	
5501000C	INFO	Management / System	Device restore failed	Device auto restore from a specific image in a USB drive disc or normal restore from a normal image failed	Device %s restore from %s image failed due to %s	Device auto restore from USB drive image failed due to USB drive not found	Device ${restore_type} restore from ${image_source} image failed for ${reason}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
5501000D	INFO	Management / System	Creating USB auto restore image failed	—	Creation of USB auto restore image failed due to %s	Creation of USB auto restore image failed due to no USB drive	Creation of USB auto restore image failed: ${reason}
5501001B	INFO	Management / System	System backup failed	—	System backup %s failed due to %s.	System backup to USB drive failed due to write file to USB drive error	System backup ${dest device} failed: ${reason}
5501001C	INFO	Management / System	USB auto restore failed reason	—	USB auto restore failed due to %s	USB auto restore failed due to not detect the USB drive	USB auto restore failed for ${reason}

Event

Management log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	ID	Message Variables
3E000002	INFO	Management / Accounting	User login succeeded	Management user admin from 10.0.1.2 logged in	A user successfully logged in. The log message specifies the user type, user name, and IP address.	%s %s%s%s from %s logged in%s%s%s%s		${user_type} ${user_name}${auth_server} from {ipaddr} logged in ${virtual_ip} ${msg}
3E000004	INFO	Management / Accounting	User logout	Management user admin from 10.0.1.2 logged out	A user successfully logged out. The log message specifies the user type, user name, and IP address.	%s %s%s%s from %s logged out%s%s%s%s		${user_type} ${user_name}${auth_server} from {ipaddr} logged out ${virtual_ip} ${msg}
3E000003	WARN	Management / Accounting	User login failed	Management user admin from 10.0.1.2 log in attempt was rejected.	A user log in attempt failed. The log message specifies the user type, user name, IP address, and the failure reason, if available.	%s %s%s%s from %s log in attempt was rejected%s%s%s%s		${user_type} ${user_name}${auth_server} from {ipaddr} rejected ${virtual_ip} ${msg}
11000003	INFO	Management / Authentication	Authentication server unavailable	Authentication server 192.168.1.1:389 is not responding	The external authentication server is not available.	Authentication server %s:%d is not responding		—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
11000004	INFO	Management / Authentication	User authentication succeeded	Authentication of firewall user [user1@Firebox-DB] from 198.51.100.2 was accepted	The user successfully authenticated. The log message specifies whether this is an administrative user, a firewall user, or another type of user.	Authentication of %s user [%s@%s] from %s was accepted	Authentication of ${user_type} user [${user_name}@${auth_server}] from ${ipaddr} was accepted.
11000006	INFO	Management / Authentication	User unlock	User test is unlocked automatically	It indicates a user unlock and how he/she is unlocked	User %s is unlocked %s	User ${name} is unlocked ${how}
11000010	INFO	Management / Authentication	Firebox connected to SSO agent	Firebox connected to the SSO agent at 10.0.1.25 successfully.	Firebox connected to the SSO agent successfully	Firebox connected to the SSO agent at %s successfully.	—
11000011	INFO	Management / Authentication	Firebox closed the connection	Firebox closed the connection to the SSO agent at 10.0.1.25.	Firebox closed the connection to the SSO agent.	Firebox closed the connection to the SSO agent at %s.	—
11000012	INFO	Management / Authentication	Firebox failed to connect to the SSO agent	Firebox failed to connect to the SSO agent at 10.0.1.25. Reason: timeout.	Firebox failed to connect to the SSO agent.	Firebox failed to connect to the SSO agent at %s. Reason: %s.	—
11000013	INFO	Management / Authentication	Successful SSO agent failover	SSO Agent failover from 10.0.1.25 to 10.0.1.26 was successful.	Successful SSO agent failover.	SSO Agent failover from %s to %s was successful.	—
11000014	INFO	Management / Authentication	Unsuccessful SSO failover	SSO agent failover from 10.0.1.25 to 10.0.1.26 failed. Reason: incompatible SSO agent version.	Unsuccessful SSO failover.	SSO agent failover from %s to %s failed. Reason: %s.	—
11000005	WARN	Management / Authentication	User authentication failed	Authentication of Firewall user [test@RADIUS] from 10.0.1.2 was rejected, received an Access-Reject response from the RADIUS server	User authentication failed. The log message specifies the reason.	Authentication of %s user [%s@%s] from %s was rejected, %s	Authentication of ${user_type} user [${user_name}@${auth_server}] from ${ip_

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
							addr} was rejected, ${reason}
11000007	WARN	Management / Authentication	user lock	User test is locked out briefly after 3 login failures	It indicates a user lockout and how and why he/she is locked out	User %s is locked out %s after %d login failures	User ${name} is locked out ${lockout_type} after ${failure_count} login failures
11000008	WARN	Management / Authentication	BOVPN TLS client authentication failed	Authentication of BOVPN TLS client [EasternOffice] from 198.51.100.2 was rejected, pre-shared key is incorrect	BOVPN TLS client authentication failed. The log message specifies the reason.	Authentication of BOVPN TLS client [%s] from %s was rejected, %s	Authentication of BOVPN TLS client [${client_name}] from ${ip_addr} was rejected, ${reason}
1100000C	WARN	Management / Authentication	Authentication error	Authentication error. Domain not found for user1.	Authentication failed. The log message specifies the reason.	Authentication error. %s for %s.	Authentication error. ${error} for ${user_name}.
1100000D	WARN	Management / Authentication	Authentication server unavailable	Authentication of user [user1@example.com] failed. Both primary and secondary servers are unavailable.	Authentication failed because both the primary and secondary authentication servers are unavailable.	Authentication of user [%s@%s] failed. Both primary and secondary servers are unavailable.	—
1100000E	WARN	Management / Authentication	Unsupported RADIUS method	Authentication of firewall user [user1@RADIUS] failed. RADIUS authentication method MSCHAP_V1 is not supported.	Authentication failed because the specified RADIUS method is not supported.	Authentication of %s user [%s@%s] failed. RADIUS authentication method %s is not supported.	—
1100000F	WARN	Management / Authentication	Groups maximum reached	The maximum number of groups (31) has been reached	Authentication failed because the maximum number of groups has been reached.	The maximum number of groups (%d) has been reached	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
40010002	ERROR	Management / Certificate	CA certificate updated failed	CA certificate update failed. Current CA certificate version: 1.2.	CA certificate updated failed.	CA certificate update failed. Current CA certificate version: %s.	CA certificate update failed. Current CA certificate version: ${current CA version number}.
40010001	INFO	Management / Certificate	CA certificate updated successfully	CA certificate updated successfully to version 1.3.	The CA certificate updated successfully to the specified new version.	CA certificate updated successfully to version %s.	CA certificate updated successfully to version ${new CA version number}.
01010001	INFO	Management / Configuration	Device configuration change	Management user admin@Firebox-DB from 10.139.36.22 {modified	added	deleted } Blocked Sites Exceptions	The device configuration has been changed.	Management user %s@%s from %s %s %s %s	Management user ${user}@${domain} from ${ipaddr} ${operation} ${subsystem} ${object}
01010002	INFO	Management / Configuration	Administrative accounts reset to default	Administrative accounts were reset to the default settings	The administrative accounts were returned to the default settings. This could be because the system is in safe mode, or because of a corrupted administrative account file.	Administrative accounts were reset to the default settings	—
01020001	INFO	Management / Configuration	Feature key added	admin added feature key '883B25CCF32949EE'	An administrator added a feature key. The log message specifies the feature key ID.	%s added feature key '%s'	—
01020002	INFO	Management / Configuration	Feature key removed	admin removed feature key '883B25CCF32949EE'	An administrator has removed a feature key. The log message specifies the feature key ID.	%s removed feature key '%s'	—
01020005	INFO	Management / Configuration	Feature expiration reminder	'LIVESECURITY' feature will expire in 90 days.	A feature will soon expire. The log message specifies the feature and the number of days until it expires.	'%s' feature will expire in %d days.	—
01040001	INFO	Management /	Default device	Device default configuration was	The device configuration was reset to the	Device default	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		Configuration	settings in use for safe mode	loaded in safe mode	default settings because the device is in safe mode.	configuration was loaded in safe mode	
01020003	WARN	Management / Configuration	Feature expired	—	'%s' feature expired. Contact WatchGuard to renew your subscription.	'LIVESECURITY' feature expired. Contact WatchGuard to renew your subscription.	
5D000001	ERROR	Management / Device Feedback	Cloud upgrade failed	Failed to finish system upgrade requested by cloud	Firebox failed to upgrade firmware requested by WatchGuard cloud.	Failed to finish system upgrade requested by cloud	—
5D000002	INFO	Management / Device Feedback	Cloud upgrade success	System upgraded from 12.2.1 to 12.3 requested by cloud	Firebox successfully upgraded firmware requested by WatchGuard cloud.	System upgraded from %s to %s requested by cloud	—
41000002	ERROR	Management / LiveSecurity	RapidDeploy failed	RapidDeploy package was not applied: Cannot find result.xml	The RapidDeploy package was not applied to the device. The log message specifies the reason.	RapidDeploy package was not applied: %s	RapidDeploy failed: ${reason}
41000004	ERROR	Management / LiveSecurity	New RSS feed update failed	New RSS feed from LiveSecurity Service was not updated: error retrieving response from server	New RSS feed from the LiveSecurity Service failed to update.	New RSS feed from LiveSecurity Service was not updated: %s	—
41000006	ERROR	Management / LiveSecurity	Feature key download failed	Feature key from LiveSecurity Service was not received: error parsing response from LiveSecurity service	The feature key could not be downloaded from the LiveSecurity Service. The log message specifies the reason.	Feature key from LiveSecurity Service was not received: %s	—
41000008	ERROR	Management / LiveSecurity	Wireless country specification update failed	Wireless country specification from LiveSecurity Service was not received: received error code <n> from LSS	The wireless country specification could not be downloaded from the LiveSecurity service. The log message specifies the failure reason and the number of retries.	Wireless country specification from LiveSecurity Service was not received: %s, (retry_count=%d)	—
41010002	ERROR	Management / LiveSecurity	RapidDeploy configuration from USB failed	RapidDeploy configuration from a USB drive was not applied: config line missing	The RapidDeploy configuration was not successfully applied from a USB drive. The log message specifies the reason.	RapidDeploy configuration from a	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						USB drive was not applied: %s	
41000001	INFO	Management / LiveSecurity	RapidDeploy succeeded	RapidDeploy package was applied successfully	The RapidDeploy package from the LiveSecurity service was successfully applied to the device.	RapidDeploy package was applied successfully	—
41000003	INFO	Management / LiveSecurity	New RSS feed update succeeded	New RSS feed from LiveSecurity Service was updated	New RSS feed from the LiveSecurity Service was updated.	New RSS feed from LiveSecurity Service was updated	—
41000005	INFO	Management / LiveSecurity	Feature key download succeeded	Feature key from LiveSecurity Service was received	The feature key for the device was successfully downloaded from the LiveSecurity Service.	Feature key from LiveSecurity Service was received	—
41000007	INFO	Management / LiveSecurity	Wireless country specification update succeeded	Wireless country specification was updated	The wireless country specification was successfully updated from the LiveSecurity service.	Wireless country specification was updated	—
41010001	INFO	Management / LiveSecurity	RapidDeploy configuration from USB succeeded	RapidDeploy configuration from a USB drive was applied successfully	The RapidDeploy configuration was successfully applied from a USB drive.	RapidDeploy configuration from a USB drive was applied successfully	—
3D040001	INFO	Management / Logging	Primary Log Server connected	Connected to the primary Log Server at 198.51.100.0	The device successfully connected to the WatchGuard Log Server designated as the primary server.	Connected to the primary Log Server at %s	—
3D040002	INFO	Management / Logging	Backup Log Server connected	Connected to the backup Log Server at 198.51.100.0	The device successfully connected to the WatchGuard Log Server designated as the backup server.	Connected to the backup Log Server at %s	—
15000000	INFO	Management / Management Client	Device configuration update with audit trail	The configuration file and feature key for the device were successfully updated after a request from admin from	The updated configuration file was successfully sent to the device from the specified Management Server. The log	The configuration file %s for the device %s successfully updated	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				the Management Server at 10.139.44.88. Revision: dummy_ config_rev_id. Comments: update tcp segment.	message indicates if the feature key was updated. The log message might also specify the revision ID and includes comments about the update.	after a request from %s from the Management Server at %s.%s%s%s%s.	
15000001	INFO	Management / Management Client	Device configuration update	Device configuration file was successfully updated. Configuration file retrieved from the Management Server at 10.139.44.88.	The device retrieved an updated configuration file from the specified Management Server. The log message also indicates if device retrieved a feature key.	Device configuration file %s successfully updated. Configuration file retrieved from the Management Server at %s.	—
15010000	INFO	Management / Management Client	IPSec certificate import	The IPSec certificate was successfully imported from the Management Server at 10.139.44.88.	The IPsec certificate was successfully imported from the specified Management Server.	The IPSec certificate was successfully imported from the Management Server at %s.	—
15010001	INFO	Management / Management Client	Management Server CA certificate import	The Management Server CA certificate was successfully imported from the Management Server at 10.139.44.88.	The Management Server CA certificate was successfully imported from the specified Management Server.	The Management Server CA certificate was successfully imported from the Management Server at %s.	—
58000001	INFO	Management / NTP	System time changed	System time changed to 2012-08-29 08:20:00 by NTP	The system time was changed by the NTP process.	System time changed to %s by NTP	—
55010002	ERROR	Management / System	LIVESECURITY feature not found	Valid 'LIVESECURITY' feature not found	—	Valid 'LIVESECURITY' feature not found	—
55010003	ERROR	Management / System	LIVESECURITY expired	'LIVESECURITY' feature expired (Tue May 14 12:25:00 2013) prior to package release date (Wed May 15 01:00:00 2013)	—	'LIVESECURITY' feature expired (%s) prior to package release date (%s)	'LIVESECURITY' feature expired (${expiration time}) prior to package release date (${package release

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
							time})
55010000	INFO	Management / System	Bootup time	System boot up at 2000-01-01 00:00:01	—	System boot up at %s	System boot up at ${time}
55010004	INFO	Management / System	Shutdown	Shutdown requested by system	—	Shutdown requested by system	—
55010005	INFO	Management / System	Reboot	System is rebooting	—	System is rebooting	—
55010006	INFO	Management / System	Upgrade succeeded	System upgrade to 11.9 successful, system needs to reboot	—	System upgrade to %s successful, %s	System upgrade to ${software version} successful ${box need reboot or not}
55010007	INFO	Management / System	Automatic reboot	System is automatically rebooting at 12:09	—	System is automatically rebooting at %d:%d	System is automatically rebooting at ${hour}:${second}
55010008	INFO	Management / System	Time change	System time changed from 2012-10-5 12:30:15 to 2012-10-6 14:10:00	—	System time changed from %s to %s	System time changed from ${old value} to ${new value}
55010013	INFO	Management / System	USB auto restore started	USB auto restore started	—	USB auto restore started	—
55010016	INFO	Management / System	Feature expiration reminder	'LIVESECURITY' feature will expire on Sat., Jan 5, 11:27:23 CST 2013.	—	'LIVESECURITY' feature will expire on %s	'LIVESECURITY' feature will expire on ${expiration time}
55010020	INFO	Management / System	Backup succeeded	System backup succeeded	—	System backup succeeded	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
55010021	INFO	Management / System	Device restore success	Device auto restore from USB drive succeeded	Device auto restore from a specific image in USB drive or normal restore from a normal image	Device %s restore from %s image succeeded	Device ${restore_type} restore from ${image_source} image succeeded
55010022	INFO	Management / System	USB auto restore image created	USB auto restore image successfully created	—	USB auto restore image successfully created	—
5501000B	INFO	Management / System	Device restore	Device auto restore from USB drive image initiated, reboot needed	Device was restored from a saved backup image. The backup image was either auto restored from a USB drive or restored from another location.	Device %s restore from %s image initiated%s	Device ${restore_type} restore from ${image_source} image initiated${reboot_option}
5501001D	INFO	Management / System	Logo upload succeeded	Upload of logo succeeded	—	Upload of logo succeeded	—
55010019	WARN	Management / System	Configuration reset failed during a downgrade	During a system downgrade, the configuration reset failed	—	During a system downgrade, the configuration reset failed	—
5501001A	WARN	Management / System	Upgrade failed	System upgrade failed: 'LIVESECURITY' feature expired	—	System upgrade failed: %s	System upgrade failed: ${reason}
50000001	WARN	Management / Web Service	User login failed (wgagent)	WSM User status from 10.0.1.2 log in attempt was rejected - Invalid credentials.	A user log in attempt failed. The log message specifies the UI type, User Name, IP address, and (if available) the failure reason.	%s %s@%s from %s log in attempt was rejected - %s.	%{ui_type} ${user_name}@${auth_server} from ${ipaddr} log in attempt was rejected ${msg}.

FireCluster Log Messages

FireCluster log messages are for events related to your Fireboxes that are members of a FireCluster. This includes actions related to management of the FireCluster, operational errors of cluster members, events that occur on cluster members, and changes to the status of a cluster member.

Diagnostic

FireCluster log messages of the *Debug (Diagnostic)* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3A00000C	ERROR	Cluster / Event Monitoring	VRRP initialization failed	Initialization of Virtual Router Redundancy Protocol (VRRP) failed.	Cluster VRRP initialization failed	Cluster VRRP initialization failed	—
3A000002	INFO	Cluster / Event Monitoring	VRRP enabled	Virtual Router Redundancy Protocol (VRRP) is now enabled for this Active/Passive Cluster.	VRRP is now enabled for Cluster.	VRRP is now enabled for Cluster.	—
3A000004	INFO	Cluster / Event Monitoring	VRRP start master	VRRP started in master state.	Virtual Router with cluster ID %d started in master state.	Virtual Router with cluster ID 1 started in master state.	
3A000005	INFO	Cluster / Event Monitoring	VR shutdown	Virtual Router returned to initial state.	Virtual Router with cluster ID %d returned to initial state.	Virtual Router with cluster ID 1 returned to initial state.	Virtual Router with cluster ID ${id} returned to initial state
3A000006	INFO	Cluster / Event Monitoring	VR pause	Virtual Router becomes backup due to a pause event.	Virtual Router with cluster ID %d becomes backup on pause event	Virtual Router with cluster ID 1 becomes backup on pause event	Virtual Router with cluster ID ${id} becomes backup on pause event
3A000007	INFO	Cluster / Event Monitoring	VR resume	Virtual Router becomes master due to a resume event.	Virtual Router with cluster ID %d becomes master on resume event	Virtual Router with cluster ID 1 becomes master on resume event	Virtual Router with cluster ID ${id} becomes master on resume event

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3A000008	INFO	Cluster / Event Monitoring	VR backup state	Virtual Router state changed from master to backup	Virtual Router with cluster ID %d state changed from master to backup	Virtual Router with cluster ID 1 state changed from master to backup	Virtual Router with cluster ID ${id} state changed from master to backup
3A00000A	INFO	Cluster / Event Monitoring	VR notification gap	Member Virtual Router changed state to master due to notification gap from current master	Member %s Virtual Router with cluster ID %d changed state to master due to %d second notification gap from current master with IP %s	Member 80B20002E5BCD Virtual Router with cluster ID 1 changed state to master due to 3 second notification gap from current master with IP 10.0.4.1	Member ${member} Virtual Router with cluster ID ${id} changed state to master due to ${value} second notification gap from current master with IP ${ip}
3A00000B	INFO	Cluster / Event Monitoring	VRRP master state	Virtual Router state changed to master	Virtual Router with cluster ID %d state changed to master	Virtual Router with cluster ID 1 state changed to master	Virtual Router with cluster ID ${id} state changed to master
38000002	ERROR	Cluster / Management	DHCP overwrite	A DHCP server has attempted to assign an IP address to cluster member on the Cluster Interface. This log message recommends the admin isolate the Cluster interface network from the DHCP server, and specifies the interface number and IP address the cluster attempted to assign to the member.	A DHCP server is interfering with static address assignment of cluster IP address %s on eth%d. Disable DHCP server access to eth%d.	A DHCP server is interfering with static address assignment of cluster IP address 10.0.0.1 on eth0. Disable DHCP server access to eth5.	A DHCP server is interfering with static address assignment of cluster IP ${ip} on eth${port}. Please disable DHCP server access to eth${port}.
38000003	INFO	Cluster / Management	Cluster interface up	Cluster interface link status changed to up.	Cluster interface %s is up.	Cluster interface eth5 is up.	Cluster interface ${ifname} is up.
3800025C	INFO	Cluster / Management	Configuration update	Cluster member received an updated configuration from the master. The log message specifies the member serial number and configuration version number.	Cluster member %s received updated configuration; version %d.	Cluster member 80B20002E5BCD received updated configuration; version 3.	Cluster member ${member} received updated configuration; version ${version}.
38000004	WARN	Cluster / Management	Cluster interface down	Cluster interface link status changed to down.	Cluster interface %s is down.	Cluster interface eth5 is down.	Cluster interface ${ifname} is down

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
38000264	WARN	Cluster / Management	Time synchronization failure	The cluster master's attempt to synchronize time to a cluster member failed	Cluster time synchronization failed.	Cluster time synchronization failed.	—
3B000001	INFO	Cluster / Transport	Channel status change	The cluster communication channel between the specified members changed state.	Cluster channel from member %s to master is %s.	Cluster channel from member 80B20002E5BCD to master is up	Cluster channel from member ${member} to master is ${state}.

Event

FireCluster log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3A00000E	INFO	Cluster / Event Monitoring	VR enabled	The Virtual Router representing the cluster is now enabled	Virtual Router with cluster ID %d is now enabled	Virtual Router with cluster ID 1 is now enabled	Virtual Router with cluster ID ${id} is now enabled
3A00000F	INFO	Cluster / Event Monitoring	VR disabled	The Virtual Router representing the cluster is now disabled	Virtual Router with cluster ID %d is now disabled	Virtual Router with cluster ID 1 is now disabled	Virtual Router with cluster ID ${id} is now disabled
38000280	ERROR	Cluster / Management	Device discovery failed	The cluster master was unable to issue a device discovery message.	Cluster master %s was unable to issue a device discovery message.	Cluster master 80B20002E5BCD was unable to issue a device discovery message.	Cluster master ${master} was unable to issue a device discovery message.
3800027E	ERROR	Cluster / Management	Factory-default reset failed	Failed to reset to factory-default settings.	Failed to reset cluster member %s to factory-default settings.	Failed to reset cluster member 80B20002E5BCD to factory-default settings.	Failed to reset member ${member} to factory-default settings.
38000282	INFO	Cluster / Management	Member ready to join	Local member has FireCluster enabled and is ready to join.	Member %s is ready to join the cluster.	Member 80B20002E5BCD is ready to join the cluster.	Member ${member} is ready to join the cluster.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3800025A	INFO	Cluster / Management	Cluster enabled	Cluster was enabled on the specified member.	Cluster enabled on member %s.	Cluster enabled on member 80B20002E5BCD.	Cluster enabled on member ${member}.
3800025B	INFO	Cluster / Management	Cluster disabled on master	Cluster disabled on the cluster member while it was the cluster master.	Cluster disabled on cluster master %s.	Cluster disabled on cluster master 80B20002E5BCD.	Cluster disabled on cluster master ${master}.
38000278	WARN	Cluster / Management	Cluster disabled	The non-master member of the cluster will be reset to factory default-settings because FireCluster is disabled.	Cluster disabled. Non-master member %s will be reset to factory-default settings.	Cluster disabled. Non-master member 80B20002E5BCD will be reset to factory-default settings.	Cluster disabled. Non-master member %s will be reset to factory-default settings.
38000279	WARN	Cluster / Management	Critical configuration change	The non-master member of the cluster will be reset to factory-default settings due to a critical configuration change. A configuration change is critical if it would cause the master and backup master to lose the TCP connection on the cluster interface.	Non-master member %s will be reset to factory-default settings due to a critical cluster configuration change.	Non-master member 80B20002E5BCD will be reset to factory-default settings due to a critical cluster configuration change.	Non-master member ${member} will be reset to factory default-settings due to a critical cluster configuration change.
3800027A	WARN	Cluster / Management	Non-master member removed	The non-master member of the Cluster will be reset to factory-default settings because it was removed from the cluster.	Non-master cluster member %s was removed from cluster, and will be reset to factory-default settings.	Non-master cluster member 80B20002E5BCD was removed from cluster, and will be reset to factory-default settings.	Non-master cluster member %s was removed from cluster, and will be reset to factory-default settings.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
39000007	ERROR	Cluster / Operations	Failover due to WAI	The master failed over to the specified member because that member has a higher health score than the master.	Master %s failed over to member %s, which has a greater Weighted Average Index.	Master 80B20002E5BCD failed over to member 80B20002E5BFE, which has a greater Weighted Average Index.	Master ${master} failover to member ${member} with greater Weighted Average Index.
39000019	ERROR	Cluster / Operations	Failover due to interface state change	A cluster failover event occurred due to a change of interface state.	Cluster failover due to interface %s link %s event.	Cluster failover due to interface eth4 link down event.	Cluster failover due to interface ${ifname} link ${state} event.
3900000C	ERROR	Cluster / Operations	Synchronization failed	Full state synchronization from the master to the specified member failed. Member state will not change to Backup Master.	Full state synchronization from master %s to backup master %s failed.	Full state synchronization from master 80B20002E5BCD to backup master 80B20002E5BFE failed.	Full state synchronization from master ${master} to backup master ${member} failed.
3900000D	ERROR	Cluster / Operations	Synchronization timeout	Full state synchronization from the master to the specified member timed out. Member state will not change to Backup Master.	Full state synchronization from master %s to backup master %s timed out.	Full state synchronization from master 80B20002E5BCD to backup master 80B20002E5BFE timed out.	Full state synchronization from master ${master} to backup master ${member} timed out.
3900000F	ERROR	Cluster / Operations	Failover due to link-down	Cluster failover due to a link failure on the current master, which now has a health index lower than the backup master. The log message specifies which interface has the link down.	Master %s failed-over to member %s due to a link-down event on interface %s.	Master 80B20002E5BCD failed-over to member 80B20002E5BFE due to a link-down event on interface eth3.	Master ${master} failed-over to member ${member} due to a link-down event on interface ${ifname}.
39000005	INFO	Cluster / Operations	Member promoted to master	The specified member has become master.	Member %s is now master.	Member 80B20002E5BCD is now master.	Member ${member} is now master.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
39000010	INFO	Cluster / Operations	Member role change	The cluster member changed to the specified role.	Member %s changed role to %s.	Member 80B20002E5BCD changed role to master	Member ${member} role changed to ${role}.
39000011	INFO	Cluster / Operations	Interface link status change	Specified monitored interface link status changed, which will change the health index for the member.	Monitored interface %s link is %s.	Monitored interface eth0 link is down.	Monitored interface ${ifname} link is ${state}.
39000012	INFO	Cluster / Operations	New master	The specified member has taken over as master..	Member %s took over as master from member %s.	Member 80B20002E5BCD took over as master from member 80B20002E5BFE.	Member ${member} took over as master from member ${member}.
39000015	INFO	Cluster / Operations	Failover initiated by administrator	The administrator has initiated a failover.	Master %s initiated failover by administrator request.	Master 80B20002E5BCD initiated failover by administrator request.	Master ${master} initiated failover by administrator request..
39000058	INFO	Cluster / Operations	Member Role Change	The role of the specified Cluster member changed.	Cluster member %s changed role from %s to %s.	Cluster member 80B20002E5BCD changed role from idle to backup master	Cluster member ${member} changed role from ${role} to ${role}.
3900000E	INFO	Cluster / Operations	Synchronization successful	Full state synchronization to the specified member was successful. Member status changed to backup master.	Full state synchronization from master %s to backup master %s completed successfully.	Full state synchronization from master 80B20002E5BCD to backup master 80B20002E5BFE completed successfully.	Full state synchronization from master ${master} to backup master ${member} completed successfully

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
39000003	WARN	Cluster / Operations	Heartbeat lost	The specified Cluster failed to receive a heartbeat message.	Master %s detected loss of heartbeat from member %s, cluster channel is up.	Master 80B20002E5BFE detected loss of heartbeat from member 80B20002E5BCD, cluster channel is up.	Master ${master} detected loss of heartbeat from member ${member}, cluster channel is up.
39000016	WARN	Cluster / Operations	Cannot initiate failover	The failover requested by administrator cannot proceed because the master has a higher health index, or the backup master is unreachable.	Cannot initiate failover from master %s to member %s due to higher Weighted Average Index on current master or backup master is unreachable.	Cannot initiate failover from master 80B20002E5BCD to member 80B20002E5BFE due to higher Weighted Average Index on current master or backup master is unreachable.	Cannot initiate failover from master ${master} to member ${member} due to higher Weighted Average Index on current master or other member is unreachable.

Security Services Log Messages

Security Services log messages are generated for processes related to the Security Services configured on your Firebox. For the log messages from Security Services traffic and events, review the proxy log messages for the proxy policies where the Security Services are enabled. For more information, see *Proxy Policy Log Messages* on page 37.

Event

Security Services log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
1F000001	ERROR	Security Services / Gateway Anti-Virus	Process failed to start	Cannot start ScanD	ScanD -- Process failed to start	Cannot start ScanD	—
1F010015	INFO	Security Services / Gateway Anti-Virus	Ready for service	ScanD ready	ScanD -- Ready for service	ScanD ready	—
2E000005	ERROR	Security Services / Signature Update	Process exiting	SIGD shutting down	SIGD -- Process exiting	SIGD shutting down	—
2E000006	ERROR	Security Services / Signature Update	Process crashed	SIGD crashed	SIGD -- Process crashed	SIGD crashed	—
2E010018	ERROR	Security Services / Signature Update	Failed to start the signature update for the specified services	Cannot start the signature update for 'IPS'	SIGD -- Failed to the start signature update for the specified services	Cannot start the signature update for '%s'	—
2E010019	ERROR	Security Services / Signature Update	Failed to check the available signature version on the server	Cannot complete the version check	SIGD -- Failed to check the available signature version on the server	Cannot complete the version check	—
2E01001A	ERROR	Security Services / Signature Update	Signature update process failed to start	Cannot start the signature update process	SIGD -- Signature update process failed to start	Cannot start the signature update process	—
2E01001B	ERROR	Security Services / Signature Update	Signature update process crashed	SIGD Worker crashed	SIGD -- Signature update process crashed	SIGD Worker crashed	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
2E020067	ERROR	Security Services / Signature Update	Signature update process for the specified version failed	Manual DLP update for version(4.94) failed (Valid feature key not available)	SIGD -- Signature update process for the specified version failed	%s %s update for version (%s) failed (%s)	—
2E020065	INFO	Security Services / Signature Update	Signature update process started	Scheduled DLP update started	SIGD -- Signature update process started	%s %s update started	—
2E020066	INFO	Security Services / Signature Update	Signature update process completed	Scheduled DLP update for version (4.94) completed	SIGD -- Signature update process completed	%s %s update for version (%s) completed	—
2E020069	INFO	Security Services / Signature Update	Device has the latest signature version for the specified service	Device already has the latest DLP signature version (4.94)	SIGD -- Device has the latest signature version for specified service	Device already has the latest %s signature version (%s)	—
2E010017	WARN	Security Services / Signature Update	License failed to load	Cannot load the license	SIGD -- License failed to load	Cannot load the license	—
23000001	ERROR	Security Services / spamBlocker	Failed to start	Cannot start spamD	spamD -- Failed to start	Cannot start spamD	—
23000002	INFO	Security Services / spamBlocker	Ready for service	spamD ready	spamD -- Ready for service	spamD ready	—

VPN Log Messages

VPN log messages are generated for processes related to the all VPNs configured on your Firebox. This includes changes to the VPN configuration, tunnel status, and daemon activity.

Alarm

VPN log messages of the *Alarm* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
020B0001	INFO	VPN / IPSEC	Tunnel status changed	BOVPN tunnel 'tunnel.2' local 172.16.12.81/255.255.255.255 remote 172.16.13.204/255.255.255.255 under gateway 'gateway.1' is down.	The status of the IPSec tunnel changed to up or down.	%s tunnel '%s' local %s remote %s under gateway '%s' is %s	${tunnel_type} tunnel '${tunnel}' local ${local} remote ${remote} under gateway '$(gateway)' is ${status}

Diagnostic

VPN log messages of the *Debug (Diagnostic)* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02000001	ERROR	VPN / IPSEC	Default certificate not found	The default IPSec certificate is not installed on the device	The IPSec tunnel could not be negotiated because the default IPSec certificate is not installed or is not valid.	The default IPSec certificate is not installed on the device	—
02000002	ERROR	VPN / IPSEC	Failed to read certificate	Could not read [DSA | RSA] certificate with [n] ID	The IPSec tunnel could not be negotiated because the IPSec certificate is not valid.	Could not read %s certificate with %d ID	Could not read ${cert_type} certificate with ${id} ID

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02030002	ERROR	VPN / IPSEC	IKE Phase 1 expecting main mode	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received 'Aggressive mode' exchange type. Expecting main mode.	IKE Phase 1 negotiation failed because of incorrect exchange type in proposal from remote gateway. The log message specifies the expected and received exchange type.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received '%s' exchange type. Expecting main mode.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received '${exchange_type}' exchange type. Expecting main mode.
02030003	ERROR	VPN / IPSEC	IKE Phase 1 expecting aggressive mode	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received 'Main mode' exchange type. Expecting aggressive mode.	IKE Phase 1 negotiation failed because of incorrect exchange type in proposal from remote gateway. The log message specifies the expected and received exchange type.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received '%s' exchange type. Expecting aggressive mode.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received '${exchange_type}' exchange type. Expecting aggressive mode.
02030004	ERROR	VPN / IPSEC	IKE Phase 1 DH group mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received DH group 2, expecting 14	IKE Phase 1 negotiation failed because of incorrect Diffe-Hellman group in proposal from remote gateway. The log message specifies the received and expected group number.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received DH group %d, expecting %d	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received DH group ${received}, expecting ${expected}
02030005	ERROR	VPN / IPSEC	IKE Phase 1 hash mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received hash SHA1, expecting MD5	IKE Phase 1 negotiation failed because of incorrect hash type in proposal from remote gateway. The log message specifies the received and expected hash type.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received hash %s, expecting %s	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received hash ${received}, expecting ${expected}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02030006	ERROR	VPN / IPSEC	IKE Phase 1 encryption mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received encryption 3DES, expecting AES	IKE Phase 1 negotiation failed because of incorrect encryption type in proposal from remote gateway. The log message specifies the received and expected encryption type.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received encryption %s, expecting %s	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received encryption ${received}, expecting ${expected}
02030007	ERROR	VPN / IPSEC	IKE Phase 1 authentication method mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received authentication method PSK, expecting RSA certificate	IKE Phase 1 negotiation failed because of incorrect authentication method in proposal from remote gateway. The log message specifies the received and expected authentication methods.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received authentication method %s, expecting %s	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received authentication method ${received}, expecting ${expected}
02030008	ERROR	VPN / IPSEC	IKE Phase 1 AES key length mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received AES key length 128, expecting 256	IKE Phase 1 negotiation failed because of incorrect AES key length in proposal from remote gateway. The log message specifies the received and expected AES key length.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received AES key length %d, expecting %d	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received AES key length ${received}, expecting ${expected}
02030009	ERROR	VPN / IPSEC	IKE Phase 1 invalid first message	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received invalid main/aggressive mode first message. Check VPN IKE diagnostic log messages for more information.	IKE Phase 1 negotiation failed because of invalid first message received by local gateway. The log message specifies the reason.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received invalid main/aggressive mode first message. Check VPN IKE diagnostic log messages for more information.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received invalid main/aggressive mode first message. Check VPN IKE diagnostic log messages for more information.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02030011	ERROR	VPN / IPSEC	IKE Phase 1 remote gateway ID mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Authentication failure due to mismatched ID setting	IKE Phase 1 negotiation failed because remote ID in gateway configuration did not match proposal from remote gateway.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Authentication failure due to mismatched ID setting	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Authentication failure due to mismatched ID setting
02030012	ERROR	VPN / IPSEC	IKE Phase 1 pre-shared key authentication failure	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Pre-shared key authentication failure	IKE Phase 1 negotiation failed because pre-shared key in proposal did not match gateway configuration.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Pre-shared key authentication failure	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Pre-shared key authentication failure
02030015	ERROR	VPN / IPSEC	IKE Phase 1 retry timeout	IKE phase-1 negotiation from 172.16.12.81:500 to 172.16.12.82:500 failed. Gateway-Endpoint='gateway.1' Reason=Message retry timeout. Check the connection between local and remote gateway endpoints.	IKE Phase 1 negotiation failed because of no response from remote site.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Message retry timeout. Check the connection between local and remote gateway endpoints.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Message retry timeout. Check the connection between local and remote gateway endpoints.
02030017	ERROR	VPN / IPSEC	CA certificate not available	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=No CA certificate available	IKE phase-1 negotiation failed because no Certificate Authority (CA) certificate is available.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=%s	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=${reason}
02030018	ERROR	VPN / IPSEC	IKE Phase 1 peer certificate CA is not supported	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Peer certificate is not issued by known trusted CA	IKE Phase 1 negotiation failed because peer certificate is not issued by a known and trusted Certificate Authority(CA).	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=%s	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=${reason}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02030019	ERROR	VPN / IPSEC	IKE Phase 1 received certificate with invalid CA name	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received certificate with invalid CA name	IKE Phase 1 negotiation failed because of invalid Certificate Authority (CA) name in certificate for remote gateway.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=%s	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=${reason}
02030020	ERROR	VPN / IPSEC	IKE Phase 1 possible shared secret mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Message decryption failed due to possible shared secret mismatch	IKE Phase 1 negotiation failed because of possible shared key mismatch.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Message decryption failed due to possible shared secret mismatch	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Message decryption failed due to possible shared secret mismatch
02030026	ERROR	VPN / IPSEC	DSS certificate ID mismatch	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Authentication failure due to mismatched DSS certificate ID setting	IKE Phase 1 negotiation failed because of mismatched DSS certificate ID setting.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Authentication failure due to mismatched DSS certificate ID setting	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Authentication failure due to mismatched DSS certificate ID setting
02030027	ERROR	VPN / IPSEC	Failed to get ID information from certificate	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Failed to get ID information from certificate 20001	IKE phase-1 negotiation failed because failed to get ID information from certificate.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Failed to get ID information from certificate %d	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Failed to get ID information from certificate ${certificate_id}
02030029	ERROR	VPN / IPSEC	IKE Phase 1 invalid aggressive mode ID	IKE phase-1 negotiation from 198.51.100.2:500 to 203.0.113.2:500 failed. Gateway-Endpoint='gateway.1' Reason=Received ID did not match	IKE Phase 1 negotiation failed because received ID did not match with configured ID on local gateway. Check aggressive mode ID information in gateway endpoint	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received ID did not match with configured	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received ID did not match with configured aggressive mode ID.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				with configured aggressive mode ID.	configuration on both local and remote gateways.	aggressive mode ID.	
02050002	ERROR	VPN / IPSEC	IKE Phase 2 PFS mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received proposal without PFS, Expecting PFS enabled	The IPSec tunnel negotiation failed because the Perfect Forward Secrecy (PFS) value did not match the Phase 2 configuration.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received proposal without PFS, Expecting PFS enabled	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received proposal without PFS, Expecting PFS enabled
02050003	ERROR	VPN / IPSEC	IKE Phase-2 proposal type mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received protocol 'AH'. Expecting 'ESP' in phase-2 proposal.	The IPSec tunnel negotiation failed because the proposal did not match the Phase 2 configuration. The log message specifies the received and expected proposals.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received protocol '%s'. Expecting '%s' in phase-2 proposal.	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received protocol '${received_proto}'. Expecting '${expected_proto}' in phase-2 proposal.
02050004	ERROR	VPN / IPSEC	IKE Phase 2 AH authentication method mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received AH authentication MD5, expecting SHA1	The IPSec tunnel negotiation failed because the proposed AH authentication method did not match the Phase 2 configuration. The log message specifies the received and expected AH authentication method.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received AH authentication %s, expecting %s	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received AH authentication ${received}, expecting ${expected}
02050005	ERROR	VPN / IPSEC	IKE Phase 2 ESP encryption method mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received ESP encryption DES, expecting AES	The IPSec tunnel negotiation failed because the proposed ESP encryption method did not match the Phase 2 configuration. The log message specifies the received and expected ESP encryption method.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received ESP encryption %s, expecting %s	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received ESP encryption ${received}, expecting ${expected}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02050006	ERROR	VPN / IPSEC	IKE Phase 2 PFS DH group mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received PFS DH group 2, expecting 5	The IPSec tunnel negotiation failed because the proposed Perfect Forward Secrecy Diffe-Hellman (PFS DH) group number did not match the Phase 2 configuration. The log message specifies the received and expected PFS DH group numbers.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received PFS DH group %d, expecting %d	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received PFS DH group ${received}, expecting ${expected}
02050007	ERROR	VPN / IPSEC	IKE Phase 2 ESP authentication method mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received ESP authentication MD5-HMAC, expecting SHA1-HMAC	The IPSec tunnel negotiation failed because the proposed ESP authentication method did not match the Phase 2 configuration. The log message specifies the received and expected ESP authentication method.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received ESP authentication %s, expecting %s	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received ESP authentication ${received}, expecting ${expected}
02050008	ERROR	VPN / IPSEC	IKE Phase 2 AES key length mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received AES key length 128, expecting 256	The IPSec tunnel negotiation failed because the proposed AES encryption key length did not match the Phase 2 configuration. The log message specifies the received and expected AES key length.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received AES key length %d, expecting %d	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received AES key length ${received}, expecting ${expected}
0203000A	ERROR	VPN / IPSEC	IKE Phase 1 invalid Main Mode second message	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received invalid main mode second message. Check VPN IKE diagnostic log messages for more information.	IKE Phase 1 negotiation failed because of invalid second message received by local gateway.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received invalid main mode second message. Check VPN IKE diagnostic log messages for more information.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received invalid main mode second message. Check VPN IKE diagnostic log messages for more information.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
0203000B	ERROR	VPN / IPSEC	IKE Phase 1 invalid Main Mode Key Exchange payload	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received invalid main mode KE payload. Check VPN IKE diagnostic log messages for more information.	IKE Phase 1 negotiation failed because local gateway received invalid Main Mode Key Exchange (KE) payload	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received invalid main mode KE payload. Check VPN IKE diagnostic log messages for more information.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received invalid main mode KE payload. Check VPN IKE diagnostic log messages for more information.
0203000C	ERROR	VPN / IPSEC	IKE Phase 1 invalid main mode ID	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received invalid main mode ID payload. Check VPN IKE diagnostic log messages for more information.	IKE Phase 1 negotiation failed because of invalid Main Mode ID payload received by local gateway.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received invalid main mode ID payload. Check VPN IKE diagnostic log messages for more information.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received invalid main mode ID payload. Check VPN IKE diagnostic log messages for more information.
0203000D	ERROR	VPN / IPSEC	IKE Phase 1 invalid aggressive mode hash	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received invalid aggressive mode hash payload. Check VPN IKE diagnostic log messages for more information.	IKE Phase 1 negotiation failed because invalid aggressive mode hash payload received by specified local gateway.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received invalid aggressive mode hash payload. Check VPN IKE diagnostic log messages for more information.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received invalid aggressive mode hash payload. Check VPN IKE diagnostic log messages for more information.
0203000E	ERROR	VPN / IPSEC	IKE Phase 1 invalid Aggressive mode SA payload	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received invalid aggressive mode SA payload. Check VPN IKE diagnostic log messages for more information.	IKE Phase 1 negotiation failed because of invalid Aggressive mode security association (SA) payload received by specified local gateway.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received invalid aggressive mode SA payload. Check VPN IKE diagnostic log messages for more information.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received invalid aggressive mode SA payload. Check VPN IKE diagnostic log messages for more information.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
0203002A	ERROR	VPN / IPSEC	IKE Phase 1 IKE version mismatch	IKE phase-1 negotiation from 198.51.100.2:500 to 203.0.113.2:500 failed. Gateway-Endpoint='gateway.1' Reason=Received IKE version did not match the configured IKE version.	IKE Phase 1 negotiation failed because the received IKE version did not match the IKE version configured on the local gateway. Check the IKE version in the gateway endpoint configuration on both the local and remote gateways.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received IKE version did not match the configured IKE version.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received IKE version did not match the configured IKE version.
0203002B	ERROR	VPN / IPSEC	IKE Phase 1 message received on wrong interface IP	IKE phase-1 negotiation from 198.51.100.2:500 to 192.0.2.2:500 failed. Gateway-Endpoint='gateway.1' Reason=Received message with wrong interface IP address 192.0.2.2. Expecting peer to use remote gateway endpoint IP address 203.0.113.2.	IKE Phase 1 negotiation failed because IKE message from the peer was received on the wrong interface IP address. Check the local and remote gateway IP address in the gateway endpoint configuration on both the local and remote gateways.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received message with wrong interface IP address %s. Expecting peer to use remote gateway endpoint IP address %s.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received message with wrong interface IP address ${received_ip}. Expecting peer to use remote gateway endpoint IP address ${expected_ip}.
0205000A	ERROR	VPN / IPSEC	IKE Phase 2 tunnel route mismatch	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway='gateway.1' Reason=No matching tunnel route for peer proposed local:192.168.81.0/24 remote:192.168.82.0/28	The IPSec tunnel negotiation failed because the proposed tunnel routes did not match the tunnel configuration. The log message specifies the received and expected tunnel routes.	IKE phase-2 negotiation from %s to %s failed. Gateway='%s' Reason=No matching tunnel route for peer proposed local:%s/%d remote:%s/%d	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Gateway='${gateway}' Reason=No matching tunnel route for peer proposed local:${tr_local} remote:${tr_remote}
0205000B	ERROR	VPN / IPSEC	IKE Phase 2 message retry timeout	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Message retry timeout. Check VPN IKE diagnostic log messages for more information.	The IPSec tunnel negotiation failed because an expected response was not received before the message retry timeout.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Message retry timeout. Check VPN IKE diagnostic log messages for more information.	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Message retry timeout. Check VPN IKE diagnostic log messages for more information.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
0205000C	ERROR	VPN / IPSEC	IKE Phase2 message retry timeout because Phase 1 SA expired	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Message retry timeout because phase-1 SA expired	The IPSec tunnel negotiation failed because the Phase 1 Security Association (SA) expired.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Message retry timeout because phase-1 SA expired	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Message retry timeout because phase-1 SA expired
0205000D	ERROR	VPN / IPSEC	IKE Phase 2 PFS not enabled	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Received proposal with PFS. PFS not enabled.	The IPSec tunnel negotiation failed because the Perfect Forward Secrecy (PFS) value did not match the Phase 2 configuration.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Received proposal with PFS. PFS not enabled.	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Received proposal with PFS. PFS not enabled.
0205000E	ERROR	VPN / IPSEC	IKE Phase 2 wait timeout	IKE phase-2 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1' Reason=Message was not received in expected time. Check the connection between local and remote gateway endpoints.	The IPSec tunnel negotiation failed because an expected response was not received before the expected time.	IKE phase-2 negotiation from %s to %s failed. Tunnel='%s' Reason=Message was not received in expected time. Check the connection between local and remote gateway endpoints.	IKE phase-2 negotiation from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}' Reason=Message was not received in expected time. Check the connection between local and remote gateway endpoints.
021A0001	ERROR	VPN / IPSEC	Dropped received IKEv2 message	Dropped IKEv2 IKE_SA_INIT message from 172.16.12.82:500. Reason=message has invalid initiator SPI (all zeros)	Dropped received invalid IKEv2 message.	Dropped IKEv2 %s message from %s. Reason=%s	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Reason=${reason}
021A0002	ERROR	VPN / IPSEC	IKE SA not found to handle IKE_SA_INIT_R message	Dropped IKEv2 IKE_SA_INIT message from 172.16.12.82:500. Reason=IKE SA not found to handle message with message ID 0x0.	IKE SA was not found to handle the received IKE_SA_INIT_R message.	Dropped IKEv2 %s message from %s. Reason=IKE SA not found to handle message with message ID 0x%x.	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Reason=IKE SA not found to handle message with message ID ${recvd_message_id}.
021A0003	ERROR	VPN / IPSEC	Gateway	Dropped IKEv2 IKE_SA_INIT	Gateway endpoint was not found to handle the received IKE_SA_	Dropped IKEv2 %s	Dropped IKEv2 ${exchange_type}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			endpoint not found to handle IKE_SA_INIT_R message	message from 172.16.12.82:500. Reason='gateway.1' gateway endpoint not found to handle message with message ID 0x0.	INIT_R message	message from %s. Reason='%s' gateway endpoint not found to handle message with message ID 0x%x.	message from ${peer_addr}. Reason='${gw-ep}' gateway endpoint not found to handle IKE_SA_INIT message with message ID ${recvd_message_id}.
021A0005	ERROR	VPN / IPSEC	Invalid message ID in IKEv2 exchange	Dropped IKEv2 IKE_SA_INIT message from 172.16.12.82:500. Gateway-Endpoint='gateway.1'. Reason=Invalid message ID in request message.	Received IKEv2 message was dropped because it has invalid message ID.	Dropped IKEv2 %s message from %s. Gateway-Endpoint='%s'. Reason=Invalid message ID in %s message.	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Gateway-Endpoint='${gw-ep}'. Reason=Invalid message ID in ${req_or_resp} message.
021A0006	ERROR	VPN / IPSEC	IKEv2 gateway endpoint was not found to handle the received message	IKEv2 IKE_SA_INIT exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Reason=Matching gateway endpoint not found.	IKEv2 gateway endpoint was not found to handle the received message.	IKEv2 %s exchange from %s to %s failed. Reason=Matching gateway endpoint not found.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Reason=Matching gateway endpoint not found.
021A0007	ERROR	VPN / IPSEC	IKEv2 gateway endpoint version not matched	IKEv2 IKE_SA_INIT exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received IKE version did not match the configured IKE version.	IKEv2 message exchange failed because the received IKE version did not match the IKE version configured on the local gateway. Check the IKE version in the gateway endpoint configuration on both local and remote gateways.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received IKE version did not match the configured IKE version.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received IKE version did not match the configured IKE version.
021A0008	ERROR	VPN / IPSEC	IKEv2 gateway endpoint is disabled	IKEv2 IKE_SA_INIT exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=gateway endpoint is disabled.	The IKEv2 gateway endpoint is disabled. It cannot be used in tunnel negotiation.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=gateway endpoint is disabled.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=gateway endpoint is disabled.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
021A0009	ERROR	VPN / IPSEC	IKEv2 gateway ID mismatch	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Gateway endpoint with matching ID was not found.	IKEv2 IKE_AUTH negotiation failed because the remote ID configured in the gateway endpoint did not match proposed ID received from the remote gateway.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Gateway endpoint with matching ID was not found.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Gateway endpoint with matching ID was not found.
021A000A	ERROR	VPN / IPSEC	IKEv2 IKE_SA_INIT message received on wrong interface	IKEv2 IKE_SA_INIT exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received message on wrong interface 'eth0'(index:3). Expecting it to be received on 'eth6'.	IKEv2 IKE_SA_INIT negotiation failed because IKE message from peer was received on the wrong interface.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received message on wrong interface '%s'(index:%d). Expecting it to be received on '%s'.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received message on wrong interface. '${received_if}' (index:${received_ifindex}). Expecting it to be received on '${expected_if}'.
021A000B	ERROR	VPN / IPSEC	IKEv2 remote gateway endpoint ID mismatch	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received ID did not match the configured remote gateway endpoint ID.	IKEv2 IKE_AUTH negotiation failed because the remote ID in the gateway endpoint configuration did not match the proposed ID received from the remote gateway.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received ID did not match the configured remote gateway endpoint ID.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received ID did not match the configured remote gateway endpoint ID.
021A000C	ERROR	VPN / IPSEC	IKEv2 local gateway endpoint ID mismatch	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received ID did not match the configured local gateway endpoint ID.	IKEv2 IKE_AUTH negotiation failed because the local ID in the gateway endpoint configuration did not match the proposed ID received from the remote gateway.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received ID did not match the configured local gateway endpoint ID.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received ID did not match the configured local gateway endpoint ID.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
021A000D	ERROR	VPN / IPSEC	Received IKEv2 message does not have expected payloads	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received IKE_AUTH response message does not have the expected payloads.	IKEv2 message exchange failed because the received message from the peer does not have the expected payloads	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received %s message does not have the expected payloads.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received ${msg_info} message does not have the expected payloads.
021A000E	ERROR	VPN / IPSEC	IKEv2 IKE proposal mismatch	IKEv2 IKE_SA_INIT exchange from 198.51.100.2:500 to 203.0.113.2:500 failed. Gateway-Endpoint='gateway.1'. Reason=IKE proposal did not match. Received encryption 3DES, expected AES.	The IKEv2 message exchange failed because the IKE proposal in the received message did not match the expected proposal.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=%s	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=${msg_info}
021A000F	ERROR	VPN / IPSEC	IKEv2 KE DH-Group mismatch	IKEv2 IKE_SA_INIT exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=DH-Group 14 in the KE payload does not match DH-Group 5 selected in the IKE_SA_INIT response proposal.	IKEv2 message exchange failed because the DH group in the received Key Exchange (KE) payload does not match the DH-Group in the selected proposal.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=DH-Group %d in the KE payload does not match DH-Group %d selected in the %s proposal.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=DH-Group ${recvd_dh_group} in the KE payload does not match the DH-Group ${selected_dh_group} selected in the ${msg_info} proposal.
021A0010	ERROR	VPN / IPSEC	IKEv2 IPSec KE DH-Group mismatch	IKEv2 CREATE_CHILD_SA exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1'. Reason=DH-Group 14 in the KE payload does not match DH-Group 5 selected in the CREATE_CHILD_SA request proposal.	IKEv2 message exchange failed because the DH group in the received Key Exchange (KE) payload does not match the DH-Group in the selected proposal.	IKEv2 %s exchange from %s to %s failed. Tunnel='%s'. Reason=DH-Group %d in the KE payload does not match DH-Group %d selected in the %s proposal.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=DH-Group ${recvd_dh_group} in the KE payload does not match the DH-Group ${selected_dh_group} selected in the ${msg_info} proposal.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
021A0011	ERROR	VPN / IPSEC	Received unacceptable traffic selector during first CHILD SA negotiation.	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received unacceptable traffic selector in IKE_AUTH request.	IKEv2 first CHILD SA creation failed because the peer sent an unacceptable traffic selector.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received unacceptable traffic selector in %s.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received unacceptable traffic selector in ${msg_info}.
021A0012	ERROR	VPN / IPSEC	IKEv2 peer authentication method mismatch.	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received authentication method PSK, expecting RSA certificate.	IKEv2 tunnel negotiation failed because the incorrect authenticate method was proposed by the remote gateway.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received authentication method %s, expecting %s.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Reason=Received authentication method ${received}, expecting ${expected}.
021A0013	ERROR	VPN / IPSEC	IKEv2 peer authentication failed	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Remote gateway endpoint RSA certificate authentication failed.	IKEv2 tunnel negotiation failed because the local gateway could not authenticate the remote gateway.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Remote gateway endpoint %s authentication failed.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Reason=Remote gateway endpoint ${auth_method} authentication failed.
021A0014	ERROR	VPN / IPSEC	IKEv2 PSK mismatch	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Remote gateway endpoint authentication failed due to a possible shared secret mismatch.	IKEv2 tunnel negotiation failed because of possible PSK mismatch.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Remote gateway endpoint authentication failed due to a possible shared secret mismatch.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Reason=Remote gateway endpoint authentication failed due to a possible shared secret mismatch.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
021A0015	ERROR	VPN / IPSEC	Received IKEv2 IKE_ SA_INIT notification error message.	IKEv2 IKE_SA_INIT exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received N(NO_ PROPOSAL_CHOSEN) message.	IKEv2 IKE_SA_INIT negotiation failed because the peer sent a notification error message.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received %s message.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=Received ${notify_msg} message.
021A0016	ERROR	VPN / IPSEC	Received IKEv2 CREATE_ CHILD_ SA/IKE_ AUTH notification error message.	IKEv2 IKE_AUTH exchange from 10.139.36.185:500 to 10.139.36.195:500 failed. Tunnel='tunnel.1'. Reason=Received N(NO_ PROPOSAL_CHOSEN) message.	IKEv2 CREATE_CHILD_ SA/IKE_AUTH negotiation failed because peer sent a notification error message.	IKEv2 %s exchange from %s to %s failed. Tunnel='%s'. Reason=Received %s message.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel_name}'. Reason=Received ${notify_msg} message.
021A0018	ERROR	VPN / IPSEC	IKEv2 tunnel proposal mismatch.	IKEv2 CREATE_CHILD_SA exchange from 198.51.100.2:500 to 203.0.113.2:500 failed. Tunnel='tunnel.1'. Reason=IPSec proposal did not match. Received encryption 3DES, expected AES.	The IKEv2 message exchange failed because the IPSec proposal in the received message did not match the expected proposal.	IKEv2 %s exchange from %s to %s failed. Tunnel='%s'. Reason=%s	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}'. Reason=${msg_info}
021A0019	ERROR	VPN / IPSEC	Received invalid SPI during first CHILD SA negotiation.	IKEv2 IKE_AUTH exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1'. Reason=Peer proposed invalid SPI in IKE_AUTH request.	IKEv2 first CHILD SA creation failed because the peer sent an invalid SPI.	IKEv2 %s exchange from %s to %s failed. Tunnel='%s'. Reason=Peer proposed invalid SPI in %s.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}'. Reason=Peer proposed invalid SPI in ${msg_info}.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
021A001A	ERROR	VPN / IPSEC	Received invalid SPI during IKEv2 IPSec SA rekey	IKEv2 CREATE_CHILD_SA exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Tunnel='tunnel.1'. Reason=Could not find child SA by received SPI 0xbaba1509 in CREATE_CHILD_ SA(REKEY[CHILD SA]) request.	IKEv2 IPSec SA rekey failed because the peer sent an invalid SPI.	IKEv2 %s exchange from %s to %s failed. Tunnel='%s'. Reason=Could not find child SA by received SPI %0x in %s.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Tunnel='${tunnel}'. Reason=Could not find child SA by received SPI ${spi} in ${msg_info}.
021A001B	ERROR	VPN / IPSEC	No response from remote gateway	IKEv2 exchange from 172.16.12.82:500 to 172.16.12.81:500 failed. Gateway-Endpoint='gateway.1'. Reason=No response for IKE_AUTH request message. Check the connection between the local and remote gateway endpoints.	IKEv2 connection was terminated because there was no response from the remote site.	IKEv2 exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=No response for %s message. Check the connection between the local and remote gateway endpoints.	IKEv2 exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'. Reason=No response for ${msg_info} message. Check the connection between the local and remote gateway endpoints.
021A001D	ERROR	VPN / IPSEC	IKEv2 gateway ID mismatch	IKEv2 IKE_AUTH exchange from 198.51.100.2 to 203.0.113.2:500 failed. Gateway-Endpoint='ikev2_ mobileuser'. Reason=The Mobile VPN with IKEv2 profile is not enabled.	IKEv2 IKE_AUTH negotiation failed because Mobile VPN for IKEv2 is not enabled on this gateway.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=The Mobile VPN with IKEv2 profile is not enabled.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Mobile VPN with IKEv2 profile is not enabled.
021A001E	ERROR	VPN / IPSEC	IKEv2 received invalid EAP information	IKEv2 IKE_AUTH EAP exchange from 198.51.100.2:4500 to 203.0.113.2:4500 failed. Gateway-Endpoint='WG IKEv2 MVPN'. Reason='example' authentication domain is not configured.	IKEv2 IKE_AUTH EAP negotiation failed because IKEv2 Mobile VPN client sent invalid information.	IKEv2 %s EAP exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=%s	IKEv2 ${exchange_type} EAP exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=${reason}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
021A001F	ERROR	VPN / IPSEC	IKEv2 IKE_ SA_INIT message received on wrong interface IP	IKEv2 IKE_SA_INIT exchange from 198.51.100.2:500 to 192.0.2.2:500 failed. Gateway-Endpoint='gateway.1'. Reason=Received message with wrong interface IP address 192.0.2.2. Expecting peer to use remote gateway endpoint IP address 203.0.113.2.	IKEv2 message exchange failed because IKE message from the peer was received on the wrong interface IP address. Check the local and remote gateway IP address in the gateway endpoint configuration on both the local and remote gateways.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received message with wrong interface IP address %s. Expecting peer to use remote gateway endpoint IP address %s.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received message with the wrong interface IP address ${received_ip}. Expecting peer to use remote gateway endpoint IP address ${expected_ip}.
021A0020	ERROR	VPN / IPSEC	IKEv2 IKE_ AUTH message received on wrong interface IP	IKEv2 IKE_AUTH exchange from 198.51.100.2:500 to 192.0.2.2:500 failed. Gateway-Endpoint='m500-197'. Reason=Received message with the wrong interface IP address 192.0.2.2. Expecting peer to use remote gateway endpoint IP address 203.0.113.2.	IKEv2 message exchange failed because IKE message from the peer was received on the wrong interface IP address. Check the local and remote gateway IP address in the gateway endpoint configuration on both the local and remote gateways.	IKEv2 %s exchange from %s to %s failed. Gateway-Endpoint='%s'. Reason=Received message with wrong interface IP address %s. Expecting peer to use remote gateway endpoint IP address %s.	IKEv2 ${exchange_type} exchange from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}' Reason=Received message with wrong interface IP address ${received_ip}. Expecting peer to use remote gateway endpoint IP address ${expected_ip}.
02030010	INFO	VPN / IPSEC	IKE Phase 1 matching Main Mode policy not found	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Reason=Main mode matching policy not found	IKE Phase 1 negotiation because local gateway did not find a matching Aggressive mode policy.	IKE phase-1 negotiation from %s to %s failed. Reason=Main mode matching policy not found	IKE phase-1 negotiation from ${local_ addr} to ${peer_addr} failed. Reason=Main mode matching policy not found
02030013	INFO	VPN / IPSEC	IKE Phase 1 negotiation failed	IKE phase-1 negotiation from 2.2.2.2:500 to 1.1.1.1:500 failed. Reason=Received invalid message	IKE Phase 1 negotiation failed because of the reason specified in the log	IKE phase-1 negotiation from %s:%d to %s:%d failed. Reason=%s	IKE phase-1 negotiation from ${src}:${sport} to ${dst}:${dport} failed - ${reason}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02030014	INFO	VPN / IPSEC	Received informational error message	Received 'Invalid Exchange Type' message from 172.16.12.81:500 for 'gateway.1' gateway endpoint. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.	Received the specified information or error message from remote gateway.	Received '%s' message from %s for '%s' gateway endpoint. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.	Received '${info_msg}' message from ${peer_addr} for '${gw-ep}' gateway endpoint. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.
02030025	INFO	VPN / IPSEC	Received IKE message for unknown Phase 1 SA	Received IKE message from 172.16.13.204:500 for unknown P1 SA. Sending delete message to remote gateway 'gateway.1'.	Received IKE message for unknown P1 SA. Sending delete message to remote gateway	Received IKE message from %s for unknown P1 SA. Sending delete message to remote gateway '%s'.	Received IKE message from ${peer_addr} for unknown P1 SA. Sending delete message to remote gateway '${gateway}'.
02030028	INFO	VPN / IPSEC	IKE Phase 1 message received on wrong interface	IKE phase-1 negotiation from 198.51.100.2:500 to 203.0.113.2:500 failed. Reason=Received IKE message on wrong interface 'eth0' (index:3). Expecting it to be received on 'eth6'.	IKE Phase 1 negotiation failed because of IKE message peer was received on wrong interface.	IKE phase-1 negotiation from %s to %s failed. Reason=Received IKE message on wrong interface '%s'(index:%d). Expecting it to be received on '%s'.	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Reason=Received IKE message on wrong interface '${received_if}' (index:${received_ifindex}). Expecting it to be received on '${expected_if}'
02050010	INFO	VPN / IPSEC	Received quick mode informational error message	Received 'No Proposal Chosen' message from 172.16.12.81:500 for 'tunnel.1' tunnel. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.	Remote gateway sent an information error message in response to VPN tunnel proposal.	Received '%s' message from %s for '%s' tunnel. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.	Received '${info_msg}' message from ${peer_addr} for '${tunnel}' tunnel. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.
02050011	INFO	VPN / IPSEC	Dropped simultaneous Phase 2 negotiation	Dropped a simultaneous phase-2 negotiation from the peer 172.16.13.204:500	Firebox or XTM device dropped phase-2 negotiation because of another Phase 2 negotiation in progress.	Dropped a simultaneous phase-2 negotiation from the peer %s	Dropped a simultaneous IPSec negotiation from the peer ${peer_addr}
02060006	INFO	VPN / IPSEC	Mobile VPN with IPSec user	MUVPN user 'user.1' is authenticated without group information.	Specified Mobile VPN with IPSec user successfully authenticated, but is not a member of any group.	MUVPN user '%s' is authenticated without group information.	MUVPN user '${user_name}' is authenticated without group information

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			connected with no group				
02060007	INFO	VPN / IPSEC	Mobile user group information	MUVPN user 'user.1' is a member of 'muvpn' group.	Specified Mobile VPN with IPSec user belongs to the specified group.	MUVPN user '%s' is a member of '%s' group.	MUVPN user '${user_name}' is a member of '${group_name}' group.
02080001	INFO	VPN / IPSEC	IKE phase-1 negotiated successful	BOVPN phase-1 main-mode completed successfully as initiator for 'gateway.1' gateway endpoint. local-gw:172.16.12.81:500 remote-gw:172.16.13.204:500 SA ID:0x9d5e7809	IKE phase-1 negotiation was successfully completed.	%s phase-1 %s completed successfully as %s for '%s' gateway endpoint. local-gw:%s:%d remote-gw:%s:%d SA ID:0x%08x	${tunnel_type} phase-1 ${nego_mode} completed successfully as ${nego_role} for '${gateway}' gateway endpoint. local-gw:${src}:${sport} remote-gw:${dst}:${dport} SA ID:${p1said}
0203000F	INFO	VPN / IPSEC	IKE Phase 1 matching aggressive mode policy not found	IKE phase-1 negotiation from 172.16.12.82:500 to 172.16.12.81:500 failed. Reason=Aggressive mode matching policy not found	IKE Phase 1 negotiation because local gateway did not find a matching aggressive mode policy.	IKE phase-1 negotiation from %s to %s failed. Reason=Aggressive mode matching policy not found	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Reason=Aggressive mode matching policy not found
021A0004	INFO	VPN / IPSEC	IKEv2 IKE SA is in deleting state	Dropped IKEv2 IKE_SA_INIT message from 172.16.12.82:500. Gateway-Endpoint='gateway.1'. Reason=IKE SA is in DELETING state.	Received IKEv2 message was ignored because the corresponding IKE SA to handle the message was in DELETING state.	Dropped IKEv2 %s message from %s. Gateway-Endpoint='%s'. Reason=IKE SA is in %s state.	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Gateway-Endpoint='${gw-ep}' Reason=IKE SA is in ${ikev2_ikesa_state} state.
021A0017	INFO	VPN / IPSEC	IKEv2 IKE SA established	IKEv2 IKE SA established successfully as initiator for 'gateway.1' gateway endpoint. local-gw:10.139.36.185:500 remote-gw:10.139.36.195:500 SA ID:0xbc2188a5.	IKEv2 IKE SA is established because IKE_AUTH negotiation is finished or IKE SA is rekeyed.	IKEv2 IKE SA established successfully as %s for '%s' gateway endpoint. local-gw:%s remote-gw:%s SA ID:0x%08x.	IKEv2 IKE SA established successfully as ${exchange_role} for '${gw-ep}' gateway endpoint. local-gw:${local_addr} remote-gw:${peer_addr} SA ID:${sa_id}.
021A001C	INFO	VPN / IPSEC	IKEv2 IKE SA is waiting for the user	Dropped IKEv2 IKE_AUTH message from 198.51.100.2:4500. Gateway-Endpoint='ikev2_	The Firebox ignored an IKEv2 message because the corresponding IKE SA is waiting	Dropped IKEv2 %s message from %s. Gateway-Endpoint='%s'.	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Gateway-Endpoint='${gw-ep}'

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			authentication result	mobileuser'. Reason=Waiting for the EAP_MSCHAPv2 user authentication result.	for the user authentication result from the authentication module.	Reason=Waiting for the %s user authentication result.	Reason=Waiting for the ${user-auth-protocol} user authentication result.
021A001C	INFO	VPN / IPSEC	IKEv2 IKE SA is waiting for the user authentication result	Dropped IKEv2 IKE_AUTH message from 198.51.100.2:4500. Gateway-Endpoint='ikev2_ mobileuser'. Reason=Waiting for the EAP_MSCHAPv2 user authentication result.	The Firebox ignored an IKEv2 message because the corresponding IKE SA is waiting for the user authentication result from the authentication module.	Dropped IKEv2 %s message from %s. Gateway-Endpoint='%s'. Reason=Waiting for the %s user authentication result.	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Gateway-Endpoint='${gw-ep}' Reason=Waiting for the ${user-auth-protocol} user authentication result.
02020001	WARN	VPN / IPSEC	IP address not available for Mobile VPN with IPSec user	Virtual IP address from 'abcd' address pool is not available for Mobile VPN with IPSec user 'Bob'	All virtual IP addresses allocated to this Mobile VPN with IPSec group are already assigned. New Mobile VPN with IPSec tunnels cannot be established unless existing tunnels are deleted.	Virtual IP address from '%s' address pool is not available for Mobile VPN with IPSec user '%s'	Virtual IP address from ${pool_name} address pool is not available for Mobile VPN with IPSec user ${user}
02030016	WARN	VPN / IPSEC	Mobile user rejected - maximum user connections reached	Rejected MUVPN IPSec user from 2.2.2.2 because maximum allowed user connections has been reached. Maximum:50	Specified Mobile VPN with IPSec user connection rejected because the specified concurrent user connections limit has been reached. The log message specifies the concurrent user connections limit.	Rejected MUVPN IPSec user from %s because maximum allowed user connections has been reached. Maximum:%d	Rejected MUVPN IPSec user from ${peer_addr} because maximum allowed user connections has been reached. Maximum:${max_value}
02030021	WARN	VPN / IPSEC	DPD R_U_THERE_ACK not received	Remote gateway 'gateway.1' with IP 172.16.13.204:500 did not send DPD R_U_THERE_ACK message. 2 retries left	Firebox or XTM device sent a DPD_R_U_THERE request to remote gateway, but did not receive DPD R_U_THERE_ACK response. The log message specifies the number of retries before it will delete the VPN tunnel.	Remote gateway '%s' with IP %s did not send DPD R_U_THERE_ACK message. %d retries left	Remote gateway '${gw-ep}' with IP ${peer_addr} did not send DPD R_U_THERE_ACK message. ${n} retries left.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02030022	WARN	VPN / IPSEC	DPD max failure	Remote gateway 'gateway.1' with IP 172.16.13.204:500 presumed dead due to DPD failure. Deleted all tunnels that use this gateway. Check the connection between local and remote gateway endpoints.	The Firebox or XTM device deleted a VPN tunnel because the remote gateway did not respond to DPD R_U_THERE requests.	Remote gateway '%s' with IP %s presumed dead due to DPD failure.%s	Remote gateway '${gw-ep}' with IP ${peer_addr} presumed dead due to DPD failure. ${action}
02030023	WARN	VPN / IPSEC	Did not receive KEEP_ ALIVE_ACK response	Remote gateway 'gateway.1' with IP 172.16.13.204:500 did not send KEEP_ALIVE_ACK message. 2 retries left.	Firebox or XTM device sent a KEEP_ALIVE request to remote gateway, but did not receive KEEP_ALIVE_ACK response. The log message specifies the number of retries before it will delete the VPN tunnel.	Remote gateway '%s' with IP %s did not send KEEP_ ALIVE_ACK message. %d retries left.	Remote gateway '${gw-ep}' with IP ${peer_addr} did not send KEEP_ ALIVE_ACK message. ${n} retries left.
02030024	WARN	VPN / IPSEC	Deleted VPN tunnels due to keep-alive failure	Remote gateway 'gateway.1' with IP 172.16.13.204:500 presumed dead due to keep-alive negotiation failure. Deleted all tunnels that use this gateway. Check the connection between local and remote gateway endpoints.	Firebox or XTM device deleted one or more VPN tunnels because the remote gateway did not respond to keep-alive requests.	Remote gateway '%s' with IP %s presumed dead due to keep-alive negotiation failure.%s	Remote gateway '${gw-ep}' with IP ${peer_addr} presumed dead due to keep-alive negotiation failure.${action}
02060001	WARN	VPN / IPSEC	Received XAuth fail notification	Received XAuth failed notification from 172.16.24.1:4500. Group:'ToFirebox_mu'	Received notification that Extended Authentication(XAuth) failed. Aborting XAuth negotiation.	Received XAuth failed notification from %s. Group:'%s'	Received XAuth failed notification from ${peer_addr}. Group:'${gateway}'
02060002	WARN	VPN / IPSEC	Rejected PSK authentication, Expect client XAUTH enabled.	Rejected phase-1 authentication method PSK from 172.16.24.1:4500, expecting client XAUTH enabled.	Rejected proposed Phase 1 authentication method because Firebox or XTM Device expects client Extended Authentication (XAuth) enabled.	Rejected phase-1 authentication method %s from %s, expecting client XAUTH enabled.	Rejected phase 1 authentication method ${auth_method} from ${peer_addr}, expecting client XAUTH enabled.
02060003	WARN	VPN / IPSEC	Rejected PSK authentication, Expect server	Rejected phase-1 authentication method PSK from 172.16.24.1:4500, expecting server XAUTH enabled.	Rejected proposed Phase 1 authentication method because Firebox or XTM Device expects	Rejected phase-1 authentication method %s from %s, expecting server	Rejected phase 1 authentication method ${auth_method} from ${peer_addr}, expecting server XAUTH

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			XAUTH enabled.		server Extended Authentication (XAuth) enabled.	XAUTH enabled.	enabled.
02060004	WARN	VPN / IPSEC	XAuth negotiation failed due to mismatched mode	XAuth negotiation from 172.16.24.1:4500 failed due to a mismatched XAuthMode.	Mobile VPN with IPSec Extended Authentication(XAuth) negotiation failed because of mismatched authentication mode.	XAuth negotiation from %s failed due to a mismatched XAuthMode.	XAuth negotiation from ${peer_addr} failed due to a mismatched XAuthMode
02060005	WARN	VPN / IPSEC	Mobile VPN with IPSec authentication failed because of unresponsive peer	MUVPN user authentication failed due to unresponsive peer at 172.16.24.1:4500	Mobile VPN with IPSec user authentication failed because the peer did not respond.	MUVPN user authentication failed due to unresponsive peer at %s	MUVPN user authentication failed due to unresponsive peer at %s
0205000F	WARN	VPN / IPSEC	Rejected Phase 2 negotiation due to incorrect gateway	Rejected phase-2 negotiation from 172.16.12.82:500 because 'gateway.1*1' is not the preferred IKE gateway endpoint.	Rejected Phase 2 negotiation the proposal did not use the preferred IKE gateway endpoint.	Rejected phase-2 negotiation from %s because '%s' is not the preferred IKE gateway endpoint.	Rejected quick mode negotiation from ${peer_addr} because '${gw-ep}' is not the preferred IKE gateway endpoint.
5B010004	INFO	VPN / L2TP	Update user session	Updated Mobile VPN with L2TP session for user 'Firebox-DB\test', virtual IP address '192.168.113.2'.	Mobile VPN with L2TP updated the session for the specified user. The log message specifies the assigned virtual IP address.	Updated Mobile VPN with L2TP session for user '%s\%s', virtual IP address '%s'.	—
5B010005	INFO	VPN / L2TP	Delete user session	Deleted Mobile VPN with L2TP session for user 'Firebox-DB\test', virtual IP address '192.168.113.2'.	Deleted a Mobile VPN with L2TP session with the specified virtual IP address.	Deleted Mobile VPN with L2TP session for user '%s\%s', virtual IP address '%s'.	—
25000000	INFO	VPN / SSLVPN	User login	Mobile VPN with SSL user tsmith logged in. Virtual IP address is	A user logged in to VPN with SSL. The log message specifies the	%s %s logged in. Virtual IP address is %s. Real IP	${vpn_user_type} ${user_name} logged in. Virtual IP address is

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				192.168.113.2. Real IP address is 192.51.100.2.	VPN user type,and the user's name, virtual IP address, and real IP address.	address is %s.	${virtual_ipaddr}. Real IP address is ${real_ipaddr}.
25000001	INFO	VPN / SSLVPN	User log off	Mobile VPN with SSL user tsmith logged off. Virtual IP address is 192.168.113.2.	The VPN with SSL user with the specified virtual IP address logged out.	%s %s logged off. Virtual IP address is %s.	${vpn_user_type} ${user_name} logged off. Virtual IP address was ${virtual_ipaddr}.

Event

VPN log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02010001	INFO	VPN / IPSEC	IKE process starts	WatchGuard iked v11.6.B341909 (C) 1996-2012 WatchGuard Technologies Inc. starts at Wed Jun 30 21:49:08 2012	The IPSec IKE process started.	WatchGuard iked v%s %s starts at %s	—
02010002	INFO	VPN / IPSEC	Configuration update started	Started processing a configuration setting	An IPSec configuration update started.	Started to process a configuration setting	—
02010003	INFO	VPN / IPSEC	Configuration update completed	A configuration setting has been processed successfully	An IPSec configuration update was successfully completed.	A configuration setting has been processed successfully	—
02070001	INFO	VPN / IPSEC	Tunnel established or re-keyed	'gateway.1' BOVPN IPSec tunnel is established. local:192.168.81.0/28 remote:192.168.25.0/28 in-SA:0x445e72b7 out-SA:0x5f9f256f role:responder	The IPSec tunnel was established or re-keyed successfully. The log message includes the security association identifiers.	'%s' %s IPSec tunnel is %s. local:%s remote:%s in-SA:0x%08x out-SA:0x%08x role:%s	${gateway} ${tunnel_type} IPSec tunnel is ${action}. local:${local} remote:${remote} in-spi:${in_spi} out-spi:${out_spi} role:${nego_role}
02090002	INFO	VPN / IPSEC	IKE process -- FireCluster role changed	A FireCluster failover occurred. The cluster master has changed.	The cluster master has changed because of a FireCluster failover. The local device will not handle IKE negotiation.	A FireCluster failover occurred. The cluster master has changed.	—
02010004	WARN	VPN / IPSEC	Device not activated	WARNING! Tunnel negotiation is NOT allowed because the local box is not activated yet(no "LIVESECURITY" feature key is found)!!	The device is not activated. IPSec tunnels cannot be established.	WARNING! Tunnel negotiation is NOT allowed because the local box is not activated yet(no "LIVESECURITY" feature key is found)!!	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
02090001	WARN	VPN / IPSEC	BOVPN tunnel limit reached	The maximum number of allowed active BOVPN tunnels has been reached (Maximum: 500 Current: 500).	The maximum allowed number of BOVPN tunnel routes have been established. No new tunnel routes can be created until active tunnel routes expire or are deleted.	The maximum number of active allowed BOVPN tunnels has been reached (Maximum: %d Current: %d)	—
5B010002	INFO	VPN / L2TP	Configuration updated	Updating configuration for Mobile VPN with L2TP.	The Mobile VPN with L2TP daemon received a configuration update.	Updating configuration for Mobile VPN with L2TP.	—
5B010003	INFO	VPN / L2TP	Daemon stopped	Stopped Mobile VPN with L2TP daemon.	The Mobile VPN with L2TP daemon stopped.	Stopped Mobile VPN with L2TP daemon.	—

Mobile Security Log Messages

Mobile Security log messages are generated for activity related to traffic through your Firebox from mobile devices. This includes traffic related to FireClient and Endpoint Manager.

Event

Mobile Security log messages of the *Event* log type.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
70000001	ERROR	Mobile Security / Endpoint Manager	Mobile security license limit reached	Rejected a FireClient user login because the licensed maximum number of concurrent Mobile Security users has been reached. Maximum: 50	A user login from FireClient was rejected because the number of concurrently connected Mobile Security users has reached the limit supported by the Mobile Security license. The log message specifies the maximum allowed number of concurrent Mobile Security users.	Rejected a FireClient user login because the licensed maximum number of concurrent Mobile Security users has been reached. Maximum: %d	—
70010000	INFO	Mobile Security / Endpoint Manager	Mobile device connect	Mobile device eee66f78-3d74-4002-8161-95938dca4390 is connected.	FireClient on the device has connected to the Firebox.	Mobile device %s is connected.	—
70010001	INFO	Mobile Security / Endpoint Manager	Mobile device user already login	Mobile device eee66f78-3d74-4002-8161-95938dca4390: user joe has already logged in.	User has logged in to Firebox from the device prior to the connection request.	Mobile device %s: user %s has already logged in.	—
70010002	INFO	Mobile Security / Endpoint Manager	Mobile device user login	Mobile device eee66f78-3d74-4002-8161-95938dca4390: user joe logged in.	User has logged in to Firebox through FireClient on the device.	Mobile device %s: user %s logged in.	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
70010003	INFO	Mobile Security / Endpoint Manager	Mobile device user logout	Mobile device eee66f78-3d74-4002-8161-95938dca4390: user joe logged out.	User has logged out of Firebox from FireClient on the device.	Mobile device %s: user %s logged out.	—
70010004	INFO	Mobile Security / Endpoint Manager	Mobile device idle disconnected	Mobile device eee66f78-3d74-4002-8161-95938dca4390 is disconnected due to FireClient inactivity.	FireClient on the device is considered disconnected due to inactivity.	Mobile device %s is disconnected due to FireClient inactivity.	—
70010005	INFO	Mobile Security / Endpoint Manager	Mobile device disconneted	Mobile device eee66f78-3d74-4002-8161-95938dca4390 is disconnected.	FireClient on the device has disconnected.	Mobile device %s is disconnected.	—
70010006	INFO	Mobile Security / Endpoint Manager	Mobile device Unknown compliance	Mobile device eee66f78-3d74-4002-8161-95938dca4390 compliance status is Unknown.	Mobile device compliance status is Unknown. This could be because the compliance check is in progress, or because FireClient on the device is not responding.	Mobile device %s compliance status is Unknown.	—
70010007	INFO	Mobile Security / Endpoint Manager	Mobile device Compliant	Mobile device eee66f78-3d74-4002-8161-95938dca4390 compliance status is Compliant.	Mobile device compliance status is Compliant, because it meets the compliance requirements.	Mobile device %s compliance status is Compliant.	—
70010008	INFO	Mobile Security / Endpoint Manager	Mobile device Not Compliant	Mobile device eee66f78-3d74-4002-8161-95938dca4390 compliance status is Not Compliant.	Mobile device compliance status is Not Compliant, because it does not meet the compliance requirements.	Mobile device %s compliance status is Not Compliant.	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
70010009	INFO	Mobile Security / Endpoint Manager	Mobile device user session recreated	Mobile device eee66f78-3d74-4002-8161-95938dca4390: session for user joe is recreated.	User session is recreated because the mobile device IP address changed. .	Mobile device %s: session for user %s is recreated.	—
70020000	INFO	Mobile Security / Endpoint Manager	Mobile device Authorization Agreement sign action	Mobile device eee66f78-3d74-4002-8161-95938dca4390: device authorization agreement (version 1) is accepted by user joe on 2015-09-01 09:10:12 +0800.	The Device Authorization Agreement is either accepted or declined by a user at the specified local time.	Mobile device %s: device authorization agreement (version %d) is %s by user %s on %s.	device ${device id}: device authorization agreement (version ${ver_number}) is ${action} by user ${user} on ${local_time}
70000002	WARN	Mobile Security / Endpoint Manager	Mobile security license high watermark reached	The number of connected Mobile Security users has reached 90 percent of the licensed capacity. Maximum: 50	The number of concurrently connected Mobile Security users has reached 90 percent of the capacity supported by the Mobile Security license. The log message specifies the supported maximum number of concurrent Mobile Security users.	The number of connected Mobile Security users has reached 90 percent of the licensed capacity. Maximum: %d	—