WatchGuard

Fireware v12.9

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*.

Search the Log Catalog

All log messages in the *Log Catalog* are first organized by the functional area and then by the log type. To quickly find a specific log message in the *Log Catalog*, you can search the *Log Catalog* for the specific details included in a log message.

When you search for a log message, you can specify any of the details included in the log message that you see in Traffic Monitor or Log Manager. The more specific your search criteria, the fewer search results are returned from your search query. To find a specific text phrase, make sure to include the phrase in quotation marks. If you search for the message ID number, make sure to remove the hyphen when you type the message ID number.

For example, to search the *Log Catalog* for the message ID number that appears in a log message that you see in Traffic Monitor:

1. In Traffic Monitor, find the `msg_id` value in the log message.
2. Open the *Fireware Log Catalog* in Adobe Acrobat.
3. Press **CTRL + F**.
4. In the **Find** text box, type the *msg_id* value from your log message, without the hyphen.
   For example, to find the *1C02-00CD* error log message for the FTP-proxy, type "`1C0200CD`".
5. Press **Enter**.
   The first instance of the message ID you searched for is highlighted.

When you search for unique text such as a message ID number, the search results will include only a few items. If your search includes text that is more generic (for example, HTTPS), the search results will include many entries.

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. 500 SYN packets dropped since last alarm.	IPv4 SYN flood attack was detected.	SYN flood attack against %s from %s detected. %llu SYN packets dropped since last alarm.	SYN flood attack against ${dst} from ${src} detected. ${gap} SYN packets dropped since last alarm.
30000154	INFO	Firewall / Packet Filter	IPv4 ICMP flood attack	ICMP flood attack against 10.0.1.51 from 216.3.21.4 detected. 500 ICMP flood packets dropped since last alarm.	IPv4 ICMP flood attack was detected.	ICMP flood attack against %s from %s detected. %llu ICMP flood packets dropped since last alarm.	ICMP flood attack against ${dst} from ${src} detected. ${gap} ICMP flood packets dropped since last alarm.
30000155	INFO	Firewall / Packet Filter	IPv4 UDP flood attack	UDP flood attack against 32.21.56.8 from 12.34.23.67 detected. 500 UDP flood packets dropped since last alarm.	IPv4 UDP flood attack was detected.	UDP flood attack against %s from %s detected. %llu UDP flood packets dropped since last alarm.	UDP flood attack against ${dst} from ${src} detected. ${gap} UDP flood packets dropped since last alarm.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
30000156	INFO	Firewall / Packet Filter	IPv4 IPSEC flood attack	IPSEC flood attack against 32.21.56.8 from 12.34.23.67 detected. 500 IPSEC flood packets dropped since last alarm.	IPv4 IPSEC flood attack was detected.	IPSEC flood attack against %s from %s detected. %llu IPSEC flood packets dropped since last alarm.	IPSEC flood attack against $dst from $src detected. $gap IPSEC flood packets dropped since last alarm.
30000157	INFO	Firewall / Packet Filter	IPv4 IKE flood attack	IKE flood attack against 32.21.56.8 from 12.34.23.67 detected. 500 IKE flood packets dropped since last alarm.	IPv4 IKE flood attack was detected	IKE flood attack against %s from %s detected. %llu IKE flood packets dropped since last alarm.	IKE flood attack against ${dst} from ${src} detected. ${gap} IKE flood packets dropped since last alarm.
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. 100 SYN packets dropped since last alarm.	IPv6 SYN flood attack was detected.	SYN flood attack against %s from %s detected. %llu SYN packets dropped since last alarm.	SYN flood attack against ${dst} from ${src} detected. ${gap} SYN packets dropped since last alarm.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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. 100 ICMP packets dropped since last alarm.	IPv6 ICMP flood attack was detected.	ICMP flood attack against %s from %s detected. %llu ICMP packets dropped since last alarm.	ICMP flood attack against ${dst} from ${src} detected. ${gap} ICMP packets dropped since last alarm.
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. 100 UDP packets dropped since last alarm.	IPv6 UDP flood attack was detected.	UDP flood attack against %s from %s detected. %llu UDP packets dropped since last alarm.	UDP flood attack against ${dst} from ${src} detected. ${gap} UDP packets dropped since last alarm.
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. 100 IPSEC packets dropped since last alarm.	IPv6 IPSEC flood attack was detected.	IPSEC flood attack against %s from %s detected. %llu IPSEC packets dropped since last alarm.	IPSEC flood attack against ${dst} from ${src} detected. ${gap} IPSEC packets dropped since last alarm.
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. 100 IKE packets dropped since last alarm.	IPv6 IKE flood attack was detected.	IKE flood attack against %s from %s detected. %llu IKE packets dropped since last alarm.	IKE flood attack against ${dst} from ${src} detected. ${gap} IKE packets dropped since last alarm.
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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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 ${dst}.
30000170	INFO	Firewall / Packet Filter	Connection table high water mark	The total number of current sessions (1024) has reached the high water mark (1024).	The total number of current sessions reached the high water mark (80%) of the maximum connection table.	The total number of current sessions (%u) has reached the high water mark (%d).	The total number of current sessions (${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
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.
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	–
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	Verify ARP entry for host at %hu.%hu.%hu.%hu	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					a given host.		
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	–
30000007	INFO	Firewall / Packet Filter	DNS forwarding deferred	Deferred DNS forwarding until valid DNS server IP address is dynamically learned	DNS server IP address is not yet known, device will enable DNS when a DNS server IP address is detected	Deferred DNS forwarding until valid DNS server IP address is dynamically learned	–
30000027	INFO	Firewall /	Firewall is	Firewall is starting up	–	Firewall is starting up	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		Packet Filter	starting up				
30000028	INFO	Firewall / Packet Filter	Firewall is shutting down	Firewall is shutting down	–	Firewall is shutting down	–
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	–
30000065	INFO	Firewall / Packet Filter	Quota amount used by the specified user	User James@Firebox-DB used 21 MB of the bandwidth quota (100 MB) and used 1 minute of the time quota (3 minutes).	–	User %s used %s	User {user} used {quota info}

Event

Firewall log messages of the *Event* log type.

ID	Level	Area	Name	Log Message 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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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 ${feature name} feature
3000012C	ERROR	Firewall / Packet Filter	ARP spoofing attack	ARP spoofing attack detected, ip=192.168.111.10, mac=00:50:da:c7:90:5d, interface=5	Detected an ARP spoofing attack. The log message specifies the source IP address, MAC address, and incoming interface of the ARP packet.	ARP spoofing attack detected, ip=%u.%u.%u.%u, mac=%02x:%02x:%02x:%02x:%02x:%02x, interface=%u	ARP spoofing attack detected, ip=${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.	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
30000174	INFO	Firewall / Packet Filter	SD-WAN failover/failback	SD-WAN action test failed over from interface Bovpn-Vif to Optional-1.	SD-WAN action failed over or failed back from one interface to another one.	SD-WAN action %name %update from interface %prev to %new.	SD-WAN action ${name} ${update} from interface ${prev} to ${new}
30011001	INFO	Firewall / Packet Filter	Temporarily blocking host	Temporarily blocking host 198.13.111.226 (reason = autoblock by policy)	The host is blocked temporarily.	Temporarily blocking host %s (reason = %s)	Temporarily blocking host ${IP} (reason = ${reason string})
30011002	INFO	Firewall / Packet Filter	Unblock host	The Temporary Blocked Sites list is full (capacity=1000). The oldest entry 10.0.5.96 was removed.	The host was unblocked because the Temporary Blocked Sites list is full.	The Temporary Blocked Sites list is full (capacity=%d). The oldest entry %s was removed.	The Temporary Blocked Sites list is full (capacity=${limit}). The oldest entry ${IP} was removed.

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" sig_vers="18.123" 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\" sig_vers=\"%s\" 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=${app_ctl_disp} sig_vers=${sig_vers} msg=${msg} [${route_type}] ${policy_name}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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" sig_ vers="18.124" 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\" sig_vers=\"%s\" 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=${severity} sig_vers=${sig_ vers} 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_bytes=\"%d\" rcvd_bytes=\"%d\" (%s)	${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=${duration} sent_ bytes=${sent_bytes} rcvd_ bytes=${rcvd_bytes} ${policy_name}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	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	–
DIAG	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	–
DIAG	09000006	INFO	Networking / PPPoE	Initiate PPPoE automatic restart	Initiating PPPoE automatic restart	PPPoE instance will restart automatically.	Initiating PPPoE automatic restart	–
DIAG	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	–
DIAG	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	31000004	INFO	Networking / Network Management	Initiate gratuitous ARP	Initiating GARP for all interfaces	Initiate gratuitous ARP for all the interfaces.	Initiating GARP for all interfaces	–
DIAG	3100000F	INFO	Networking / Network Management	Add bridge interface	Adding bridge tbr0	Add bridge interface in bridge mode.	Adding bridge %s	Adding bridge ${dev_ name}
DIAG	31000030	INFO	Networking / Network Management	Send interface logical link status event	[eth0] Sending interface status event, logical=up link=up ip=10.0.0.1 mask=255.255.255.0	Interface status event is sent for logical link status change.	[%s] Sending interface status event%s, logical=%s link=%s ip=%u.%u.%u.%u mask=%u.%u.%u.%u	[${dev_name}] Sending interface status event, logical=${logical} link=${link} ip=${ip} mask=${mask}
DIAG	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 ${link}
DIAG	31000034	INFO	Networking / Network Management	A change was made to the IP address of the external interface	[eth0 (External)] External Interface set IP address	Handle IP address for the specified external interface.	[%s (%s)] External Interface %s IP address	[${dev_name} (${if_ name})] External Interface ${operation} IP address
DIAG	31000035	ERROR	Networking / Network Management	Ignore unknown address operation	[eth0 (External)] Ignoring unknown address operation sss	Ignore unknown address operation on the specified interface.	[%s (%s)] Ignoring unknown address operation %s	[${dev_name} (${if_ name})] Ignoring unknown address operation ${operation}
DIAG	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	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}
DIAG	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}
DIAG	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}
DIAG	3100004F	INFO	Networking / Network Management	Fix up multipath gateways	[ECMP] Fix up 2 multipath gateway successfully	Fix up multipath gateways of the specified number successfully.	[ECMP] Fix up %d multipath gateway successfully	[ECMP] Fix up ${num} multipath gateway successfully
DIAG	31000050	INFO	Networking / Network Management	Starting wireless AP	Starting wireless AP ath1	Starting specified wireless AP.	Starting wireless AP %s	–
DIAG	31000051	INFO	Networking / Network Management	Stopping wireless AP	Stopping wireless AP ath1	Stopping the specified wireless Access Point.	Stopping wireless AP %s	–
DIAG	31000057	INFO	Networking / Network Management	Start processing configuration	Starts processing a configuration setting	Started to process configuration settings.	Starts processing a configuration setting	–
DIAG	31000058	INFO	Networking /	Update bridge mode	Updating global bridge mode	Update global	Updating global bridge	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			Network Management	settings	setting	bridge mode settings.	mode setting	
DIAG	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	–
DIAG	3100005A	INFO	Networking / Network Management	Update wireless settings	Updating wireless setting	Update wireless settings	Updating wireless setting	–
DIAG	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
DIAG	3100005C	INFO	Networking / Network Management	Update route settings	Updating route setting	Update route settings.	Updating route setting	–
DIAG	3100005D	INFO	Networking / Network Management	Update 1to1 NAT settings	Updating 1to1 NAT setting	Update 1-to-1 NAT settings.	Updating 1to1 NAT setting	–
DIAG	3100005E	INFO	Networking / Network Management	Update DNS settings	Updating DNS setting	Update DNS settings.	Updating DNS setting	–
DIAG	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	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.	
DIAG	31130001	ERROR	Networking / Network Management	Capture stopped	Capture stopped, insufficient space	Capture stopped due to the specified reason.	Capture stopped, %s	Capture stopped, ${reason}
DIAG	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	–
DIAG	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})
DIAG	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	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}
DIAG	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}
DIAG	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}
DIAG	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}
DIAG	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}
DIAG	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	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}
DIAG	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} / ${server_ip}
DIAG	5A00000B	ERROR	Networking / Dynamic DNS	Invalid response from server	Invalid response from server (-2)	The dynamic DNS server returned an invalid response code. The log message specifies that code.	Invalid response from server (%d)	Invalid response from server (${ret_code})
DIAG	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	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}
DIAG	56000001	INFO	Networking / Dynamic Routing	Update IPv4 Dynamic Routes	Sync add an IPv4 dynamic route (10.0.1.2/24 gw 10.0.1.254 ifindex 1 metric 10)	Updated an IPv4 dynamic route. The log message specifies the route that is changed.	%s %s an IPv4 dynamic route (%s/%d gw %s ifindex %d metric %d)	${event} ${action} an IPv4 dynamic route (${ip}/${mask} gw ${gw} ifindex ${ifindex} metric ${metric}
DIAG	56010002	ERROR	Networking / Dynamic Routing	Failed to retrieve license	Failed to retrieve active license features	Failed to retrieve license features for dynamic routing.	Failed to retrieve active license features	–
DIAG	56010003	ERROR	Networking / Dynamic Routing	Failed to parse license	Failed to parse the active license features	Failed to parse license features for dynamic routing.	Failed to parse the active license features	–
DIAG	56010004	ERROR	Networking / Dynamic Routing	Not able to get license	Could not get license for dynamic routing features	Not able to get license for dynamic routing features.	Could not get license for dynamic routing features	–
DIAG	56020002	DEBUG	Networking / Dynamic Routing	Received cluster event	Received cluster ready event	Received cluster ready event.	Received cluster ready event	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	56020003	DEBUG	Networking / Dynamic Routing	Received cluster event	Received cluster role change event	Received cluster role change event.	Received cluster role change event	–
DIAG	56020004	DEBUG	Networking / Dynamic Routing	Received license event	Received License Update event	Received a license update event.	Received License Update event	–
DIAG	56020005	ERROR	Networking / Dynamic Routing	RCS unresponsive	RCS(10.10.10.10) is unresponsive, and is considered stopped	The RCS at the specified IP address has become unresponsive	RCS(%s) is unresponsive, and is considered stopped	RCS(${ip}) is unresponsive, and is considered stopped
DIAG	56020006	INFO	Networking / Dynamic Routing	Not able to forward request to RCS	Could not forward request to RCS, not connected	Not able to forward request to RCS due to no connection.	Could not forward request to RCS, not connected	–
DIAG	56030001	ERROR	Networking / Dynamic Routing	–	Configuration error detected in ripd.conf, line 12: 'network 192.168.53.0/24 area 0'	An error was detected in the configuration. The log message specifies the line number of the error.	Configuration error detected in %s, line %d: '%s'	Configuration error detected in ${config}, line ${lineno}: '${line}'
DIAG	56040001	ERROR	Networking / Dynamic Routing	Not able to connect to RCS	Could not connect to RCS, 10.0.1.10	Not able to connect to RCS with the specified IP address.	Could not connect to RCS, %s	Could not connect to RCS, ${ip}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	56040002	ERROR	Networking / Dynamic Routing	Connection to RCS closed	Connection to RCS was closed	Connection to RCS closed.	Connection to RCS was closed	–

Event

Networking log messages of the *Event* log type.

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	56000002	INFO	Networking / Dynamic Routing	Cluster role failed over to backup	Failed over from master to backup	Cluster role failed over from master to backup	Failed over from master to backup	–
EVENT	56000003	INFO	Networking / Dynamic Routing	Cluster role failed over to master	Failed over from backup to master	Cluster role failed over from backup to master	Failed over from backup to master	–
EVENT	56010001	WARN	Networking / Dynamic Routing	No valid feature key	Invalid or missing feature key for dynamic routing protocol OSPF	No valid feature key for the specified dynamic routing protocol.	Invalid or missing feature key for dynamic routing protocol %s	–
EVENT	56010005	INFO	Networking / Dynamic Routing	License status	License for dynamic routing protocol BGP is valid	Specifies the license status for a dynamic routing protocol.	License for dynamic routing protocol %s is %s	License for dynamic routing protocol ${proto} is ${status}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	09000004	ERROR	Networking / PPPoE	Authentication failure	PPPoE authentication failed	The Firebox or XTM device failed to authenticate for PPPoE.	PPPoE authentication failed	–
EVENT	09000005	ERROR	Networking / PPPoE	PPPoE stopped	PPPoE stopped unexpectedly (unknown error)	PPPoE stopped unexpectedly due to an unknown error.	PPPoE stopped unexpectedly (unknown error)	–
EVENT	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 ${static_ip}
EVENT	09000009	INFO	Networking / PPPoE	Session established	[eth0 (External)] PPPoE session[11] is established, acquired IP address 192.168.3.48, peer 192.168.3.254	The specified interface established a PPPoE session. The log message also specifies the session ID, acquired IP address, and peer IP address.	[%s (%s)] PPPoE session[%d] is established, acquired IP address %s, peer %s	[${physical_name} (${ifname})] PPPoE session[${session_id}] is established, acquired IP address ${ipaddr}, peer ${peer_addr}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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.	–
EVENT	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	–
EVENT	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	–
EVENT	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	–
EVENT	16000004	WARN	Networking / DHCP Server	Overlapping subnets	Subnet 100.64.1.0/24 for address pool on interface vlan10 overlaps subnet 100.64.0.0/16 on interface eth1. Edit the configuration so that DHCP server functions properly	Subnets for address pools overlap	Subnet %s for address pool on interface %s overlaps subnet %s on interface %s. Edit the configuration so that DHCP server functions properly	

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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
EVENT	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
EVENT	3100000B	INFO	Networking / Network Management	Multi-WAN interface activated.	[eth1 (Trusted)] Interface is activated as link state becomes UP.	Interface is activated as link state becomes UP. The log message specifies the interface.	[%s (%s)] Interface is activated as link state becomes UP.	–
EVENT	3100000D	WARN	Networking / Network Management	Multi-WAN interface deactivated	[eth1 (Trusted)] Interface is deactivated as link state becomes DOWN.	Interface is deactivated as link state becomes DOWN. The log message specifies the interface.	[%s (%s)] Interface is deactivated as link state becomes DOWN.	–
EVENT	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	–
EVENT	31000029	ERROR	Networking / Network Management	Failed to add interface IP address	[eth1 (Trusted)] Failed to add address 198.51.100.0	Failed to add the specified IP address to the specified interface.	[%s (%s)] Failed to %s address %s	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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
EVENT	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	–
EVENT	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
EVENT	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	–
EVENT	3100003B	WARN	Networking / Network Management	Cluster setting changed to disabled	Cluster setting changed from enabled to disabled	The cluster setting was changed from	Cluster setting changed from enabled to	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						enabled to disabled.	disabled	
EVENT	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.	–
EVENT	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.	–
EVENT	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
EVENT	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
EVENT	31000052	INFO	Networking / Network Management	Starting wireless AP service	Starting wireless AP service	Starting wireless AP service.	Starting wireless AP service	–
EVENT	31000054	INFO	Networking /	Detect rogue wireless AP	Starting the scan for	Starting rogue	Starting the scan	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			Network Management		rogue wireless AP detection	wireless AP detection scan.	for rogue wireless AP detection	
EVENT	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	–
EVENT	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	–
EVENT	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.	–
EVENT	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.	–
EVENT	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
EVENT	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

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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 ${new_ip}
EVENT	31000072	INFO	Networking / Network Management	No change for PPPoE IP address during cluster failover	[eth0 (External)] PPPoE IP address 192.168.1.22 did not change during cluster failover	PPPoE IP address did not change during cluster failover.	[%s (%s)] PPPoE IP address %u.%u.%u.%u did not change during cluster failover	–
EVENT	31000073	INFO	Networking / Network Management	DHCP IP address change during cluster failover	[eth0 (External)] DHCP IP address changed during cluster failover, from 192.168.1.22 to 192.168.1.23	The cluster completed a failover. During the failover, the DHCP IP address changed.	[%s (%s)] DHCP IP address changed during cluster failover, from %s to %s	[${dev_name} (${if_name})] DHCP IP address changes during cluster failover, from ${pre_ip} to ${new_ip}
EVENT	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	–
EVENT	45000003	INFO	Networking / Modem	Modem disconnected	modem0 disconnected	Specified modem is disconnected.	%s disconnected	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	45000004	ERROR	Networking / Modem	Modem authentication failed	Modem authentication failed, check your modem configuration	Modem authentication failed.	Modem authentication failed, check your modem configuration	–
EVENT	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	–
EVENT	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}
EVENT	49000003	ERROR	Networking / Link Monitoring	Probe failure	[Link Monitor] Interface External 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] Interface %s failed because a probe to the target host failed	–
EVENT	49000004	WARN	Networking / SD-WAN	Status change from performance metric	[SD-WAN] Interface External is now disqualified because one or more metrics (loss rate) exceed the value specified in the SD-WAN action test	Specified interface marked as Qualified / Disqualified when performance metric no longer	[SD-WAN] Interface %s is now qualified / disqualified because one or more metrics (%s, %s, %s) no	

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						exceeds / exceeds the value specified in the SD-WAN action	longer exceed / exceed the value specified in the SD-WAN action %s	
EVENT	68000001	INFO	Networking / Discovery	Network scan completed	On demand scan completed	Specified type of scan completed	%s scan completed	${scan_type} scan completed
EVENT	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
EVENT	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

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 142.

Event

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

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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	–
EVENT	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'	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	0F010016	INFO	Proxy / Connection Framework Manager	Safe APT Analysis result	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'	When the APT Blocker server returns a clean analysis result, this event log contains information about the scanned file.	APT safe result from file submission. Details='%s'	–
EVENT	1B0400CE	ERROR	Proxy / SMTP	Ruleset lookup failed	Ruleset 'envelope/greeting' lookup failed	SMTP proxy -- Failed to check the specified ruleset	Ruleset '%s' lookup failed	–
EVENT	1C0200CD	ERROR	Proxy / FTP	Ruleset lookup failed	Cannot get the rule from ruleset 'request/download'	FTP proxy -- Failed to check the specified ruleset	Cannot get the rule from ruleset '%s'	–
EVENT	1F000001	ERROR	Security Services / Gateway Anti-Virus	Process failed to start	Cannot start ScanD	ScanD -- Process failed to start	Cannot start ScanD	–
EVENT	1F010015	INFO	Security Services / Gateway Anti-Virus	Ready for service	ScanD ready	ScanD -- Ready for service	ScanD ready	–
EVENT	23000001	ERROR	Security Services / spamBlocker	Failed to start	Cannot start spamD	spamD -- Failed to start	Cannot start spamD	–
EVENT	23000002	INFO	Security Services / spamBlocker	Ready for service	spamD ready	spamD -- Ready for service	spamD ready	–
EVENT	2E000005	ERROR	Security Services	Process exiting	SIGD shutting down	SIGD -- Process	SIGD shutting	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			/ Signature Update			exiting	down	
EVENT	2E000006	ERROR	Security Services / Signature Update	Process crashed	SIGD crashed	SIGD -- Process crashed	SIGD crashed	–
EVENT	2E010017	WARN	Security Services / Signature Update	License failed to load	Cannot load the license	SIGD -- License failed to load	Cannot load the license	–
EVENT	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'	–
EVENT	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	–
EVENT	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	–
EVENT	2E01001B	ERROR	Security Services / Signature Update	Signature update process crashed	SIGD Worker crashed	SIGD -- Signature update process crashed	SIGD Worker crashed	–
EVENT	2E020065	INFO	Security Services / Signature Update	Signature update process started	Scheduled DLP update started	SIGD -- Signature update process started	%s %s update started	–
EVENT	2E020066	INFO	Security Services	Signature update	Scheduled DLP update for version (4.94) completed	SIGD -- Signature	%s %s update	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			/ Signature Update	process completed		update process completed	for version (%s) completed	
EVENT	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)	–
EVENT	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)	–

Traffic

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

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0001	INFO	Proxy / HTTP	Session timeout with server idle	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)	The HTTP session has timed out because no traffic has been received from the server for the specified amount of time. (Default: 10 minutes)	HTTP server response timeout	–
TRAFFIC	1AFF0002	INFO	Proxy / HTTP	Session timeout with client idle	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)	The HTTP session has timed out because no traffic has been received from the client for the specified amount of time. (Default: 10 minutes)	HTTP client request timeout	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0003	INFO	Proxy / HTTP	Session timeout with close complete command timeout	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)	The Close HTTP Session command timed out because no response to the FIN packet was received within the response time limit (3 minutes).	HTTP close complete timeout	–
TRAFFIC	1AFF0004	INFO	Proxy / HTTP	Oversize Start-Line	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)	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.	HTTP Start-Line oversize	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0005	INFO	Proxy / HTTP	Invalid Request-Line format	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)	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.	HTTP Invalid Request-Line Format	–
TRAFFIC	1AFF0006	INFO	Proxy / HTTP	Invalid Status-Line format	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)	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.	HTTP invalid Status-Line format	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0007	INFO	Proxy / HTTP	Header line oversize	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)	A single client request or server response line is longer than the configured maximum line length. The default maximum length is 4,096 bytes.	HTTP header line oversize	–
TRAFFIC	1AFF0008	INFO	Proxy / HTTP	Header block oversize	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)	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.	HTTP header block oversize	–
TRAFFIC	1AFF0009	INFO	Proxy / HTTP	header block parse error	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)	The HTTP proxy cannot process the header line because the format is incorrect. The required format is [Name]: [Value].	HTTP header block parse error	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF000A	INFO	Proxy / HTTP	Request missing URL path	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"	The HTTP proxy cannot complete the URL because the host or URI value is missing. The HTTP request is denied.	HTTP request URL path missing	–
TRAFFIC	1AFF000B	INFO	Proxy / HTTP	Request URL match	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)	The requested URL matched a configured URL path in the HTTP proxy. By default, all URL paths are allowed.	HTTP request URL match	–
TRAFFIC	1AFF000C	INFO	Proxy / HTTP	Chunk size line oversize	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)	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.	HTTP chunk size line oversize	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF000D	INFO	Proxy / HTTP	Chunk size line invalid	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)	The HTTP chunk size line has an invalid hexadecimal value. The invalid line is specified in the log message.	HTTP chunk size invalid	–
TRAFFIC	1AFF000E	INFO	Proxy / HTTP	Chunk no CRLF tail	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)	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.	HTTP chunk CRLF tail missing	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF000F	INFO	Proxy / HTTP	Footer line oversize	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)	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.	HTTP footer line oversize	–
TRAFFIC	1AFF0010	INFO	Proxy / HTTP	Footer block oversize	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)	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.	HTTP footer block oversize	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0011	INFO	Proxy / HTTP	Footer block parse error	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)	The HTTP footer includes an additional header field with syntax that violates the header format restrictions.	HTTP footer block parse error	–
TRAFFIC	1AFF0012	INFO	Proxy / HTTP	Body content type match	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)	The HTTP content either matches a configured Body Content Type or no Body Content Type is defined (only the default rule is in use).	HTTP Body Content Type match	–
TRAFFIC	1AFF0013	INFO	Proxy / HTTP	Header content malformed	Allow 1-Trusted 0-External tcp 10.0.1.2 192.168.53.92 41048 80 msg="ProxyStrip: HTTP header malformed" proxy_act="393296" header="WWW-Authenticate: \x0d\x0a"	The HTTP header line does not follow the correct syntax for a client request or server response header. The log message contains the header line with the syntax error.	HTTP header malformed	–
TRAFFIC	1AFF0016	INFO	Proxy / HTTP	Header Transfer-	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 40719 80 msg="ProxyAllow: HTTP header Transfer-Encoding match" proxy_	The Transfer-	HTTP header transfer	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				Encoding match	act="HTTP-Client.2" rule_name="chunked" encoding="chunked" (HTTP-proxy-00)	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.	encoding match	
TRAFFIC	1AFF0018	INFO	Proxy / HTTP	Header content type match	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)	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.	HTTP header Content Type match	–
TRAFFIC	1AFF0019	INFO	Proxy / HTTP	Request version match	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)	The HTTP version specified in the HTTP request line matches a configured rule, or the default rule of no match.	HTTP request version match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						The log specifies the matched rule name and the request line.		
TRAFFIC	1AFF001A	INFO	Proxy / HTTP	Request method match	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)	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.	HTTP request method match	–
TRAFFIC	1AFF001B	INFO	Proxy / HTTP	Header match	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)	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.	HTTP header match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF001C	INFO	Proxy / HTTP	Header cookie domain match	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)	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.	HTTP header cookie domain match	–
TRAFFIC	1AFF001D	INFO	Proxy / HTTP	Request host missing	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)	The HTTP request header is missing the host value.	HTTP request host missing	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF001E	INFO	Proxy / HTTP	Header authentication scheme match	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)	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.	HTTP header auth scheme match	–
TRAFFIC	1AFF001F	INFO	Proxy / HTTP	Request method not supported	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)	The HTTP request method does not match a configured rule. The log message specifies the method in use.	HTTP request method unsupported	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0020	INFO	Proxy / HTTP	Request port mismatch	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)	Relative-URI is in use and the port specified in the HTTP request host header does not match the port used for the connection.	HTTP request port mismatch	–
TRAFFIC	1AFF0021	INFO	Proxy / HTTP	Request categories	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)	The HTTP request matched a WebBlocker category. The log message specifies the action taken by the proxy, the URL, and the category matched.	HTTP Request categories	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0022	INFO	Proxy / HTTP	Service unavailable	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)	WebBlocker categorization failed because the configured WebBlocker server is not available. The log message specifies the profile name and a more detailed error message.	HTTP service unavailable	–
TRAFFIC	1AFF0023	INFO	Proxy / HTTP	Request URL path oversize	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-lfADpBbs0T0xmHzDv3tYNK4R4eAMZSmuX1YAUWVQlL6kSI-xpS-vSmdvbuQg/extension_0_1_0_12919.crx" (HTTP-proxy-00)	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.	HTTP request URL path oversize	–
TRAFFIC	1AFF0024	INFO	Proxy / HTTP	Request	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)	A detailed summary of the last HTTP proxy transaction.	HTTP request	–
TRAFFIC	1AFF0025	INFO	Proxy / HTTP	Header IPS rule match	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" sig_vers="18.001"	Intrusion Prevention Service (IPS)	HTTP header IPS match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					host="intext.nav-links.com" path="/util/intexteval.pl?action=startup" (HTTP-proxy-00)	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.		

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0026	INFO	Proxy / HTTP	Body IPS rule match	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" sig_vers="18.001" host="secure.eicar.org" path="/eicar.com.txt" src_ user="testuser@test.net" (HTTPS-proxy-00)	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.	HTTP body IPS match	–
TRAFFIC	1AFF0028	INFO	Proxy / HTTP	GAV Virus found	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)	Gateway AntiVirus (GAV) detected a virus or malware. The log message specifies the virus name, destination host name, and URI path.	HTTP Virus found	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0029	INFO	Proxy / HTTP	GAV scan error	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)	Gateway AntiVirus (GAV) failed to scan because of an error. The log message specifies the error message, the destination host name, and URI path.	HTTP AV scanning error	–
TRAFFIC	1AFF002B	INFO	Proxy / HTTP	Trusted host	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)	The destination host name matches a proxy exception configured in the HTTP proxy.	HTTP Trusted host	–
TRAFFIC	1AFF002C	INFO	Proxy / HTTP	Bad reputation	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)	The HTTP proxy blocked access to the destination address because of a bad reputation score for the URL.	HTTP bad reputation	–
TRAFFIC	1AFF002D	INFO	Proxy / HTTP	Good reputation	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)	The HTTP proxy did not complete a Gateway AntiVirus (GAV) scan for traffic to	HTTP good reputation	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						the destination address because the URL received a good reputation score.		
TRAFFIC	1AFF002E	INFO	Proxy / HTTP	Application match	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" sig_vers="18.001" src_user="test@test.net" (HTTP-00)	Application Control identified the application type from the HTTP client request or server response stream.	HTTP App match	–
TRAFFIC	1AFF002F	INFO	Proxy / HTTP	DLP violation found	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)	Data Loss Prevention (DLP) detected a violation of DLP rules. The log message only includes information about the first rule matched.	HTTP DLP violation found	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0030	INFO	Proxy / HTTP	DLP cannot perform scan	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)	Data Loss Prevention (DLP) failed to scan the traffic because of the error specified in the log message.	HTTP cannot perform DLP Scan	–
TRAFFIC	1AFF0031	INFO	Proxy / HTTP	DLP object unscannable	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)	Data Loss Prevention (DLP) cannot extract data from an object because it is encrypted.	HTTP DLP object unscannable	–
TRAFFIC	1AFF0032	INFO	Proxy / HTTP	HTTP object too large	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_sensor="DLPSensor.1" error="DLP scan limit exceeded" (HTTP-proxy-00)	Data Loss Prevention (DLP) cannot scan the object because it is larger than the configured limit. The default value varies by device type and ranges between 1 and 5 MB.	HTTP DLP object too large	–
TRAFFIC	1AFF0033	INFO	Proxy / HTTP	Range header	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)	This is the configured action (allow or	HTTP Range header	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						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.		
TRAFFIC	1AFF0034	INFO	Proxy / HTTP	APT threat detected	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"	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.	HTTP APT detected	–
TRAFFIC	1AFF0036	INFO	Proxy / HTTP	File submitted to 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)	File submitted to APT analysis server for deep threat analysis. The analysis	HTTP File submitted to APT analysis server	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						result will be notified when the analysis result is fetched from APT analysis server.		
TRAFFIC	1AFF0037	INFO	Proxy / HTTP	Connect tunnel port match	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)	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.	HTTP connect tunnel port match	–
TRAFFIC	1AFF0038	INFO	Proxy / HTTP	Webproxy redirect	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)	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.	HTTP webproxy redirect	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0039	INFO	Proxy / HTTP	File reported safe from APT hash check	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)	APT hash check did not report a threat from the object	HTTP File reported safe from APT hash check	–
TRAFFIC	1AFF003A	INFO	Proxy / HTTP	Content redirect	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)	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.	HTTP Content redirect	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF003B	INFO	Proxy / HTTP	Request Content match	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_src="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)	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.	HTTP Request content match	–
TRAFFIC	1AFF0040	INFO	Proxy / HTTP	DNSWatch blackholed domain	Allow 1-Trusted 0-External tcp 10.0.1.2 54.173.101.99 58477 80 msg="ProxyAllow: HTTP DNSWatch blackholed domain" proxy_act="HTTP-Client.Standard.1" host="www.wine.com" path="/" geo_dst="USA" (HTTP-proxy-00)	DNSWatch DNS server returned the blackhole server IP address for the name resolution for requested domain. HTTP proxy acknowledge the blackhole server IP address and generates the log for the client request	HTTP DNSWatch blackholed domain	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1AFF0041	INFO	Proxy / HTTP	DNSWatch content filtered domain	Deny 1-Trusted 0-External tcp 10.0.1.2 54.173.101.99 58477 80 msg="ProxyAllow: HTTP DNSWatch content filtered domain" proxy_act="HTTP-Client.Standard.1" host="www.wine.com" path="/" geo_dst="USA" (HTTP-proxy-00)	DNSWatch DNS server returned the filterhole server IP address for the name resolution for requested domain from the content filtered domain configuration. HTTP proxy acknowledge the filterhole server IP address and generates the log for the client request	HTTP DNSWatch content filtered domain	–
TRAFFIC	1BFF0000	INFO	Proxy / SMTP	Greeting	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)	The host name in the SMTP proxy HELO or EHLO command matched one of the Greeting Rules, or the default rule of no match.	SMTP greeting	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF0001	INFO	Proxy / SMTP	ESMTP option	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39371 25 msg="ProxyStrip: SMTP ESMTP option" proxy_act="SMTP-Outgoing.1" keyword="VRFY" (SMTP-proxy-00)	The EHLO response from the SMTP server includes an ESMTP option that is disabled or unknown.	SMTP ESMTP option	–
TRAFFIC	1BFF0002	INFO	Proxy / SMTP	Authentication (AUTH)	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)	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.	SMTP AUTH	–
TRAFFIC	1BFF0003	INFO	Proxy / SMTP	Header	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)	A MIME header matched a configured rule, or the default rule of no match.	SMTP header	–
TRAFFIC	1BFF0004	INFO	Proxy /	From address	Deny 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 39383 25	The sender	SMTP From	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			SMTP		msg="ProxyDeny: SMTP From address" proxy_act="SMTP-Outgoing.1" rule_name="jsmith@*.com->ex-employee" address="dbonn@testnet.com" (SMTP-proxy-00)	address matched a rule specified in the Mail From rules.	address	
TRAFFIC	1BFF0005	INFO	Proxy / SMTP	To address	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)	The recipient address matched a rule specified in the Rcpt To rules.	SMTP To address	–
TRAFFIC	1BFF0006	INFO	Proxy / SMTP	Content type	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)	Some of the message content matched a content filter rule.	SMTP content type	–
TRAFFIC	1BFF0007	INFO	Proxy / SMTP	Filename	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)	An email attachment matched a file name rule, or the attachment is uuencoded and the SMTP proxy allows uuencoded attachments.	SMTP filename	–
TRAFFIC	1BFF000A	INFO	Proxy / SMTP	Timeout	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)	The SMTP connection was idle for longer than the configured idle timeout limit.	SMTP timeout	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						The default is 10 minutes.		
TRAFFIC	1BFF000C	INFO	Proxy / SMTP	GAV Virus found	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)	Gateway AntiVirus (GAV) detected a virus or malware in an email attachment.	SMTP Virus found	–
TRAFFIC	1BFF000E	INFO	Proxy / SMTP	GAV cannot perform scan	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)	Gateway AntiVirus (GAV) could not complete the scan because of the error that is specified in the log message.	SMTP cannot perform Gateway AV scan	–
TRAFFIC	1BFF000F	INFO	Proxy / SMTP	Request	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)	This SMTP audit log specifies the bytes sent, bytes received, the sender and recipient addresses, and the sender and recipient TLS cipher.	SMTP request	–
TRAFFIC	1BFF0010	INFO	Proxy / SMTP	Message format	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-	The email message format matched a message format	SMTP message format	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					00)	rule specified in the SMTP proxy. The log message includes the error message.		
TRAFFIC	1BFF0011	INFO	Proxy / SMTP	IPS match	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" sig_vers="18.001" (SMTP-proxy-00)	Intrusion Prevention Service (IPS) detected a threat. The log message specifies the signature name and ID, threat severity, and signature category.	SMTP IPS match	–
TRAFFIC	1BFF0013	INFO	Proxy / SMTP	Too many 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" num_recipients="15" (SMTP-proxy-00)	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	SMTP too many recipients	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						proxy action and number of recipients.		
TRAFFIC	1BFF0014	INFO	Proxy / SMTP	Response size too long	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)	The SMTP server response exceeds the configured limit. The default limit is 10,000 KB. The log message specifies the size of the response.	SMTP response size too long	–
TRAFFIC	1BFF0015	INFO	Proxy / SMTP	Line too long	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)	The email message contains a line that exceeds the configured limit. The default is 1,000 bytes. The log message specifies the line length.	SMTP line length too long	–
TRAFFIC	1BFF0016	INFO	Proxy / SMTP	Message too long	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)	The SMTP message length exceeds the configured limit. The default limit is 10,000 kb.	SMTP message size too long	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF0017	INFO	Proxy / SMTP	Header too long	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)	The SMTP message contains a header that exceeds the configured Maximum Header Length. The default is 20,000 bytes.	SMTP header size too long	–
TRAFFIC	1BFF0018	INFO	Proxy / SMTP	Command	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)	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 response code.	SMTP command	–
TRAFFIC	1BFF0019	INFO	Proxy / SMTP	spamBlocker confirmed spam	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)	spamBlocker has classified the message as confirmed SPAM. The log message	SMTP Classified as confirmed SPAM	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						specifies the proxy action, the action taken, and the sender and recipient addresses.		
TRAFFIC	1BFF001A	INFO	Proxy / SMTP	spamBlocker bulk spam	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)	spamBlocker has classified the message as bulk SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	SMTP Classified as bulk mail	–
TRAFFIC	1BFF001B	INFO	Proxy / SMTP	spamBlocker suspect spam	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)	spamBlocker has classified the message as suspect SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	SMTP Classified as suspect SPAM	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF001C	INFO	Proxy / SMTP	spamBlocker not SPAM	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)	spamBlocker has classified the message as not SPAM. The log message specifies the proxy action, the action taken, and the sender and recipient addresses.	SMTP Classified as not SPAM	–
TRAFFIC	1BFF001D	INFO	Proxy / SMTP	spamBlocker classification unknown	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)	spamBlocker was unable to classify the email message because of an error. The log message specifies the sender and recipient addresses.	SMTP message classification is unknown because an error occurred while classifying	–
TRAFFIC	1BFF001E	INFO	Proxy / SMTP	spamBlocker exception matched	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)	The sender or recipient of the email message matches a spamBlocker exception specified in the SMTP proxy.	SMTP spamBlocker exception was matched	–
TRAFFIC	1BFF001F	INFO	Proxy /	Decoder error	Allow 1-Trusted 0-External tcp 10.0.55.253 100.100.100.155 36921 25	The SMTP proxy	SMTP An	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			SMTP		msg="ProxyStrip: SMTP An error was found by our decoder" proxy_act="SMTP-Outgoing.1" message="invalid b64 characters in input" (SMTP-OUT-00)	was unable to decode the email message due to the error specified in the log message.	error was found by our decoder	
TRAFFIC	1BFF0021	INFO	Proxy / SMTP	Extra pad characters in base64 encoding	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)	The SMTP proxy encountered extra pad characters when the body of the base64-encoded message was processed.	SMTP extra pad characters in base64 input	–
TRAFFIC	1BFF0022	INFO	Proxy / SMTP	Mail from address too long	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)	A sender email address exceeded the configured maximum address length. The address length is unlimited by default.	SMTP Mail From address too long	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF0023	INFO	Proxy / SMTP	Application match	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" app_beh_name="access" app_beh_id="6" sig_vers="18.001" (SMTP-proxy-00)	Application Control identified the application in the mail message that is specified in the log message.	SMTP App match	–
TRAFFIC	1BFF0024	INFO	Proxy / SMTP	DLP violation found	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)	Data Loss Prevention (DLP) detected the rule violation that is specified in the log message.	SMTP DLP violation Found	–
TRAFFIC	1BFF0025	INFO	Proxy / SMTP	DLP cannot perform scan	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)	Data Loss Prevention (DLP) is unable to scan because of the error specified in the log message.	SMTP cannot perform DLP Scan	–
TRAFFIC	1BFF0026	INFO	Proxy / SMTP	DLP cannot scan object	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)	Data Loss Prevention (DLP) is unable to extract data from an object because the object is encrypted.	SMTP DLP object unscannable	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF0027	INFO	Proxy / SMTP	DLP object too large	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)	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.	SMTP DLP object too large	–
TRAFFIC	1BFF0028	INFO	Proxy / SMTP	APT threat detected	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)	APT Blocker found the threat specified in the log message in an attached file.	SMTP APT detected	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF002A	INFO	Proxy / SMTP	File submitted to 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)	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.	SMTP File submitted to APT analysis server	–
TRAFFIC	1BFF002B	INFO	Proxy / SMTP	File reported safe from APT hash check	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)	APT hash check did not report a threat from the object	SMTP File reported safe from APT hash check	–
TRAFFIC	1BFF002C	INFO	Proxy / SMTP	Protocol invalid	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)	The SMTP proxy detected invalid TLS protocol.	SMTP invalid TLS protocol	–
TRAFFIC	1BFF002D	INFO	Proxy / SMTP	Content Inspection	Allow 1-Trusted 0-External tcp 10.0.1.2 192.168.53.143 40742 25 msg="ProxyInspect: SMTP content inspection" proxy_act="SMTP-Outgoing.Standard.1" tls_profile="TLS-Client.Standard" tls_version="TLSv1.3" content_inspection="yes" server_ssl="TLS_AES_256_GCM_SHA384" client_ssl="NONE" (SMTP-proxy-00)	The SMTP proxy content inspection action for a secure connection.	SMTP TLS content inspection	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1BFF0032	INFO	Proxy / SMTP	spamBlocker spam ID	Deny Trusted External tcp 10.0.1.2 100.100.100.10 47324 25 msg="ProxyDeny: SMTP spamBlocker spam ID" proxy_act="SMTP-Outgoing.Standard.1" wgrd_spam_id="v=2.4 cv=UcAy9IeN c=1 sm=1 tr=0 ts=61d873c5 p=MQD9vsuScg4A:10 a=deaM/syu8nPsmUxY89PwZA==:117 a=3DxCuoXD4FnOMnt2MpZ/VQ==:17 a=pl62oyiqAIg65rFOYjJB3Aoq8KE=:19 a=9cW_t1CCXrUA:10 a=HpEJnUIJZJkA:10 a=e_q4qTt1xDgA:10 a=V7XAPc_yuWIx1lMyBqUA:9" (SMTP-proxy-00)	The log message specifies the spam ID generated by spamBlocker.	SMTP spamBlocker spam ID	–
TRAFFIC	1CFF0000	INFO	Proxy / FTP	User name too long	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)	The user name exceeds the maximum length specified in the FTP proxy. The default is 64 characters.	FTP user name too long	–
TRAFFIC	1CFF0001	INFO	Proxy / FTP	Password too long	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)	The password specified for the user exceeds the maximum length configured in the FTP proxy. The default maximum length is 32 characters.	FTP user password too long	–
TRAFFIC	1CFF0002	INFO	Proxy / FTP	File or directory name too long	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)	The file or directory name exceeds the maximum length configured in the	FTP file or directory name too long	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						FTP proxy. The default maximum length is 1,024 bytes.		
TRAFFIC	1CFF0003	INFO	Proxy / FTP	Command line too long	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)	The command exceeded the maximum length configured in the FTP proxy. The default maximum length is 1,030 characters.	FTP command line too long	–
TRAFFIC	1CFF0004	INFO	Proxy / FTP	Exceeded maximum allowed login attempts	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)	The user exceeded the configured maximum number of allowed failed log in attepmts per connection. The default limit is 6.	FTP exceeded maximum permitted login attempts	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF0005	INFO	Proxy / FTP	Command match	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)	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.	FTP command match	–
TRAFFIC	1CFF0006	INFO	Proxy / FTP	Download match	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)	The file type matched a configured download rule, or the default rule of no match. The log message specifies the	FTP download match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						proxy action, action taken, and file type.		
TRAFFIC	1CFF0007	INFO	Proxy / FTP	Upload match	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)	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.	FTP upload match	–
TRAFFIC	1CFF0008	INFO	Proxy / FTP	Timeout	Deny 1-Trusted 0-External tcp 10.0.1.49 11.11.11.2 49561 21 msg="ProxyDrop: FTP timeout" proxy_act="FTP-Proxy" (FTP-proxy-00)	The connection exceeded the configured idle time value. The default is 180 seconds.	FTP timeout	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF0009	INFO	Proxy / FTP	Invalid request	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)	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.	FTP invalid request	–
TRAFFIC	1CFF000C	INFO	Proxy / FTP	Request	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)	This log message for the FTP request transaction includes the source and destination IP addresses for the initial connections.	FTP request	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF000D	INFO	Proxy / FTP	IPS match	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" sig_vers="18.001" (FTP-proxy-00)	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.	FTP IPS match	–
TRAFFIC	1CFF000E	INFO	Proxy / FTP	GAV Virus found	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)	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.	FTP Virus found	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF000F	INFO	Proxy / FTP	GAV scan error	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)	Gateway AntiVirus (GAV) failed to scan due to the error specified in the log message.	FTP AV scanning error	–
TRAFFIC	1CFF0010	INFO	Proxy / FTP	Application match	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" sig_vers="18.001" (FTP-proxy-00)	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 ID.	FTP App match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF0011	INFO	Proxy / FTP	DLP violation found	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)	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.	FTP DLP violation found	–
TRAFFIC	1CFF0012	INFO	Proxy / FTP	DLP cannot perform scan	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)	Data Loss Prevention (DLP) failed to scan because of the error specified in the log message.	FTP cannot perform DLP scan	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF0013	INFO	Proxy / FTP	DLP cannot scan object	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)	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.	FTP DLP object unscannable	–
TRAFFIC	1CFF0014	INFO	Proxy / FTP	DLP object too large	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)	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	FTP DLP object too large	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						name and error message.		
TRAFFIC	1CFF0015	INFO	Proxy / FTP	APT threat detected	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)	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.	FTP APT detected	–
TRAFFIC	1CFF0017	INFO	Proxy / FTP	File submitted to 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"	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.	FTP File submitted to APT analysis server	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1CFF0018	INFO	Proxy / FTP	File reported safe from APT hash check	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"	APT hash check did not report a threat from the object	FTP File reported safe from APT hash check	–
TRAFFIC	1CFF0019	ERROR	Proxy / FTP	FTP Bounce Attempt	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"	The user attempted an FTP bounce attack by sending a PORT command specifying the IP address of a third party instead of the user's own IP address	FTP Bounce Attempt	–
TRAFFIC	1DFF0000	INFO	Proxy / DNS	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" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The traffic was blocked because the message included an invalid number of questions.	DNS invalid number of questions	–
TRAFFIC	1DFF0001	INFO	Proxy / DNS	Query name oversized	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56702 53 msg="ProxyDeny: DNS oversized query name" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS query was blocked because the DNS query name exceeded the allowed buffer size,	DNS oversized query name	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						which varies from 0 kilobytes to 64 kilobytes.		
TRAFFIC	1DFF0002	INFO	Proxy / DNS	Query name compressed	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56703 53 msg="ProxyDeny: DNS compressed query name" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS query was blocked because the domain name was compressed.	DNS compressed query name	–
TRAFFIC	1DFF0003	INFO	Proxy / DNS	Parse error	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56704 53 msg="ProxyDeny: DNS parse error" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS request was blocked because the proxy failed to parse the domain name.	DNS Parse error	–
TRAFFIC	1DFF0004	INFO	Proxy / DNS	Not Internet 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)	The DNS query was not Internet CLASS. The log message specifies the action taken and the CLASS.	DNS Not Internet CLASS	–
TRAFFIC	1DFF0005	INFO	Proxy / DNS	OPcode match	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)	The OpCode matched a configured rule, or the default rule of no match. The log message	DNS OpCode match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						specifies the action taken, the rule, and the OpCode.		
TRAFFIC	1DFF0006	INFO	Proxy / DNS	Query type match	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)	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.	DNS query type match	–
TRAFFIC	1DFF0007	INFO	Proxy / DNS	Question undersized	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56704 53 msg="ProxyDeny: DNS undersized question" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS query was blocked because the query size was less than the minimum valid size of 17 bytes.	DNS undersized question	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1DFF0008	INFO	Proxy / DNS	Question oversized	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56705 53 msg="ProxyDeny: DNS oversized question" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS query was blocked because the query size exceeds the maximum allowed size of 271 bytes.	DNS oversized question	–
TRAFFIC	1DFF0009	INFO	Proxy / DNS	Timeout	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 54807 53 msg="ProxyDrop: DNS timeout" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS connection was idle longer than the configured timeout value in the DNS policy.	DNS timeout	–
TRAFFIC	1DFF000A	INFO	Proxy / DNS	Response answer undersized	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56706 53 msg="ProxyDeny: DNS undersized answer" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS response was blocked because the response size was less than the minimum value of 17 bytes.	DNS undersized answer	–
TRAFFIC	1DFF000C	INFO	Proxy / DNS	Response ID Invalid	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 56706 53 msg="ProxyDeny: DNS invalid response" proxy_act="DNS-Outgoing.1" (DNS-proxy-00)	The DNS response was blocked because the response ID did not match the current or previous request	DNS invalid response	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						ID.		
TRAFFIC	1DFF000E	INFO	Proxy / DNS	Query question match	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)	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.	DNS question match	–
TRAFFIC	1DFF000F	INFO	Proxy / DNS	Request	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" app_id="61" app_cat_id="9" app_name="DNS" app_cat_name="Network Management" sig_vers="18.001" (DNS-proxy-00)	The DNS request audit log specifies the query type and name.	DNS request	–
TRAFFIC	1DFF0010	INFO	Proxy / DNS	IPS match	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" sig_vers="18.001" (DNS-proxy-00)	Intrusion Prevention Service (IPS) detected an intrusion threat. The log message specifies the signature ID, threat severity, signature name, and signature category.	DNS IPS match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	1DFF0012	INFO	Proxy / DNS	Application match	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" sig_vers="18.001" (DNS-proxy-00)	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.	DNS App match	–
TRAFFIC	21FF0000	INFO	Proxy / POP3	CAPA	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)	The CAPA response contained the unknown or blocked capability that is specified in the log message.	POP3 CAPA	–
TRAFFIC	21FF0001	INFO	Proxy / POP3	Authentication	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)	The authentication type matched a rule, or the default rule of no match. The log message specifies the rule	POP3 AUTH	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						name and authentication type.		
TRAFFIC	21FF0002	INFO	Proxy / POP3	Command	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)	The client sent an authentication command when it was not allowed.	POP3 command	–
TRAFFIC	21FF0005	INFO	Proxy / POP3	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)	A POP3 header matched a configured Header rule, or the default rule of no match. The log message specifies the rule and header.	POP3 header	–
TRAFFIC	21FF0006	INFO	Proxy / POP3	Content type	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)	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.	POP3 content type	–
TRAFFIC	21FF0007	INFO	Proxy /	File name	Allow 1-Trusted 0-External tcp 10.0.1.2 100.100.100.11 44035 110	The attachment	POP3	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			POP3		msg="ProxyAvScan: POP3 filename" proxy_act="POP3-Client.1" rule_name="Text files" file_name="high-triggerme.txt" user="wg" (POP3-proxy-00)	matches a configured file name rule, or the default rule of no match. The log message specifies the rule, file name, and user name.	filename	
TRAFFIC	21FF0009	INFO	Proxy / POP3	Timeout	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)	The connection was idle for longer than the configured timeout limit. The default limit is 1 minute.	POP3 timeout	–
TRAFFIC	21FF000A	INFO	Proxy / POP3	Request	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)	This audit log message specifies the bytes sent, bytes received, and user.	POP3 request	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	21FF000C	INFO	Proxy / POP3	IPS match	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" sig_vers="18.001" (POP3-proxy-00)	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.	POP3 IPS match	–
TRAFFIC	21FF000F	INFO	Proxy / POP3	GAV Virus found	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)	Gateway AntiVirus detected a virus or malware in the file. The log message specifies the virus name, user, and file name.	POP3 Virus found	–
TRAFFIC	21FF0010	INFO	Proxy / POP3	GAV cannot perform scan	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)	Gateway AntiVirus (GAV) failed to scan because of the error specified in the log message.	POP3 cannot perform Gateway AV	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	21FF0012	INFO	Proxy / POP3	Line length too long	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)	A line exceeds the configured limit. The default is 1,000 bytes. The log message specifies the line length.	POP3 line length too long	–
TRAFFIC	21FF0014	INFO	Proxy / POP3	Message format	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)	The message is not in an allowed format. The log message specifies the error and the user.	POP3 message format	–
TRAFFIC	21FF0015	INFO	Proxy / POP3	Encoding error	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)	The proxy was unable to decode and encode the message because of the error specified in the log message.	POP3 encoding error	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	21FF0016	INFO	Proxy / POP3	spamBlocker confirmed spam	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)	spamBlocker classified the message as confirmed SPAM. The log message specifies the sender and recipients.	POP3 Classified as confirmed SPAM	–
TRAFFIC	21FF0017	INFO	Proxy / POP3	spamBlocker BULK spam	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)	spamBlocker classified the message as bulk SPAM. The log message specifies the sender and recipients.	POP3 Classified as suspect SPAM	–
TRAFFIC	21FF0018	INFO	Proxy / POP3	spamBlocker suspect spam	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)	spamBlocker classified the message as suspect SPAM. The log message specifies the sender and recipients.	POP3 Classified as suspect SPAM	–
TRAFFIC	21FF001A	INFO	Proxy / POP3	spamBlocker exception matched	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)	The sender for the email matched a spamBlocker exception rule.	POP3 spamBlocker exception was matched	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						The log message specifies the sender, recipient, and subject.		
TRAFFIC	21FF001B	INFO	Proxy / POP3	spamBlocker not spam	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)	spamBlocker classified the message as not SPAM. The log message specifies the sender and recipients.	POP3 Classified as not SPAM	–
TRAFFIC	21FF001C	INFO	Proxy / POP3	spamBlocker classification unknown	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)	spamBlocker was unable to classify the message because of the error specified in the log message.	POP3 message classification is unknown because an error occurred while classifying	–
TRAFFIC	21FF001D	INFO	Proxy / POP3	Extra pad characters	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)	The POP3 proxy encountered extra pad characters in the body of a base64-encoded message.	POP3 extra pad characters in base64 input	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	21FF001E	INFO	Proxy / POP3	Application match	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" sig_vers="18.001" (POP3-proxy-00)	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.	POP3 App match	–
TRAFFIC	21FF001F	INFO	Proxy / POP3	APT threat detected	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)	APT Blocker found the threat specified in the log message in an attached file.	POP3 APT detected	–
TRAFFIC	21FF0021	INFO	Proxy / POP3	File submitted to 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)	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.	POP3 File submitted to APT analysis server	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	21FF0022	INFO	Proxy / POP3	File reported safe from APT hash check	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)	APT hash check did not report a threat from the object	POP3 File reported safe from APT hash check	–
TRAFFIC	22FF0000	INFO	Proxy / IMAP	Request	Allow 1-Trusted 0-External tcp 10.0.1.70 10.148.22.60 53589 143 msg="IMAP Request" proxy_act="IMAP-Client.Standard.1" email_len="652" action="allow" reason="" mbx="INBOX" user="wg" auth_method="plain" (IMAP-proxy-00)	This audit log message specifies the email message transaction result.	IMAP Request	–
TRAFFIC	22FF0001	INFO	Proxy / IMAP	Timeout	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)	The connection was idle for longer than the configured timeout limit. The default limit is 1 minute.	IMAP Timeout	–
TRAFFIC	22FF0005	INFO	Proxy / IMAP	Content Type	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)	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.	IMAP Content Type	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	22FF0006	INFO	Proxy / IMAP	Filename	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)	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.	IMAP Filename	–
TRAFFIC	22FF0008	INFO	Proxy / IMAP	Virus Found	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)	Gateway AntiVirus detected a virus or malware in the file. The log message specifies the virus name, file name, and user-related information.	IMAP Virus Found	–
TRAFFIC	22FF0009	INFO	Proxy / IMAP	Cannot Perform Gateway AV Scan	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)	Gateway AntiVirus (GAV) failed to scan because of the error specified in the log message	IMAP Cannot Perform Gateway AV Scan	–
TRAFFIC	22FF000A	INFO	Proxy / IMAP	APT detected	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"	APT Blocker found the threat specified in the	IMAP APT detected	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					md5="7abebcf53e97b586c92a9ce5b9985cd4" task_ uuid="e8a3730d1f88491c8821712e85d94929" threat_level="high" mbx="INBOX" user="wg" (IMAP-proxy-00)	log message in an attached file.		
TRAFFIC	22FF000C	INFO	Proxy / IMAP	File Submitted to 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)	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.	IMAP File Submitted to APT analysis server	–
TRAFFIC	22FF000D	INFO	Proxy / IMAP	File reported safe from APT hash check	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)	APT hash check did not report a threat from the object.	IMAP File reported safe from APT hash check	–
TRAFFIC	22FF000E	INFO	Proxy / IMAP	spamBlocker confirmed spam	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)	spamBlocker classified the message as confirmed SPAM. The log message specifies the user-related information	IMAP Classified as confirmed SPAM	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	22FF000F	INFO	Proxy / IMAP	spamBlocker bulk mail	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)	spamBlocker classified the message as bulk mail. The log message specifies the user-related information	IMAP Classified as bulk mail	–
TRAFFIC	22FF0010	INFO	Proxy / IMAP	spamBlocker suspect spam	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)	spamBlocker classified the message as suspect SPAM. The log message specifies the user-related information	IMAP Classified as suspect SPAM	–
TRAFFIC	22FF0012	INFO	Proxy / IMAP	spamBlocker exception matched	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)	The sender for the email matched a spamBlocker exception rule. The log message specifies the rule and user-related information.	IMAP spamBlocker exception was matched	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	22FF0013	INFO	Proxy / IMAP	spamBlocker not spam	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)	spamBlocker classified the message as not SPAM. The log message specifies the user-related information.	IMAP Classified as not SPAM	–
TRAFFIC	22FF0014	INFO	Proxy / IMAP	spamBlocker not spam	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)	spamBlocker was unable to classify the message because of the error specified in the log message. The log message specifies the user-related information.	IMAP Message classification is unknown because an error occurred while classifying	–
TRAFFIC	22FF0015	INFO	Proxy / IMAP	GAV file too large	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)	The attachment file size exceeds the Gateway AV scan size limit.	IMAP Gateway AV object too large	–
TRAFFIC	22FF0016	INFO	Proxy / IMAP	GAV file encrypted	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)	The attachment file is encrypted or password-protected.	Gateway AV object encrypted (password-protected)	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	22FF1017	INFO	Proxy / IMAP	Protocol invalid	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)	The IMAP proxy detected invalid TLS protocol.	IMAP invalid TLS protocol	–
TRAFFIC	22FF1018	INFO	Proxy / IMAP	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)	The IMAP proxy content inspection action for a secure connection.	IMAP TLS content inspection	–
TRAFFIC	22FF001B	INFO	Proxy / IMAP	IMAP spamBlocker spam ID	Allow Trusted External tcp 10.0.1.2 100.100.100.10 49166 143 msg="ProxyReplace: IMAP spamBlocker spam ID" proxy_act="IMAP-Client.Standard.1" wgrd_spam_id="v=2.4 cv=SPAh6MjH c=1 sm=1 tr=0 ts=61d874d5 p=MQD9vsuScg4A:10 a=3DxCuoXD4FnOMnt2MpZ/VQ==:17 a=pl62oyiqAlg65rFOYjJB3Aoq8KE=:19 a=9cW_t1CCXrUA:10 a=HpEJnUlJZJkA:10 a=DghFqjY3_ZEA:10 a=1lTjgDyuTKhQ4lGAEX4A:9" (IMAP-proxy-00)	The log message specifies the spam ID generated by spamBlocker.	IMAP spamBlocker spam ID	–
TRAFFIC	28FF0000	INFO	Proxy / SIP	Timeout	Deny 1-Trusted 0-External udp 10.0.1.5 192.168.53.143 5060 5060 msg="ProxyDrop: SIP timeout" (SIP-ALG-00)	The connection was idle for longer than the configured timeout value. The default value is 180 seconds.	SIP timeout	–
TRAFFIC	28FF0004	INFO	Proxy / SIP	Request	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_to="192.168.53.143" (SIP-ALG-00)	The log message specifies the source and destination of the allowed call.	SIP request	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	28FF0005	INFO	Proxy / SIP	Codec	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)	The codec is allowed or denied based on the setting for Denied Codecs in the SIP policy.	SIP codec	–
TRAFFIC	28FF0006	INFO	Proxy / SIP	Access control	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" From-header="102@10.0.1.2" (SIP-ALG-00)	The header address is allowed or denied based on the Access Control settings. The log message specifies the action taken, header and message ID.	SIP Access control	–
TRAFFIC	28FF0008	INFO	Proxy / SIP	IPS match	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" sig_vers="18.001" (SIP-ALG-00)	Intrusion Prevention Service (IPS) detected an intrusion threat. The log message specifies the signature ID, threat severity, signature name, signature category, destination host	SIP IPS match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						name and URI path.		
TRAFFIC	28FF0009	INFO	Proxy / SIP	Application match	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" app_id="12" app_name="SIP" app_beh_name="communicate" sig_vers="18.001" (SIP-ALG-00)	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.	SIP App match	–
TRAFFIC	2AFF0000	INFO	Proxy / H.323	Timeout	Deny 1-Trusted 0-External tcp 10.0.1.5 192.168.53.143 1720 1720 msg="ProxyDrop: H323 timeout" proxy_act="H.323-Client.1" (H323-ALG-00)	The connection was idle longer than the configured timeout value. The default value is 180 seconds.	H323 timeout	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	2AFF0001	INFO	Proxy / H.323	Request	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)	This log message specifies the IP addresses for the completed H323 call.	H323 request	–
TRAFFIC	2AFF0002	INFO	Proxy / H.323	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)	The media codec is denied because it matched a configured Denied Codec. The log message specifies the codec.	H323 codec	–
TRAFFIC	2AFF0003	INFO	Proxy / H.323	Access control	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" To-header="192.168.53.143" (H323-ALG-00)	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.	H323 Access control	–
TRAFFIC	2AFF0006	INFO	Proxy / H.323	IPS match	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	Intrusion Prevention	H323 IPS match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					Asterisk Invalid RTP Payload Type Number Memory Corruption" signature_cat="Access Control" sig_vers="18.001" (H323-ALG-00)	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.		
TRAFFIC	2AFF0007	INFO	Proxy / H.323	Application match	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" sig_vers="18.001" (H323-ALG-00)	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.	H323 App match	–
TRAFFIC	2CFF0000	INFO	Proxy / HTTPS	Request	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"	HTTPS transaction log	HTTPS Request	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					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)	includes server name, certificate details and action taken.		
TRAFFIC	2CFF0001	INFO	Proxy / HTTPS	WebBlocker Request categories	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)	WebBlocker identified the category for a web request. The log message specifies the category and host name.	HTTPS Request categories	–
TRAFFIC	2CFF0002	INFO	Proxy / HTTPS	WebBlocker service unavailable	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)	WebBlocker failed because a WebBlocker Server was not available.	HTTPS service unavailable	–
TRAFFIC	2CFF0003	INFO	Proxy / HTTPS	Domain name match	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)	This rule log includes the matched rule name or default rule of no match and the patterns its been matched against.	HTTPS domain name match	–
TRAFFIC	2CFF0005	INFO	Proxy / HTTPS	IPS Match	Deny 1-Trusted 0-External tcp 10.0.1.2 173.194.33.176 59545 443 msg="ProxyDrop: HTTPS IPS Match" proxy_act="HTTPS-Client.Standard.3" "signature_id="1110070" severity="4" signature_	Intrusion Prevention Service (IPS)	HTTPS IPS Match	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					name="DOS Apache mod_ssl HTTPS Request DOS -1" signature_cat="Dos/DDoS" sig_vers="18.001" (HTTPS-proxy-00)	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.		
TRAFFIC	2CFF0006	INFO	Proxy / HTTPS	HTTPS App Match	Deny 1-Trusted 0ssh -External tcp 10.0.1.2 173.194.33.176 59545 443 msg="ProxyDrop: HTTPS App Match" proxy_act="HTTPS-Client.Standard.3" app_cat_name="Network Protocols(3)" app_cat_id="19" app_name="HTTP Protocol over TLS SSL" app_id="94" app_beh_name="access" app_beh_id="6" sig_vers="18.001" (HTTPS-proxy-00)	Application Control identified the application type from the HTTPS 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.	HTTPS APP Match	–
TRAFFIC	2CFF0007	INFO	Proxy / HTTPS	Protocol invalid	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)	The HTTPS proxy detected an invalid SSL version.	HTTPS invalid protocol	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	2CFF0008	INFO	Proxy / HTTPS	Timeout	Deny 1-Trusted 0-External tcp 10.0.1.5 192.168.53.143 54707 443 msg="ProxyDrop: HTTPS timeout" (HTTPS-proxy-00)	The HTTPS connection was idle longer than the timeout value configured in the HTTPS policy. The default is 180 seconds.	HTTPS timeout	–
TRAFFIC	2CFF0009	INFO	Proxy / HTTPS	Content inspection	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)	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.	HTTPS content inspection	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
TRAFFIC	2CFF000A	INFO	Proxy / HTTPS	HTTPS content inspection exceptuion rule match	Allow 1-Trusted 0-External tcp 10.0.1.2 173.194.33.180 59276 443 msg="ProxyAllow: content inspection exception list match" proxy_act="HTTPS-Client.Standard.3" sni="www.gstatic.com" cn="*.google.com" exception_rule="allow google" action="allow" (HTTPS-proxy-00)	The HTTPS connection matches the content inspection exception rule and the defined action is taken.	HTTPS exception rule match	–
TRAFFIC	2DFF0000	INFO	Proxy / TCP-UDP	Request	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)	TCP-UDP transaction log for the traffic that is configured to allow or deny.	IP Request	–
TRAFFIC	2DFF0001	INFO	Proxy / TCP-UDP	IPS match	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" sig_vers="18.001" (TCP-UDP-proxy-00)	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.	IP IPS match	–
TRAFFIC	2DFF0004	INFO	Proxy / TCP-UDP	Protocol	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-	The TCP-UDP proxy recognized the	IP protocol	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					00)	protocol. The log message specifies the action taken, and the rule name.		
TRAFFIC	2DFF0005	INFO	Proxy / TCP-UDP	Application match	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" sig_vers="18.001" (TCP-UDP-proxy-00)	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.	IP App match	–
TRAFFIC	2DFF0006	INFO	Proxy / TCP-UDP	DNSWatch content filtered domain	Allow 1-Trusted 0-External tcp 10.0.1.2 54.173.101.99 60180 23 msg="ProxyAllow: IP DNSWatch blackholed domain" proxy_act="TCP-UDP-Proxy.Standard.1" Protocol="telnet" geo_dst="USA" (TCP-UDP-proxy-00)	DNSWatch DNS server returned the blackhole server IP address for the name resolution for requested domain. TCPUDP proxy	IP DNSWatch blackholed domain	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						acknowledge the blackhole server IP address and generates the log for the client request		
TRAFFIC	2DFF0007	INFO	Proxy / TCP-UDP	DNSWatch content filtered domain	Deny 1-Trusted 0-External tcp 10.0.1.2 54.173.101.99 60180 23 msg="ProxyAllow: IP DNSWatch content filtered domain" proxy_act="TCP-UDP-Proxy.Standard.1" Protocol="telnet" geo_dst="USA" (TCP-UDP-proxy-00)	DNSWatch DNS server returned the filterhole server IP address for the name resolution for requested domain from the content filtered domain configuration. TCPUDP proxy acknowledge the filterhole server IP address and generates the log for the client request	IP DNSWatch content filtered domain	–

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.

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
DIAG	5501000C	INFO	Management / System	Device restore failed	Device auto restore from USB drive image failed due to USB drive not found	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 ${restore_type} restore from ${image_source} image failed for ${reason}
DIAG	5501000D	INFO	Management / System	Creating USB auto restore image failed	Creation of USB auto restore image failed due to no USB drive	–	Creation of USB auto restore image failed due to %s	Creation of USB auto restore image failed: ${reason}
DIAG	55010010	INFO	Management / System	USB drive format	USB drive format operation was successful	–	USB drive format operation was %s	USB drive format ${result}
DIAG	55010014	INFO	Management / System	Generate system diagnostic file failed	Generate system diagnostic file to USB drive failed	–	Generate system diagnostic file to %s failed	Generate system diagnostic file to ${device} failed
DIAG	55010015	INFO	Management / System	Periodic support snapshot is enabled	System periodic support snapshot is enabled	–	System periodic support snapshot is enabled	–
DIAG	55010017	INFO	Management / System	Generate system	Exported system diagnostic file to server successfully	–	Exported system diagnostic file to %s successfully	Generate system diagnostic file to

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				diagnostic successfully				${device} successfully
DIAG	55010018	INFO	Management / System	Reset to the default configuration failed	Reset to the default configuration failed when the device was rebooted.	The default configuration settings were not restored after a system reset.	Reset to the default configuration failed when the device was rebooted.	–
DIAG	5501001B	INFO	Management / System	System backup failed	System backup to USB drive failed due to write file to USB drive error	–	System backup %s failed due to %s.	System backup ${dest device} failed: ${reason}
DIAG	5501001C	INFO	Management / System	USB auto restore failed reason	USB auto restore failed due to not detect the USB drive	–	USB auto restore failed due to %s	USB auto restore failed for ${reason}

Event

Management log messages of the *Event* log type.

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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}
EVENT	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	–
EVENT	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'	–
EVENT	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'	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	01020003	WARN	Management / Configuration	Feature expired	'LIVESECURITY' feature expired. Contact WatchGuard to renew your subscription.	–	'%s' feature expired. Contact WatchGuard to renew your subscription.	–
EVENT	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.	–
EVENT	01040001	INFO	Management / Configuration	Default device settings in use for safe mode	Device default configuration was loaded in safe mode	The device configuration was reset to the default settings because the device is in safe mode.	Device default configuration was loaded in safe mode	–
EVENT	01050001	INFO	Management / Configuration	Moved the policy to new position	Moved Ping policy from position 2 to 6	When change the policy order, there will be move operation to move the policies.	Moved %s policy from position %d to %d	Moved ${policy name} from ${old position} to ${new position}
EVENT	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	–
EVENT	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	Authentication of %s user [%s@%s] from %s was accepted	Authentication of ${user_type} user [${user_name}@${auth_server}] from ${ipaddr} was accepted.

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						this is an administrative user, a firewall user, or another type of user.		
EVENT	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_addr} was rejected, ${reason}
EVENT	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}
EVENT	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 ${failure_count} login failures
EVENT	11000008	WARN	Management / Authentication	BOVPN TLS client authentication failed	Authentication of BOVPN TLS client [EasternOffice] from 198.51.100.2 was rejected, pre-shared key is incorrect	BOVPN TLS client authentication failed. The log message specifies the reason.	Authentication of BOVPN TLS client [%s] from %s was rejected, %s	Authentication of BOVPN TLS client [${client_name}] from ${ip_addr} was rejected, ${reason}
EVENT	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}.
EVENT	1100000D	WARN	Management / Authentication	Authentication server unavailable	Authentication of user [user1@example.com] failed. Both primary and	Authentication failed because both the primary	Authentication of user [%s@%s] failed. Both primary and secondary	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					secondary servers are unavailable.	and secondary authentication servers are unavailable.	servers are unavailable.	
EVENT	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.	–
EVENT	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	–
EVENT	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.	–
EVENT	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.	–
EVENT	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.	–
EVENT	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.	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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.	–
EVENT	11000015	INFO	Management / Authentication	Logon Disclaimer configuration change	Logon Disclaimer was enabled	The configuration of Logon Disclaimer was changed when Firebox is on CSFC mode.	%s %s	–
EVENT	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 Management Server at 10.139.44.88. Revision: dummy_config_ rev_id. Comments: update tcp segment.	The updated configuration file was successfully sent to the device from the specified Management Server. The log message indicates if the feature key was updated. The log message might also specify the revision ID and includes comments about the update.	The configuration file %s for the device %s successfully updated after a request from %s from the Management Server at %s.%s%s%s%s.	–
EVENT	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	Device configuration file %s successfully updated. Configuration file retrieved from the Management Server at %s.	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						Server. The log message also indicates if device retrieved a feature key.		
EVENT	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.	–
EVENT	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.	–
EVENT	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	—
EVENT	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	Connected to the backup Log Server at %s	—

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
						Server designated as the backup server.		
EVENT	3D040003	INFO	Management / Logging	Add/Remove syslog server	Deleted syslog server : 3.3.3.3	Log the event when add/remove syslog server	%s	—
EVENT	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}
EVENT	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}
EVENT	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	3E000005	INFO	Management / Accounting	Property change	Updated the value of the management session idle timeout from 3600 seconds to 7200 seconds	Config changed. The log message specifies the name of the property, the old and new value.	Updated the value of %s from %ld%sto %ld%s.	Updated the value of ${property name} from ${old value} ${unit} to ${new value} ${unit}
EVENT	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}.
EVENT	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: ${current CA version number}.
EVENT	40010003	INFO	Management / Certificate	Certificate not valid yet	Certificate (subject=o=WatchGuard ou=Fireware cn=Fireware web CA) is not valid.	Certificate not valid yet	Certificate (subject=%s) is not valid.	Certificate (subject=${certificate subject}) is not valid.
EVENT	40010004	INFO	Management / Certificate	Certificate expired	Certificate (subject=o=WatchGuard ou=Fireware cn=Fireware web CA) is expired.	Certificate expired	Certificate (subject=%s) is expired.	Certificate (subject=${certificate subject}) is expired.
EVENT	40010005	INFO	Management / Certificate	Certificate revoked	Certificate (subject=o=WatchGuard ou=Fireware cn=Fireware web CA) is revoked.	Certificate revoked	Certificate (subject=%s) is revoked.	Certificate (subject=${certificate subject}) is revoked.

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	40010006	INFO	Management / Certificate	Generated/imported ertificate signing request	Generated certificate signing request CN=test2, O=wgti2.net, C=US	Generated Certificate signing request or imported certificate signed with csr	%s certificate%s%s.	>%s certificate%s%s
EVENT	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	–
EVENT	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}
EVENT	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	–
EVENT	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	–
EVENT	41000005	INFO	Management / LiveSecurity	Feature key download succeeded	Feature key from LiveSecurity Service was	The feature key for	Feature key from LiveSecurity Service was	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					received	the device was successfully downloaded from the LiveSecurity Service.	received	
EVENT	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	–
EVENT	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	–
EVENT	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)	–
EVENT	41010001	INFO	Management /	RapidDeploy	RapidDeploy configuration	The RapidDeploy	RapidDeploy	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			LiveSecurity	configuration from USB succeeded	from a USB drive was applied successfully	configuration was successfully applied from a USB drive.	configuration from a USB drive was applied successfully	
EVENT	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 USB drive was not applied: %s	–
EVENT	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}.
EVENT	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 ${time}
EVENT	55010002	ERROR	Management / System	LIVESECURITY feature not found	Valid 'LIVESECURITY' feature not found	–	Valid 'LIVESECURITY' feature not found	–
EVENT	55010003	ERROR	Management / System	LIVESECURITY expired	'LIVESECURITY' feature expired (Tue May 14 12:25:00 2013) prior to package release date (Wed May 15 01:00:00 2013)	–	'LIVESECURITY' feature expired (%s) prior to package release date (%s)	'LIVESECURITY' feature expired (${expiration time}) prior to package release date (${package release time})
EVENT	55010004	INFO	Management /	Shutdown	Shutdown requested by	–	Shutdown requested by	–

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
			System		system		system	
EVENT	55010005	INFO	Management / System	Reboot	System is rebooting	–	System is rebooting	–
EVENT	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}
EVENT	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}
EVENT	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}
EVENT	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}
EVENT	55010013	INFO	Management / System	USB auto restore started	USB auto restore started	–	USB auto restore started	–
EVENT	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}

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	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	–
EVENT	5501001A	WARN	Management / System	Upgrade failed	System upgrade failed: 'LIVESECURITY' feature expired	–	System upgrade failed: %s	System upgrade failed: ${reason}
EVENT	5501001D	INFO	Management / System	Logo upload succeeded	Upload of logo succeeded	–	Upload of logo succeeded	–
EVENT	55010020	INFO	Management / System	Backup succeeded	System backup succeeded	–	System backup succeeded	–
EVENT	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
EVENT	55010022	INFO	Management / System	USB auto restore image created	USB auto restore image successfully created	–	USB auto restore image successfully created	–
EVENT	55010023	INFO	Management / System	System integrity check started	System integrity check started	–	System integrity check started	System integrity check started
EVENT	55010024	INFO	Management / System	System integrity check passed	System integrity check passed	–	System integrity check passed	System integrity check passed

Type	ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
EVENT	55010025	ERROR	Management / System	System integrity check failed	System integrity check failed. Checksum check: Signature did not verify	–	System integrity check failed. %s%s: %s	System integrity check failed. ${reason}
EVENT	55010026	ERROR	Management / System	System integrity check error	System integrity check could not complete because of an error. Checksum check: Failed to access file etc/code-signed	–	System integrity check could not complete because of an error. %s%s: %s	System integrity check could not complete because of an error. ${reason}

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
3A000002	INFO	Cluster / Event Monitoring	VRRP enabled	VRRP is now enabled for Cluster.	Virtual Router Redundancy Protocol (VRRP) is now enabled for this Active/Passive Cluster.	VRRP is now enabled for Cluster.	–
3A000004	INFO	Cluster / Event Monitoring	VRRP start master	Virtual Router with cluster ID 1 started in master state.	VRRP started in master state.	Virtual Router with cluster ID %d started in master state.	Virtual Router with cluster ID ${value} started in master state.
3A000005	INFO	Cluster / Event Monitoring	VR shutdown	Virtual Router with cluster ID 1 returned to initial state.	Virtual Router returned to initial state.	Virtual Router with cluster ID %d returned to initial state.	Virtual Router with cluster ID ${id} returned to initial state
3A000006	INFO	Cluster / Event Monitoring	VR pause	Virtual Router with cluster ID 1 becomes backup on pause event	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 ${id} becomes backup on pause event
3A000007	INFO	Cluster / Event Monitoring	VR resume	Virtual Router with cluster ID 1 becomes master on resume event	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 ${id} becomes master on resume event
3A000008	INFO	Cluster / Event Monitoring	VR backup state	Virtual Router with cluster	Virtual Router state	Virtual Router with cluster ID %d state changed from master to backup	Virtual Router with

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				ID 1 state changed from master to backup	changed from master to backup		cluster ID ${id} state changed from master to backup
3A00000A	INFO	Cluster / Event Monitoring	VR notification gap	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 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 ${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 with cluster ID 1 state changed to master	Virtual Router state changed to master	Virtual Router with cluster ID %d state changed to master	Virtual Router with cluster ID ${id} state changed to master
3A00000C	ERROR	Cluster / Event Monitoring	VRRP initialization failed	Cluster VRRP initialization failed	Initialization of Virtual Router Redundancy Protocol (VRRP) failed.	Cluster VRRP initialization failed	–
38000002	ERROR	Cluster / Management	DHCP overwrite	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 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	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 ${ip} on eth${port}. Please disable DHCP server access to eth${port}.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					specifies the interface number and IP address the cluster attempted to assign to the member.		
38000003	INFO	Cluster / Management	Cluster interface up	Cluster interface eth5 is up.	Cluster interface link status changed to up.	Cluster interface %s is up.	Cluster interface ${ifname} is up.
38000004	WARN	Cluster / Management	Cluster interface down	Cluster interface eth5 is down.	Cluster interface link status changed to down.	Cluster interface %s is down.	Cluster interface ${ifname} is down
3800025C	INFO	Cluster / Management	Configuration update	Cluster member 80B20002E5BCD received updated configuration; version 3.	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 ${member} received updated configuration; version ${version}.
38000264	WARN	Cluster / Management	Time synchronization failure	Cluster time synchronization failed.	The cluster master's attempt to synchronize time to a cluster member failed	Cluster time synchronization failed.	

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3B000001	INFO	Cluster / Transport	Channel status change	Cluster channel from member 80B20002E5BCD to master is up	The cluster communication channel between the specified members changed state.	Cluster channel from member %s to master is %s.	Cluster channel from member ${member} to master is ${state}.
3B000002	INFO	Cluster / Transport	Cluster interface down	Cluster interface eth5 is down.	The specified Cluster interface is down.	Cluster interface %s is down.	Cluster interface ${ifname} is down.

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	Virtual Router with cluster ID 1 is now enabled	The Virtual Router representing the cluster is now enabled	Virtual Router with cluster ID %d is now enabled	Virtual Router with cluster ID ${id} is now enabled
3A00000F	INFO	Cluster / Event Monitoring	VR disabled	Virtual Router with cluster ID 1 is now disabled	The Virtual Router representing the cluster is now disabled	Virtual Router with cluster ID %d is now disabled	Virtual Router with cluster ID ${id} is now disabled

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
38000278	WARN	Cluster / Management	Cluster disabled	Cluster disabled. Non-master member 80B20002E5BCD will be reset to factory-default settings.	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 %s will be reset to factory-default settings.
38000279	WARN	Cluster / Management	Critical configuration change	Non-master member 80B20002E5BCD will be reset to factory-default settings due to a critical cluster 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 ${member} will be reset to factory default-settings due to a critical cluster configuration change.
38000280	ERROR	Cluster / Management	Device discovery failed	Cluster master 80B20002E5BCD was unable to issue a device discovery message.	The cluster master was unable to issue a device discovery message.	Cluster master %s was unable to issue a device discovery message.	Cluster master ${master} was unable to issue a device discovery message.
38000282	INFO	Cluster / Management	Member ready to join	Member 80B20002E5BCD is ready to join the cluster.	Local member has FireCluster enabled and is	Member %s 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
					ready to join.		
3800025A	INFO	Cluster / Management	Cluster enabled	Cluster enabled on member 80B20002E5BCD.	Cluster was enabled on the specified member.	Cluster enabled on member %s.	Cluster enabled on member ${member}.
3800025B	INFO	Cluster / Management	Cluster disabled on master	Cluster disabled on cluster master 80B20002E5BCD.	Cluster disabled on the cluster member while it was the cluster master.	Cluster disabled on cluster master %s.	Cluster disabled on cluster master ${master}.
3800027A	WARN	Cluster / Management	Non-master member removed	Non-master cluster member 80B20002E5BCD was removed from cluster, and will be reset to factory-default settings.	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 %s was removed from cluster, and will be reset to factory-default settings.
3800027E	ERROR	Cluster / Management	Factory-default reset failed	Failed to reset cluster member 80B20002E5BCD to factory-default settings.	Failed to reset to factory-default settings.	Failed to reset cluster member %s to factory-default settings.	Failed to reset member ${member} to factory-default settings.
39000003	WARN	Cluster / Operations	Heartbeat lost	Master 80B20002E5BFE detected loss of heartbeat from member 80B20002E5BCD, cluster channel is up.	The specified Cluster failed to receive a heartbeat message.	Master %s detected loss of heartbeat from member %s, cluster channel is up.	Master ${master} detected loss of heartbeat from member ${member}, cluster channel is up.
39000005	INFO	Cluster / Operations	Member promoted to master	Member 80B20002E5BCD is now master.	The specified member has become master.	Member %s is now master.	Member ${member} is now master.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
39000007	ERROR	Cluster / Operations	Failover due to WAI	Master 80B20002E5BCD failed over to member 80B20002E5BFE, which has a greater Weighted Average Index.	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 ${master} failover to member ${member} with greater Weighted Average Index.
39000010	INFO	Cluster / Operations	Member role change	Member 80B20002E5BCD changed role to master	The cluster member changed to the specified role.	Member %s changed role to %s.	Member ${member} role changed to ${role}.
39000011	INFO	Cluster / Operations	Interface link status change	Monitored interface eth0 link is down.	Specified monitored interface link status changed, which will change the health index for the member.	Monitored interface %s link is %s.	Monitored interface ${ifname} link is ${state}.
39000012	INFO	Cluster / Operations	New master	Member 80B20002E5BCD took over as master from member 80B20002E5BFE.	The specified member has taken over as master..	Member %s took over as master from member %s.	Member ${member} took over as master from member ${member}.
39000015	INFO	Cluster / Operations	Failover initiated by administrator	Master 80B20002E5BCD initiated failover by administrator request.	The administrator has initiated a failover.	Master %s initiated failover by administrator request.	Master ${master} initiated failover by administrator request..
39000016	WARN	Cluster / Operations	Cannot initiate failover	Cannot initiate failover from master 80B20002E5BCD to member 80B20002E5BFE due to higher Weighted Average Index on current master or	The failover requested by administrator cannot proceed because the	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 ${master} to member ${member} due to higher Weighted Average Index on current master or other

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				backup master is unreachable.	master has a higher health index, or the backup master is unreachable.		member is unreachable.
39000019	ERROR	Cluster / Operations	Failover due to interface state change	Cluster failover due to interface eth4 link down event.	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 ${ifname} link ${state} event.
39000058	INFO	Cluster / Operations	Member Role Change	Cluster member 80B20002E5BCD changed role from idle to backup master	The role of the specified Cluster member changed.	Cluster member %s changed role from %s to %s.	Cluster member ${member} changed role from ${role} to ${role}.
3900000C	ERROR	Cluster / Operations	Synchronization failed	Full state synchronization from master 80B20002E5BCD to backup master 80B20002E5BFE 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 ${master} to backup master ${member} failed.
3900000D	ERROR	Cluster / Operations	Synchronization timeout	Full state synchronization from master 80B20002E5BCD to backup master 80B20002E5BFE timed out.	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 ${master} to backup master ${member} timed out.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
3900000E	INFO	Cluster / Operations	Synchronization successful	Full state synchronization from master 80B20002E5BCD to backup master 80B20002E5BFE completed successfully.	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 ${master} to backup master ${member} completed successfully
3900000F	ERROR	Cluster / Operations	Failover due to link-down	Master 80B20002E5BCD failed-over to member 80B20002E5BFE due to a link-down event on interface eth3.	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 ${master} failed-over to member ${member} due to a link-down event on interface ${ifname}.

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 38.

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	—

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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	—
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
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}
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	IKE Phase 1 negotiation failed	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s'	IKE phase-1 negotiation from ${local_addr} to ${peer_addr}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				172.16.12.81:500 failed. Gateway-Endpoint='gateway.1' Reason=Received DH group 2, expecting 14	because of incorrect Diffe-Hellman group in proposal from remote gateway. The log message specifies the received and expected group number.	Reason=Received DH group %d, expecting %d	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}
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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.
0203000A	ERROR	VPN /	IKE Phase 1 invalid	IKE phase-1 negotiation	IKE Phase 1	IKE phase-1 negotiation from %s to	IKE phase-1 negotiation from

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		IPSEC	Main Mode second message	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.	negotiation failed because of invalid second message received by local gateway.	%s failed. Gateway-Endpoint='%s' Reason=Received invalid main mode second message. Check VPN IKE diagnostic log messages for more information.	${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.
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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.
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
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

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
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 - ${reason}
02030014	INFO	VPN / IPSEC	Received informational error message	Received 'Invalid Exchange Type' message from 172.16.12.81:500 for 'gateway.1' gateway endpoint. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.	Received the specified information or error message from remote gateway.	Received '%s' message from %s for '%s' gateway endpoint. Check VPN IKE diagnostic log messages on the remote gateway endpoint for more information.	Received '${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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.
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}
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-	IKE Phase 1 negotiation failed because peer certificate is not	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}'

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				Endpoint='gateway.1' Reason=Peer certificate is not issued by known trusted CA	issued by a known and trusted Certificate Authority (CA).		Reason=${reason}
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

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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. ${n} retries left.
02030022	WARN	VPN / IPSEC	DPD max failure	Remote gateway 'gateway.1' with IP 172.16.13.204:500 presumed dead due to DPD failure. Deleted all tunnels that use this gateway. Check the connection between local and remote gateway endpoints.	The Firebox or XTM device deleted a VPN tunnel because the remote gateway did not respond to DPD R_U_THERE requests.	Remote gateway '%s' with IP %s presumed dead due to DPD failure.%s	Remote gateway '${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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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}
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}'.
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

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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}
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}'
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 with configured aggressive mode ID.	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 configuration on both local and remote gateways.	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received ID did not match with configured aggressive mode ID.	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.
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-	IKE Phase 1 negotiation failed because the received IKE version did not	IKE phase-1 negotiation from %s to %s failed. Gateway-Endpoint='%s' Reason=Received IKE version did not match the configured IKE	IKE phase-1 negotiation from ${local_addr} to ${peer_addr} failed. Gateway-Endpoint='${gw-ep}'

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				Endpoint='gateway.1' Reason=Received IKE version did not match the configured IKE version.	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.	version.	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}.
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

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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}
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 Diffie-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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.
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	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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					configuration.		
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.
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.
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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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 XAUTH enabled.	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 server Extended Authentication (XAuth) enabled.	Rejected phase-1 authentication method %s from %s, expecting server XAUTH enabled.	Rejected phase 1 authentication method ${auth_method} from ${peer_addr}, expecting server XAUTH 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

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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
02060006	INFO	VPN / IPSEC	Mobile VPN with IPSec user connected with no group	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 '${user_name}' is authenticated without group information
02060007	INFO	VPN / IPSEC	Mobile user group information	MUVPN user 'user.1' is a member of 'muvpn' group.	Specified Mobile VPN with IPSec user belongs to the specified group.	MUVPN user '%s' is a member of '%s' group.	MUVPN user '${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}
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}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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 endpoint not found to handle IKE_SA_INIT_R message	Dropped IKEv2 IKE_SA_INIT message from 172.16.12.82:500. Reason='gateway.1' gateway endpoint not found to handle message with message ID 0x0.	Gateway endpoint was not found to handle the received IKE_SA_INIT_R message	Dropped IKEv2 %s message from %s. Reason='%s' gateway endpoint not found to handle message with message ID 0x%x.	Dropped IKEv2 ${exchange_type} message from ${peer_addr}. Reason='${gw-ep}' gateway endpoint not found to handle IKE_SA_INIT message with message ID ${recvd_message_id}.
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.
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.	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

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				Reason=Matching gateway endpoint not found.			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.
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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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	IKEv2 message exchange failed	IKEv2 %s exchange from %s to %s failed. Tunnel='%s'. Reason=DH-	IKEv2 ${exchange_type} exchange from ${local_addr}

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				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.	because the DH group in the received Key Exchange (KE) payload does not match the DH-Group in the selected proposal.	Group %d in the KE payload does not match DH-Group %d selected in the %s proposal.	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.
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}.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.
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)	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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				message.			
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}.
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}.
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	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

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				SA by received SPI 0xbaba1509 in CREATE_CHILD_SA(REKEY[CHILD SA]) request.			${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.
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.
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.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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}
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	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	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}.

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				203.0.113.2.	endpoint configuration on both the local and remote gateways.		
25000000	INFO	VPN / SSLVPN	User login	Mobile VPN with SSL user tsmith logged in. Virtual IP address is 192.168.113.2. Real IP address is 192.51.100.2.	%s %s logged in. Virtual IP address is %s. Real IP address is %s.	A user logged in to VPN with SSL. The log message specifies the VPN user type,and the user's name, virtual IP address, and real IP address.	${vpn_user_type} ${user_name} logged in. Virtual IP address is ${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.	%s %s logged off. Virtual IP address is %s.	The VPN with SSL user with the specified virtual IP address logged out.	${vpn_user_type} ${user_name} logged off. Virtual IP address was ${virtual_ipaddr}.
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'.	Updated Mobile VPN with L2TP session for user '%s\%s', virtual IP address '%s'.	Mobile VPN with L2TP updated the session for the specified user. The log message specifies the assigned virtual IP address.	–
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 Mobile VPN with L2TP session for user '%s\%s', virtual IP address '%s'.	Deleted a Mobile VPN with L2TP session with the specified virtual IP address.	–

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	–
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)!!	–
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}
02090001	WARN	VPN / IPSEC	BOVPN tunnel limit reached	The maximum number of allowed active BOVPN	The maximum allowed number of BOVPN	The maximum number of active allowed BOVPN tunnels has been	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
				tunnels has been reached (Maximum: 500 Current: 500).	tunnel routes have been established. No new tunnel routes can be created until active tunnel routes expire or are deleted.	reached (Maximum: %d Current: %d)	
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.	–
5B010001	INFO	VPN / L2TP	Daemon started	The Mobile VPN with L2TP daemon started successfully.	The Mobile VPN with L2TP daemon started successfully.	The Mobile VPN with L2TP daemon started.	–
5B010002	INFO	VPN / L2TP	Configuration updated	Updating configuration for Mobile VPN with L2TP.	Updating configuration for Mobile VPN with L2TP.	The Mobile VPN with L2TP daemon received a configuration update.	–
5B010003	INFO	VPN / L2TP	Daemon stopped	Stopped Mobile VPN with L2TP daemon.	Stopped Mobile VPN with L2TP daemon.	The Mobile VPN with L2TP daemon stopped.	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
78000000	ERROR	VPN / VPN TDR Host Sensor Enforcement Module	VPN TDR Host Sensor Enforcement failure	VPN (SSL) connection by user jdoe@myexample.com failed to meet TDR Host Sensor Enforcement requirement: Host Sensor connection failed.	VPN (%s) connection by user %s%s%s failed to meet TDR Host Sensor Enforcement requirement: %s.	Mobile VPN connection did not meet TDR Host Sensor Enforcement requirement	VPN (${$vpn_type}) connection by user ${user}@${domain} failed to meet TDR Host Sensor Enforcement requirement: ${reason}.
78000001	INFO	VPN / VPN TDR Host Sensor Enforcement Module	VPN TDR Host Sensor Enforcement success	VPN (IKEv2) connection by user jdoe@Firebox-DB met all TDR Host Sensor Enforcement requirements.	VPN (%s) connection by user %s%s%s met all TDR Host Sensor Enforcement requirements.	Mobile VPN connection met all TDR Host Sensor Enforcement requirement	VPN (${$vpn_type}) connection by user ${user}@${domain} met all TDR Host Sensor Enforcement requirements.

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	–
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	The number of connected Mobile Security users has reached 90 percent of the licensed capacity. Maximum: %d	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
					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.		
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.	–
70010003	INFO	Mobile Security /	Mobile device user logout	Mobile device eee66f78-3d74-4002-8161-	User has logged out of Firebox	Mobile device %s: user %s logged out.	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
		Endpoint Manager		95938dca4390: user joe logged out.	from FireClient on the device.		
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.	–

ID	Level	Area	Name	Log Message Example	Description	Format	Message Variables
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.	–
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}