# Firewall Log

**Syslog Priority** – the priority of the log messages.

|  |  |  |
| --- | --- | --- |
| **Level** | **System** | **Description** |
| Emergency | 0 | System unusable messages |
| Alert | 1 | Immediate action required messages |
| Critical | 2 | Critical condition messages |
| Error | 3 | Error condition messages |
| Warning | 4 | Warning condition messages |
| Notification | 5 | Normal but significant messages |
| Information | 6 | Informational messages |
| Debugging | 7 | Debugging messages |

**“**Syslog messages can be one of eight predefined severity levels. The following table briefly summarizes the different severity logging levels:” -https://www.cisco.com/c/en/us/about/security-center/identify-incidents-via-syslog.html

**Operations –** type of activity being performed

Build

Tear down

Deny

Empty

**Message Code**

*Place to find error codes*

<https://www.cisco.com/en/US/docs/security/asa/asa80/system/message/logmsgs.html#wp5611140>

|  |  |
| --- | --- |
| **Code** | Message |
| ASA--4-733100 | When a Basic Drop Rate is Exceeded and %ASA-4-733100 is Generated. With this information, check the output of show asp drop in order to determine the reasons why traffic is being dropped. For a more detailed view of traffic that is dropped for a specific reason, use an ASP drop capture with the reason in question in order to see all of the packets that are being dropped. (Operation is empty)  <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html>  Error Message    %ASA-4-733100: Object drop rate rate\_ID exceeded. Current burst rate  is rate\_val per second, max configured rate is rate\_val; Current average rate is  rate\_val per second, max configured rate is rate\_val; Cumulative total count is  total\_cnt  •https://www.cisco.com/en/US/i/templates/blank.gifObject—The general or particular source of a drop rate count, which might include the following:  - Firewall  - Bad pkts  - Rate limit  - DoS attck  - ACL drop  - Conn limit  - ICMP attk  - Scanning  - SYN attck  - Inspect  - Interface |
| ASA-bridge-6-110002 | Error Message    %PIX|ASA-6-110002: Failed to locate egress interface for *protocol* from  *src interface*:*src IP/src port* to *dest IP/dest port*  Explanation **An error occurred when the security appliance tried to find the interface through which to send the packet.**  •https://www.cisco.com/en/US/i/templates/blank.gif*protocol*—The protocol of the packet  •https://www.cisco.com/en/US/i/templates/blank.gif*src interface*—The interface from which the packet was received  •https://www.cisco.com/en/US/i/templates/blank.gif*src IP*—The source IP address of the packet  •https://www.cisco.com/en/US/i/templates/blank.gif*src port*—The source port number  •https://www.cisco.com/en/US/i/templates/blank.gif*dest IP*—The destination IP address of the packet  •https://www.cisco.com/en/US/i/templates/blank.gif*dest port*—The destination port number  Recommended Action    Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.  Operation is empty |
| ASA-session-6-106015 | Error Message    %PIX|ASA-6-106015: Deny TCP (no connection) from IP\_address/*port* to  IP\_address/*port* flags *tcp\_flags* on interface *interface\_name*.  Explanation    **The security appliance discarded a TCP packet that has no associated connection in the security appliance connection table. The security appliance looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is not an existing connection, the security appliance discards the packet.**  **Recommended Action    None required unless the security appliance receives a large volume of these invalid TCP packets. If this is the case, trace the packets to the source and determine the reason these packets were sent.**  Operation is deny |
| ASA-session-6-302010 | Error Message    %PIX|ASA-6-302010: connections in use, connections most used    Explanation    **This is a connection-related message. This message appears after a TCP connection restarts. connections is the number of connections.**  **Recommended Action    None required.**  Operation is empty |
| ASA-session-6-302013 | Error Message    %PIX|ASA-6-302013: **Built** {inbound|outbound} TCP connection\_id for  interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address*/*real-port  (mapped-address/mapped-port) [(user)]  Explanation   **A TCP connection slot between two hosts was created.**  •https://www.cisco.com/en/US/i/templates/blank.gifconnection\_id is a unique identifier.  •https://www.cisco.com/en/US/i/templates/blank.gifinterface, real-address, real-port identify the actual sockets.  •https://www.cisco.com/en/US/i/templates/blank.gifmapped-address, mapped-port identify the mapped sockets.  •https://www.cisco.com/en/US/i/templates/blank.gifuser is the AAA name of the user.  If inbound is specified, the original control connection was initiated from the outside. For example, for FTP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, the original control connection was initiated from the inside.  Recommended Action    None required  Operation is build (TCP) |
| ASA-session-6-302014 | Error Message    %PIX|ASA-6-302014: **Teardown** TCP connection id for  interface:real-address/real-portto interface:real-address/real-portduration hh:mm:ss bytes  bytes [reason] [(user)]  Explanation    **A TCP connection between two hosts was deleted. The following list describes the message values:**  **•https://www.cisco.com/en/US/i/templates/blank.gifconnection id is an unique identifier.**  **•https://www.cisco.com/en/US/i/templates/blank.gifinterface, real-address, real-port identify the actual sockets.**  **•https://www.cisco.com/en/US/i/templates/blank.gifduration is the lifetime of the connection.**  **•https://www.cisco.com/en/US/i/templates/blank.gifbytes bytes is the data transfer of the connection.**  **•https://www.cisco.com/en/US/i/templates/blank.gifuser is the AAA name of the user.**  The website provides a chart of all the explanations  Operation is teardown (TCP) |
| ASA-session-6-302015 | Error Message    %PIX|ASA-6-302015: Built {inbound|outbound} UDP connection number for  interface\_name:real\_address/real\_port(mapped\_address/mapped\_port) to  interface\_name:real\_address/real\_port(mapped\_address/mapped\_port) [(user)]  Explanation    **A UDP connection slot between two hosts is created. The following list describes the message values:**  •https://www.cisco.com/en/US/i/templates/blank.gifconnectionnumber—A unique identifier.  •https://www.cisco.com/en/US/i/templates/blank.gifinterface, real\_address, real\_port—The actual sockets.  •https://www.cisco.com/en/US/i/templates/blank.gifmapped\_address and mapped\_port—The mapped sockets.  •https://www.cisco.com/en/US/i/templates/blank.gifuser—The AAA name of the user.  If inbound is specified, then the original control connection is initiated from the outside. For example, for UDP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, then the original control connection is initiated from the inside.  Recommended Action    None required.  Operation is build (UDP) |
| ASA-session-6-302016 | 302016  Error Message    %PIX|ASA-6-302016: **Teardown** UDP connection number for  interface:real-address/real-port to interface:real-address/real-portduration hh:mm:ss bytes  bytes [(user)]  Explanation    **A UDP connection slot between two hosts was deleted. The following list describes the message values:**  •https://www.cisco.com/en/US/i/templates/blank.gifconnection number is an unique identifier.  •https://www.cisco.com/en/US/i/templates/blank.gifinterface, real\_address, real\_port are the actual sockets.  •https://www.cisco.com/en/US/i/templates/blank.giftime is the lifetime of the connection.  •https://www.cisco.com/en/US/i/templates/blank.gifbytes is the data transfer of the connection.  •https://www.cisco.com/en/US/i/templates/blank.gifconnection id is an unique identifier.  •https://www.cisco.com/en/US/i/templates/blank.gifinterface, real-address, real-port are the actual sockets.  •https://www.cisco.com/en/US/i/templates/blank.gifduration is the lifetime of the connection.  •https://www.cisco.com/en/US/i/templates/blank.gifbytes is the data transfer of the connection.  •https://www.cisco.com/en/US/i/templates/blank.gifuser is the AAA name of the user.  Recommended Action    None required.  Operation is Teardown (UDP) |
| ASA-session-6-302020 | Error Message    %PIX|ASA-6-302020: **Built** {in | out}bound ICMP connection for faddr  {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr  Explanation    **An ICMP session was established in the fast-path when stateful ICMP is enabled using the inspect icmp command.**  Recommended Action    None required.  Operation is Build (ICMP) |
| ASA-session-6-302021 | Error Message    %PIX|ASA-6-302021: **Teardown** ICMP connection for faddr {faddr |  icmp\_seq\_num} gaddr {gaddr |cmp\_type} laddr laddr  Explanation    **An ICMP session was removed in the fast-path when stateful ICMP is enabled using the inspect icmp command.**  Recommended Action    None required.  Operation is Teardown (ICMP) |
| ASA-session-0-106100 | Error Message    %PIX|ASA-6-106100: access-list acl\_ID {permitted | denied |  est-allowed} protocol interface\_name/source\_address(source\_port) ->  interface\_name/dest\_address(dest\_port) hit-cnt number ({first hit |  number-second interval}) hash codes  Explanation    **This message is generated any time that a packet is seen that does not match an existing connection on the security appliance. The message indicates either the initial occurrence or the total number of occurrences during an interval. This message provides more information than message 106023, which only logs denied packets, and does not include the hit count or a configurable level.**  When an access-list line has the log argument, it is expected that this syslog ID might be triggered because of a non-synchronized packet reaching the security appliance and being evaluated by the access-list. For example, if an ACK packet is received on the security appliance (for which no TCP connection exists in the connection table), the device might generate syslog 106100, indicating that the packet was permitted; however, the packet is later correctly dropped because of no matching connection.  The following list describes the message values:  Explanation    permitted | denied | est-allowed —These values specify if the packet was permitted or denied by the ACL. If the value is est-allowed, the packet was denied by the ACL but was allowed for an already established session (for example, an internal user is allowed to accesss the Internet, and responding packets that would normally be denied by the ACL are accepted).  Operation is permitted |
| ASA-session-4-106023 | Error Message    %PIX|ASA-4-106023: Deny *protocol* src  [interface\_name:source\_address/source\_port] dst  interface\_name:dest\_address/dest\_port [type {string}, code {code}] by  access\_group acl\_ID  Explanation    **A real IP packet was denied by the ACL. This message displays even if you do not have the log option enabled for an ACL.**  **Recommended Action    If messages persist from the same source address, messages might indicate a foot-printing or port-scanning attempt. Contact the remote host administrators.**  Operation is deny |
| ASA-session-4-405001 | Error Message    %PIX|ASA-4-405001: Received ARP {request | response} collision from  IP\_address/MAC\_address on interface interface\_name to IP\_address/MAC\_address on  interface interface\_name  Explanation    **The security appliance received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.**  **Recommended Action    This traffic might be legitimate, or it might indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and check to see if it belongs to a valid host.**  The operation is empty |
| ASA-ssl-6-725007 | Error Message    %ASA-6-725007 SSL session with remote\_device interface\_name: IP\_address/port  terminated.  Explanation    The SSL session has terminated.  •https://www.cisco.com/en/US/i/templates/blank.gifremote\_device—Either the server or the client depending on the device that initiates the connection.  •https://www.cisco.com/en/US/i/templates/blank.gifinterface\_name—The interface that the SSL session is using.  •https://www.cisco.com/en/US/i/templates/blank.gifIP\_address—The remote device IP address.  •https://www.cisco.com/en/US/i/templates/blank.gifport—The remote device IP port number.  Recommended Action    None required. |
| ASA-sys-6-606002 | 606002  Error Message    %PIX|ASA-6-606002: ASDM session number number from IP\_address ended  Explanation    This message indicates that a ASDM session ended.  Recommended Action    None required. |
| ASA-sys-6-606004 | Error Message    %PIX|ASA-6-606004: ASDM logging session number id from IP\_address ended  Explanation    An ASDM logging connection is terminated.  •https://www.cisco.com/en/US/i/templates/blank.gifid—session ID assigned  •https://www.cisco.com/en/US/i/templates/blank.gifIP\_address—IP address of remote management client  Recommended Action    No action is required from the user. |

**Destination Service**

Name of the service associate with the destination port such as UDP, TCP, ICMP, etc.