

Appendix A

Adaptive Services PIC System Log Messages

This appendix describes messages generated by the Adaptive Services PIC (AS PIC) and the services that run on it, including stateful firewall, Network Address Translation, and intrusion detection. It has the following sections:

System Log Message Fields on page 281

System Log Message Severity Levels on page 282

Startup System Log Messages on page 283

Authentication and Login System Log Messages on page 283

Policy Change System Log Messages on page 285

Policy Lookup System Log Messages on page 286

NAT-related System Log Messages on page 289

Hacker Defense System Log Messages on page 289

Intrusion Detection System Log Messages on page 296

ALG-related System Log Messages on page 297

System Log Message Fields

Each system log message is composed of the following fields:

Date—The time when the system logging utility received the message.

Example: Jun 11 14:36:60

PIC location—The physical location of the PIC that generated the message.

Example: (FPC Slot 1, PIC Slot 3)

Service set name—The service set that generated the message.

Example: {smartbits}

Service name—The service that generated the message.

Example: [FWNAT]

Message contents—The message, which can be freely formatted text or can contain the following fields:

IP protocol—The IP protocol string and value of the packet received.

Example: IP proto TCP (6)

ALG (application-level gateway protocol)—The ALG that matches the packet.

Example: ALG (ftp)

IP and port information—The source and destination fields of the packet.

Example: 10.58.255.34:8610 -> 10.58.255.162:21

Message string—A text description of the message.

Example: SFW rules request packet to be accepted; attempting to create forward or watch flow

The following is an example of a message logged to the `/var/log/messages` file:

```
Jun 11 14:36:50 (FPC Slot 1, PIC Slot 3) {smartbits} [FWNAT]: IP proto TCP (6) ALG (ftp),  
10.58.255.34:8610 -> 10.58.255.162:21, 10.100.1.1:1029 SFW rules request packet to  
be accepted; attempting to create forward or watch flow; NAT rules require source address  
and port translation to 10.100.1.1:1029
```

System Log Message Severity Levels

Table 13 lists the severity levels that the AS PIC assigns to system log messages.

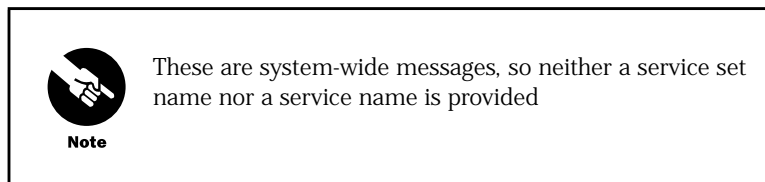
Table 13: System Log Message Severity Levels

Severity Level	Description
emergency (LOG_EMERG)	A PIC-wide failure, such as reboot.
critical (LOG_CRIT)	A critical condition that affects a complete service set, such as a policy change or removal.
error (LOG_ERR)	An intrusion detected by the intrusion detection system (this level is reserved for intrusion detection services).
warning (LOG_WARNING)	A service-level transient error condition that might not be tracked by the intrusion detection system (for example, the pool of NAT address/ports is exhausted).
notice (LOG_NOTICE)	A firewall dropped a packet (for example, header integrity check failure, stateful firewall rule drops, TCP reconstructor failures); the intrusion detection system always tracks messages with this severity.
info (LOG_INFO)	Events or nonerror conditions of interest (for example, creation of a new flow based on firewall rules, flow termination due to timeout, allocation of a NAT port from the given NAT pool); some messages with this severity are also tracked by the intrusion detection system.
debug	Reserved.

We recommend setting the system logging severity level to LOG_ERR during normal operation. To monitor PIC resource usage, set the level to LOG_WARNING. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to LOG_NOTICE for a specific service set. To debug a configuration or log NAT functionality, set the level to LOG_INFO.

Startup System Log Messages

The following messages are generated when the Adaptive Services PIC goes online.



EID_SYS_ONLINE

System Log Message	PIC online and initial configuration received
Description	The Adaptive Services PIC is online and ready to process traffic.
Type	Event: This message reports an event, not an error.
Severity	notice

Authentication and Login System Log Messages

The following messages are generated when a user or administrator logs into the router.



Note

These are system-wide messages, so neither a service set name nor a service name is provided

EID_SSH_LOGIN_ACCEPT

System Log Message Accepted password for *username* from *address* port *port-number*

Description The ssh process (sshd) reports login success.

Type Event: This message reports an event, not an error.

Severity info

EID_LOGIN_ACCEPT

System Log Message login on *tty* as *username*

Description The login process reports login success.

Type Event: This message reports an event, not an error.

Severity info

EID_SSH_LOGIN_FAILED

System Log Message Failed password for *username* from *address* port *port-number*

Description The ssh process (sshd) reports login failure.

Type Event: This message reports an event, not an error.

Severity notice

EID_LOGIN_FAILED

System Log Message *n* LOGIN FAILURES ON *tty*

Description The login process reports login failure.

Type Event: This message reports an event, not an error.

Severity notice

EID_START_AUTHEN

System Log Message	tac_send_authen:
Description	The login or ssh process starts to authenticate user login.
Type	Event: This message reports an event, not an error.
Severity	info

EID_AUTHEN_ERROR

System Log Message	Authentication service cannot retrieve authentication info
Description	The login or ssh process is unable to retrieve authentication info.
Type	Event: This message reports an event, not an error.
Severity	notice

EID_AUTHEN_FAILURE

System Log Message	Authentication failure
Description	Authentication has failed.
Type	Event: This message reports an event, not an error.
Severity	notice

Policy Change System Log Messages

The following messages are generated when the service policy changes.

EID_FW_TIMER_CHANGE

System Log Message	{ <i>service-set</i> } [FWNAT]: change global inactivity timer to <i>inactivity-timeout</i> and open timeout to <i>open-timeout</i>
Description	The global inactivity timer or open timer is changed by the user through a configuration commit. If the global inactivity timer or open timeout value is not set by the user, the word default appears instead of numbers in the <i>inactivity-timeout</i> and <i>open-timeout</i> fields.
Type	Event: This message reports an event, not an error.
Severity	critical

EID_SYS_CONFIG_DELETE

System Log Message { *service-set* } [SYSTEM]: service set is deleted

Description A policy is successfully deleted through a configuration commit.

Type Event: This message reports an event, not an error.

Severity critical

EID_SYS_CONFIG_DELETE_ERROR

System Log Message { *service-set* } [SYSTEM]: deletion of service set failed because rule memory was exceeded

Description A policy is not successfully deleted because of memory resources.

Type Event: This message reports an event, not an error.

Severity critical

Cause Rule memory is exhausted. In this case the system memory utilization is very high.

Action Wait some time for the system to reclaim memory or forcibly free up memory by deleting active flows. Resources are divided among service sets. Consider partitioning the configuration into more service sets. Otherwise, contact your technical support representative.

EID_SYS_CONFIG_ERROR

System Log Message { *service-set* } [SYSTEM]: reject configuration because of unknown action

Description A policy is downloaded but not installed because of an error.

Type: Error: An error occurred.

Severity critical

Cause An internal software failure occurred.

Action Contact your technical support representative.

EID_SYS_CONFIG_INSTALL

System Log Message { *service-set* } [SYSTEM]: install new configuration

Description A policy is successfully downloaded and installed through a configuration commit.

Type Event: This message reports an event, not an error.

Severity critical

Policy Lookup System Log Messages

When a packet reaches the Adaptive Services PIC and no existing flow has been established for the packet, the system performs a stateful firewall policy lookup. If a matching term is found, a system log message is generated, along with the matching term's action, which can be accept, reject, or discard.

If no matching firewall term is found, a system log message is generated for this event, and the incoming packet is dropped.

EID_FW_NO_POLICY_ERROR

System Log Message { *service-set* } [*service*]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, No policy

Description No matching policy is found because of an error.

Type Error: An error occurred.

Severity critical

Cause An internal software failure occurred.

Action Contact your technical support representative.

EID_FW_NO_RULE_DROP

System Log Message { *service-set* } [*service*]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, No matching SFW rule; attempting to create discard flow

Description The stateful firewall's rules have no matching action. If no match is found, the default rule is discard.

Type Event: This message reports an event, not an error.

Severity notice

EID_FW_RULE_ACCEPT

System Log Message { *service-set* } [*service*]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW rules request packet to be accepted; attempting to create forward or watch flow; NAT rules require source address and port translation to rules request packet to be accepted; attempting to create forward or watch flow; NAT rules require source address and port translation to *translated-address:port*

Description The matching action is accepted for a new flow. The NAT policy is analyzed for a matching NAT term. If one is found, the NAT translation information is appended to the system log accept message. If NAT translation is not necessary, no NAT information appears in the system log accept message.

Type Event: This message reports an event, not an error.

Severity info

Example The following is an example of a TCP rule accept system log. NAT is also configured:

```
Jun 24 17:02:23 (FPC Slot 0, PIC Slot 3) {ids_test}[FWNAT]: IP proto 6 (TCP) application (any), 10.62.1.1:2308 -> 10.62.2.2:23, SFW rules request packet to be accepted; attempting to create forward or watch flow; NAT rules require source address and port translation to 10.62.101.50:1026
```

EID_FW_RULE_DROP

System Log Message { *service-set* } [*service*]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW rules request packet to be discarded; attempting to create discard flow

Description The stateful firewall's rules have a matching action for discard. The default rule, if no match is found, is discard.

Type Event: This message reports an event, not an error.

Severity notice

EID_FW_RULE_PROMO_ERROR

System Log Message { *service-set* } [*service*]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, ALG promotion failed. SFW ALG *application-protocol* conflicts with NAT ALG *application-protocol*; request creation of discard flow

Description A matching application protocol (ALG) is found from both a firewall rule and a NAT rule, but the two ALGs are not at the same level.

Type Error: An error occurred.

Severity critical

Action Resolve the conflicting *application-protocol* matching conditions in the corresponding rules in the configuration.

EID_FW_RULE_REJECT

- System Log Message** { *service-set* } [*service*]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW rules request packet to be rejected; attempting to create reject flow
- Description** The stateful firewall's rules have a matching action for reject. For UDP flows, an ICMP error is generated. For TCP flows, a TCP RST is generated.
- Type** Event: This message reports an event, not an error.
- Severity** notice
- Example** The following are examples of discard and reject messages.
- Jun 24 18:59:51 (FPC Slot 0, PIC Slot 3) {ids_test} [FWNAT]: proto 6 (TCP), 10.62.0.2:3000 -> 10.62.2.2:3000, SFW rules request packet to be discarded; attempting to create discard flow
- Jun 24 19:00:52 (FPC Slot 0, PIC Slot 3) {ids_test} [FWNAT]: proto 6 (TCP), 10.62.0.2:3000 -> 10.62.2.2:3000, SFW rules request packet to be rejected; attempting to create reject flow

NAT-related System Log Messages

A NAT port allocation message is generated along with the firewall accept message.

EID_NAT_NO_PORTS

- System Log Message** { *service-set* } [NAT]: natpool *natpool* is out of ports
- Description** The NAT pool fails to allocate a port.
- Type** Event: This message reports an event, not an error.
- Severity** warning
- Action** Change the configuration to allow more ports or add more NAT pools if this occurs frequently.

EID_NAT_PORT_RELEASE

- System Log Message** { *service-set* } [NAT]: natpool release *address: port* [*num-ports*]
- Description** A port is returned to a NAT pool.
- Type** Event: This message reports an event, not an error.
- Severity** info

Hacker Defense System Log Messages

All packets passing through the stateful firewall are subject to a packet-level sanity check. All packets that fail sanity checks are logged.

EID_ICMP_HEADER_LEN_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:id* -> *destination*, ICMP header length check failed

Description An ICMP packet is discarded because it fails a header-length check.

Type Event: This message reports an event, not an error.

Severity notice

EID_ICMP_PACKET_ERROR_LENGTH

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:id* -> *destination*, ICMP packet length greater than 64K

Description An ICMP packet is discarded because it is longer than 64 KB.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_FRAGMENT_ASSEMBLY_TIMEOUT

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP fragment assembly timeout

Description Not all of the fragments are received within four seconds and all related fragments are discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_FRAGMENT_OVERLAP

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP fragment overlap

Description An IP fragment overlaps with another one and all related fragments are discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_CHECKSUM_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*),
source:port -> *destination:port*, IP packet with checksum error

Description An IP packet is discarded because it has a checksum error.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_DST_BROADCAST

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*),
source:port -> *destination:port*, IP packet with broadcast destination address

Description An IP packet is discarded because it has a broadcast destination address.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_FRAGMENT_LENGTH_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*),
source:port -> *destination:port*, IP fragment length error

Description An IP fragment has the wrong length and all related fragments are discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_INCORRECT_LENGTH

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*),
source:port -> *destination:port*, IP packet with incorrect length

Description An IP packet is discarded because it has an incorrect length.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_LAND_ATTACK

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, Land attack (IP src address = dest address)

Description An IP packet is discarded because it has an equal source and destination address, indicating a Land attack.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_NOT_VERSION_4

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP packet with version other than 4

Description An IP packet is discarded because its version is not IPv4.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_PROTOCOL_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP packet protocol error

Description An IP packet is discarded because it has a protocol error.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_SRC_BAD

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP packet with bad source address

Description An IP packet is discarded because it has a bad source address.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_TOO_LONG

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP packet length greater than 64K

Description An IP packet is discarded because it is longer than 64 KB.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_TOO_SHORT

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP packet too short

Description An IP packet is discarded because it is too short.

Type Event: This message reports an event, not an error.

Severity notice

EID_IP_PACKET_TTL_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, IP packet with TTL equal to 0

Description An IP packet is discarded because the TTL is equal to 0.

Type Event: This message reports an event, not an error.

Severity notice

EID_SMURF_ATTACK

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination*, Smurf attack (ping to IP broadcast address)

Description A Smurf attack is detected and is discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_SYN_DEFENSE

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW SYN defense

Description A duplicated SYN is received for an existing flow and is discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_TCP_FLAGS_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, TCP FIN/RST or SYN/(URG|FIN|RST) flags set

Description A TCP packet is discarded because it has the FIN and RST flags set, or because SYN is set and one or more of the URG, FIN, or RST flags are set.

Type Event: This message reports an event, not an error.

Severity notice

EID_TCP_HEADER_LEN_ERROR

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, TCP header length check failed

Description The TCP packet is discarded because it failed the header length check.

Type Event: This message reports an event, not an error.

Severity notice

EID_TCP_NON_SYN_FIRST_PACKET

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, First packet of TCP session not SYN

Description The first packet of a TCP session is not SYN and is discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_TCP_PORT_ZERO

- System Log Message** { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, TCP source or destination port zero
- Description** A TCP packet is discarded because it has a source or destination port equal to zero.
- Type** Event: This message reports an event, not an error.
- Severity** notice

EID_TCP_SEQNUM_AND_FLAGS_ZERO

- System Log Message** { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, TCP seq number zero and no flags set
- Description** A TCP packet is discarded because it has a zero sequence number and no flags set.
- Type** Event: This message reports an event, not an error.
- Severity** notice

EID_TCP_SEQNUM_ZERO_FLAGS_SET

- System Log Message** { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, TCP seq number zero and FIN/PSH/RST flags set
- Description** A TCP packet is discarded because it has a zero sequence number and one or more of the FIN, PSH, or RST flags are set.
- Type** Event: This message reports an event, not an error.
- Severity** notice

EID_UDP_HEADER_LEN_ERROR

- System Log Message** { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, UDP header length check failed
- Description** A UDP packet is discarded because it fails a header length check.
- Type** Event: This message reports an event, not an error.
- Severity** notice

EID_UDP_PORT_ZERO

- System Log Message** { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, UDP source or destination port zero
- Description** A UDP packet is discarded because it has a source or destination port equal to zero.
- Type** Event: This message reports an event, not an error.
- Severity** notice

Intrusion Detection System Log Messages

In addition to the stateful firewall, the intrusion detection system provides some extra security checks and logs any violations.

EID_FW_UDP_SCAN

- System Log Message** { *service-set* } [IDS]:dest *destination*, UDP port scan (port not in LISTEN state) ... rate= *rate* events/s
- Description** A UDP port scan has been detected by the intrusion detection system and is above the configured events-per-second threshold.
- Type** Event: This message reports an event, not an error.
- Severity** error

EID_IDS_SYN_PROTECTION_MEMORY_ERROR

- System Log Message** { *service-set* } [IDS]: dest *destination*, host *destination*, SYNCOOKIE protection activated FAILED
- Description** The SYN cookie protection activation has failed because of resource limitations.
- Type** Event: This message reports an event, not an error.
- Severity** error
- Action** Wait some time for the system to reclaim memory or forcibly free up memory by deleting active flows. Resources are divided among service sets. Consider partitioning the configuration into more service sets. Otherwise, contact your technical support representative.

EID_IDS_SYN_PROTECTION_OFF

- System Log Message** { *service-set* } [IDS]: dest *destination*, host *destination*, SYNCOOKIE protection deactivated
- Description** The SYN cookie protection has been deactivated.
- Type** Event: This message reports an event, not an error.
- Severity** error

EID_IDS_SYN_PROTECTION_ON

System Log Message { *service-set* } [IDS]: dest *destination* , host *destination* , SYNCOOKIE protection activated

Description The SYN cookie protection has been activated.

Type Event: This message reports an event, not an error.

Severity error

EID_TCP_BAD_SYN_COOKIE_RESPONSE

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, Bad SYN cookie response or 1st packet is ACK

Description SYN cookie defense is enabled and a bad SYN cookie response is received, or the first packet of the session is ACK and is discarded.

Type Event: This message reports an event, not an error.

Severity notice

EID_TCP_SCAN

System Log Message { *service-set* } [IDS]: dest *destination* , TCP port scan (port not in LISTEN state) ... rate = *rate* events/s

Description A TCP port scan has been detected by the intrusion detection system and is over the configured events-per-second threshold.

Type Event: This message reports an event, not an error.

Severity error

EID_TCP_SYN_ATTACK

System Log Message { *service-set* } [IDS]: dest *destination* , TCP SYN flood attack ... rate= *rate* events/s

Description A SYN flood attack has been detected by the intrusion detection system and is over the configured events-per-second threshold.

Type Event: This message reports an event, not an error.

Severity error

ALG-related System Log Messages

Application-level gateway protocols (ALGs) have system log messages that follow the general message format. TCP-based ALGs typically require the ALG to scan the TCP stream, looking for the embedded IP address and port number information. The scanning process is called TCP reconstruction.

EID_FTP_ACTIVE_ACCEPT

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW rules request FTP active mode data packets to be accepted; attempting to create forward flow

Description As part of an FTP conversation, the active mode data channel is accepted.

Type Event: This message reports an event, not an error.

Severity notice

EID_FTP_PASSIVE_ACCEPT

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW rules request FTP passive mode data packets to be accepted; attempting to create forward flow

Description As part of an FTP conversation, the passive mode data channel is accepted.

Type Event: This message reports an event, not an error.

Severity notice

EID_FW_APP_MSG_TOO_LONG

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port* -> *destination:port*, SFW application message too long

Description A TCP packet that is being watched has exhausted memory resources and is discarded.

Type Event: This message reports an event, not an error.

Severity notice

Action Wait some time for the system to reclaim memory or forcibly free up memory by deleting active flows. Resources are divided among service sets. Consider partitioning the configuration into more service sets. Otherwise, contact your technical support representative.

EID_PING_DUPLICATED_SEQNO

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:id -> destination*, ICMP echo request dropped, because sequence number duplicated

Description An ICMP echo request is discarded because it has a duplicated sequence number.

Type Event: This message reports an event, not an error.

Severity notice

EID_PING_MISMATCHED_SEQNO

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:id -> destination*, ICMP echo reply dropped, no matching sequence number

Description An ICMP echo reply is discarded because it has no corresponding echo request.

Type Event: This message reports an event, not an error.

Severity notice

EID_PING_OUTOF_SEQNO_CACHE

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:id -> destination*, ICMP echo request dropped, too many echo requests without echo reply

Description An ICMP echo request is discarded because there are too many outstanding echo requests without an echo reply.

Type Event: This message reports an event, not an error.

Severity notice

EID_TCP_RECONSTRUCT_DROP

System Log Message { *service-set* } [FWNAT]: IP proto *protocol* (*protocol-name*) application (*application-protocol*), *source:port -> destination:port*, SFW dropping TCP watch packet

Description A TCP packet that is being watched violates the TCP protocol and is discarded.

Type Event: This message reports an event, not an error.

Severity notice

