



## Syslog Messages 776201 to 8300006

---

This chapter contains the following sections:

- [Messages Messages 776201 to 780004, on page 1](#)
- [Messages 802005 to 880001 and 8300001 to 8300006, on page 10](#)

### Messages Messages 776201 to 780004

This section includes messages from 776201 to 780004.

#### 776201

**Error Message** %ASA-4-776201: CTS PAC: CTS PAC for Server *IP\_address* , A-ID *PAC issuer name* will expire in *number* days

**Explanation** A CTS PAC is nearing its expiration date.

**Recommended Action** Obtain a new PAC and import it.

#### 776202

**Error Message** %ASA-3-776202: CTS PAC for Server *IP\_address* , A-ID *PAC issuer name* has expired

**Explanation** A CTS PAC has expired.

**Recommended Action** Obtain a new PAC and import it.

#### 776203

**Error Message** %ASA-3-776203: Unable to retrieve CTS Environment data due to: *reason*

**Explanation** The ASA was unable to retrieve the CTS environment data and SGT name table for one of the following reasons:

- PAC has expired
- PAC data not available
- Error response from ISE
- Unable to retrieve server secret from the PAC

- Database error
- Invalid SG info value received
- Unable to add SG tag to database
- Error closing database
- Database update aborted

**Recommended Action** If this message persists, contact the Cisco TAC for assistance.

## 776204

**Error Message** %ASA-3-776204: CTS Environment data has expired

**Explanation** The CTS environment data and SGT name table have expired, which is likely to occur after unresolved environment data retrieval failures have occurred.

**Recommended Action** If this message persists, contact the Cisco TAC for assistance.

## 776251

**Error Message** %ASA-6-776251: CTS SGT-MAP: Binding *binding IP - SGname (SGT)* from *source name* added to binding manager.

**Explanation** Binding from the specified source was added to the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

**Recommended Action** None required.

## 776252

**Error Message** %ASA-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding *binding IP - SGname (SGT)* from *source name* deleted from binding manager.

**Explanation** Binding from the specified source was deleted from the binding manager.

Binding from the specified source was added to the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

**Recommended Action** None required.

## 776253

**Error Message** %ASA-6-776253: CTS SGT-MAP: Binding *binding IP - new SGname (SGT)* from *new source name* changed from old sgt: *old SGname (SGT)* from old source *old source name* .

**Explanation** A particular IP to SGT binding has changed in the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *new SGname (SGT)*—New binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *new source name* —Name of the new contributing source.
- *old SGname (SGT)*—Old binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *old source name* —Name of the old contributing source.

**Recommended Action** None required.

## 776254

**Error Message** %ASA-3-776254: CTS SGT-MAP: Binding manager unable to *action* binding *binding IP* - *SGname (SGT)* from *source name*.

**Explanation** The binding manager cannot insert, delete, or update the binding

- *action*— Binding manager operation. Either insert, delete or update.
- *binding IP* —IPv4 or IPv6 binding address.
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

**Recommended Action** Contact the Cisco TAC for assistance.

## 776301

**Error Message** %ASA-7-776301: CTS Policy: Security-group tag *sgt* is mapped to security-group name "*sgname* "

**Explanation** The security group tag referenced in the policy is known and the lookup in the security group table is successful. As a result, the tag name mapping is derived.

- *sgt* —Security group tag referenced in the policy
- *sgname* —Security group name mapping derived from the table

**Recommended Action** None required.

## 776302

**Error Message** %ASA-7-776302: CTS Policy: Unknown security-group tag *sgt* referenced in policies

**Explanation** The security group tag referenced in the policy was unknown and the lookup in the security group table failed. However, the policy referencing the tag can still be enforced.

- *sgt* —Security group tag referenced in the policy

**Recommended Action** Check to see if the security group tag exists in the ISE. If the tag exists, it will become known after the next refresh. If the tag does not exist in the ISE, consider removing all associated policies on the ASA.

## 776303

**Error Message** %ASA-6-776303: CTS Policy: Security-group name "*sgname*" is resolved to security-group tag *sgt*

**Explanation** The securitygroup name referenced in the policy was resolved and the lookup in the security group table was successful. As a result, the tag derived from the table is used for policy enforcement.

- *sgname* —Security group name referenced in the policy
- *sgt* —Security group tag mapping derived from the table

**Recommended Action** None required.

## 776304

**Error Message** %ASA-4-776304: CTS Policy: Unresolved security-group name "*sgname*" referenced, policies based on this name will be inactive

**Explanation** The securitygroup name referenced in the policy cannot be resolved to a tag and the lookup in the security group table failed. AS a result, the policy referencing the name is inactive, but remains in the configuration.

- *sgname* —Security group name referenced in the policy

**Recommended Action** Check to see if the security group name exists in the ISE. If the name exists, the table can be refreshed so the name gets resolved and policies can be enforced. If the name does not exist in the ISE, consider removing all associated policies on the ASA.

## 776305

**Error Message** %ASA-4-776305: CTS Policy: Security-group table cleared, all polices referencing security-group names will be deactivated

**Explanation** The security group table downloaded from the ISE is cleared on the ASA and policies based on security group tags continue to be enforced. However, policies based on names become inactive, but remain in the configuration.

**Recommended Action** Refresh the security group table on the ASA so all policies based on security group names can be enforced.

## 776307

**Error Message** %ASA-7-776307: CTS Policy: Security-group name for security-group tag *sgt* renamed from *old\_sgname* " to "*new\_sgname* "

**Explanation** In the newly downloaded security group table on the ASA, a change in the security group name for a security group tag was detected; however, there was no change in policy status.

- *sgt* —Security group tag referenced in the policy
- *old\_sgname* —Old security group name
- *new\_sgname* —New security group name

**Recommended Action** None required.

## 776308

**Error Message** %ASA-7-776308: CTS Policy: Previously unknown security-group tag *sgt* is now mapped to security-group name "*sgname* "

**Explanation** In the newly downloaded security group table on the ASA, a previously unknown security group tag was found in the table; however, there was no change in policy status.

- *sgt* —Security group tag referenced in the policy
- *sgname* —Security group name derived from the new security group table

**Recommended Action** None required.

## 776309

**Error Message** %ASA-5-776309: CTS Policy: Previously known security-group tag *sgt* is now unknown

**Explanation** In the newly downloaded security group table on the ASA, a previously known security group tag no longer exists. There is no change in policy status, and the policy can still be enforced.

- *sgt* —Security group tag referenced in the policy

**Recommended Action** If the security group tag does not exist in the new table, the security group has been removed in the ISE. Consider removing all policies that reference the tag.

## 776310

**Error Message** %ASA-5-776310: CTS Policy: Security-group name "*sgname* " remapped from security-group tag *old\_sgt* to *new\_sgt*

**Explanation** In the newly downloaded security group table on the ASA, a change in the security group tag for a security group name was detected. All policies referencing the name are updated to reflect the new tag, and policies are enforced based on the new tag.

- *sgname* —Security group name referenced in the policy
- *old\_sgt* —Old security group tag
- *new\_sgt* —New security group tag

**Recommended Action** Because of the change in tag value, make sure that the configured policies are still accurate.

## 776311

**Error Message** %ASA-6-776311: CTS Policy: Previously unresolved security-group name "*sgname* " is now resolved to security-group tag *sgt*

**Explanation** In the newly downloaded security group table on the ASA, a previously unresolved security group name was resolved to a tag, and the new tag can be used to enforce policies.

- *sgname* —Security group name referenced in the policy
- *sgt* —Security group tag derived from the new security group table

**Recommended Action** None required.

## 776312

**Error Message** %ASA-4-776312: CTS Policy: Previously resolved security-group name "*sgname*" is now unresolved, policies based on this name will be deactivated

**Explanation** In the newly downloaded security group table on the ASA, a previously resolved security group name no longer exists. As a result, all policies based on this security group name become inactive, but remain in the configuration.

- *sgname* —Security group name referenced in the policy

**Recommended Action** If the security group name does not exist in the new table, the security group has been removed in the ISE. Check the policy configuration on the ASA, consider removing policies referencing the name.

## 776313

**Error Message** %ASA-3-776313: CTS Policy: Failure to update policies for security-group "*sgname*"-*sgt*

**Explanation** An error was encountered in updating the policies. Policy enforcement will continue based on old tag values and is no longer accurate.

- *sgname* —Security group name that has a change in tag value
- *sgt* —New security group tag value

**Recommended Action** To reflect the correct tag value, remove all policies referencing the security group name and reapply them. If the error persists, contact the Cisco TAC for assistance.

## 778001

**Error Message** %ASA-6-778001: VXLAN: Invalid VXLAN segment-id *segment-id* for protocol from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port).

**Explanation** The Secure Firewall ASA tries to create an inner connection for a VXLAN packet, but the VXLAN packet has an invalid segment ID.

**Recommended Action** None required.

## 778002

**Error Message** %ASA-6-778002: VXLAN: There is no VNI interface for segment-id *segment-id* .

**Explanation** A decapsulated ingress VXLAN packet is discarded, because the segment ID in the VXLAN header does not match the segment ID of any VNI interface configured on the Secure Firewall ASA.

**Recommended Action** None required.

## 778003

**Error Message** %ASA-6-778003: VXLAN: Invalid VXLAN segment-id *segment-id* for protocol from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port) in FP.

**Explanation** The Secure Firewall ASA Fast Path sees a VXLAN packet with an invalid segment ID.

**Recommended Action** Check the VNI interface segment ID configurations to see if the dropped packet has the VXLAN segment ID that does not match any VNI segment ID configuration.

## 778004

**Error Message** %ASA-6-778004: VXLAN: Invalid VXLAN header for *protocol* from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port) in FP.

**Explanation** The Secure Firewall ASA VTEP sees a VXLAN packet with an invalid VXLAN header.

**Recommended Action** None required.

## 778005

**Error Message** %ASA-6-778005: VXLAN: Packet with VXLAN segment-id *segment-id* from *ifc-name* is denied by FP L2 check.

**Explanation** A VXLAN packet is denied by a Fast Path L2 check.

**Recommended Action** Check the VNI interface segment ID configurations to see if the dropped packet has the VXLAN segment ID that does not match any VNI segment ID configuration. Check to see if the STS table has an entry that matches the dropped packet's segment ID.

## 778006

**Error Message** %ASA-6-778006: VXLAN: Invalid VXLAN UDP checksum from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port) in FP.

**Explanation** The Secure Firewall ASA VTEP received a VXLAN packet with an invalid UDP checksum value.

**Recommended Action** None required.

## 778007

**Error Message** %ASA-6-778007: VXLAN: Packet from *ifc-name* : IP-address/port to IP-address/port was discarded due to invalid NVE peer.

**Explanation** The Secure Firewall ASA VTEP received a VXLAN packet from an IP address that is different from the configured NVE peer.

**Recommended Action** None required.

## 779001

**Error Message** %ASA-6-779001: STS: Out-tag lookup failed for in-tag *segment-id* of *protocol* from *ifc-name* : IP-address /port to IP-address /port .

**Explanation** The Secure Firewall ASA tries to create a connection for a VXLAN packet, but failed to use the STS lookup table to locate the out-tag for the in-tag (segment ID) in the VXLAN packet.

**Recommended Action** None required.

## 779002

**Error Message** %ASA-6-779002: STS: STS and NAT locate different egress interface for segment-id *segment-id* , protocol from *ifc-name* :*IP-address* /*port* to *IP-address* /*port*

**Explanation** The Secure Firewall ASA tries to create a connection for a VXLAN packet, but the STS lookup table and NAT policy locate a different egress interface.

**Recommended Action** None required.

## 779003

**Error Message** %ASA-3-779003: STS: Failed to read tag-switching table - *reason*

**Explanation** The Secure Firewall ASA tried to read the tag-switching table, but failed.

**Recommended Action** None required.

## 779004

**Error Message** %ASA-3-779004: STS: Failed to write tag-switching table - *reason*

**Explanation** The Secure Firewall ASA tried to write to the tag-switching table, but failed.

**Recommended Action** None required.

## 779005

**Error Message** %ASA-3-779005: STS: Failed to parse tag-switching request from http - *reason*

**Explanation** The Secure Firewall ASA tried to parse the HTTP request to see what to do on the tag-switching table, but failed.

**Recommended Action** None required.

## 779006

**Error Message** %ASA-3-779006: STS: Failed to save tag-switching table to flash - *reason*

**Explanation** The Secure Firewall ASA tried to save the tag-switching table to flash memory, but failed.

**Recommended Action** None required.

## 779007

**Error Message** %ASA-3-779007: STS: Failed to replicate tag-switching table to peer - *reason*

**Explanation** The Secure Firewall ASA attempts to replicate the tag-switching table to the failover standby unit or clustering data units, but failed to do so.

**Recommended Action** None required.



## 780001

**Error Message** %ASA-6-780001: RULE ENGINE: Started compilation for access-group transaction - *description of the transaction* .

**Explanation** The rule engine has started compilation for an access group transaction. The description of the transaction is the command line input of the access group itself.

**Recommended Action** None required.

## 780002

**Error Message** %ASA-6-780002: RULE ENGINE: Finished compilation for access-group transaction - *description of the transaction* .

**Explanation** The rule engine has finished compilation for a transaction. Taking access group as an example, the description of the transaction is the command line input of the access group itself.

**Recommended Action** None required.

## 780003

**Error Message** %ASA-6-780003: RULE ENGINE: Started compilation for nat transaction - *description of the transaction* .

**Explanation** The rule engine has started compilation for a NAT transaction. The description of the transaction is the command line input of the **nat** command itself.

**Recommended Action** None required.

## 780004

**Error Message** %ASA-6-780004: RULE ENGINE: Finished compilation for nat transaction - *description of the transaction* .

**Explanation** The rule engine has finished compilation for a NAT transaction. The description of the transaction is the command line input of the **nat** command itself.

**Recommended Action** None required.

## 785001

**Error Message** %ASA-7-785001: Clustering: Ownership for existing flow from <in\_interface>:<src\_ip\_addr>/<src\_port> to <out\_interface>:<dest\_ip\_addr>/<dest\_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.

**Explanation** This syslog is generated when clustering moved the flow from one unit in one site to another unit in another site in inter-DC environment. Reason must be whatever triggered the move, such as LISP notification.

**Recommended Action** Verify the flow status in the new unit at new site.

## Messages 802005 to 880001 and 8300001 to 8300006

This section includes messages from 802005 to 880001 and 8300001 to 8300006.

### 802005

**Error Message** %ASA-6-802005: IP *ip\_address* Received MDM request *details*

**Explanation** A new MDM request has been received while the MDM proxy service is active.

**Recommended Action** None required.

### 802006

**Error Message** %ASA-4-802006: IP *ip\_address* MDM request *details* has been rejected: *details*

**Explanation** An MDM request has been rejected by the device.

**Recommended Action** None required.

### 803001

**Error Message** %ASA-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

**Explanation** Informational message to the user that the hardware bypass will be continued after bootup.

**Recommended Action** None required.

**Error Message** %ASA-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4

**Explanation** Informational message to the user that the hardware bypass will be continued after bootup.

**Recommended Action** None required.

### 803002

**Error Message** %ASA-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

**Explanation** Informational message to the user that hardware bypass is manually enabled.

**Recommended Action** None required.

**Error Message** %ASA-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4

**Explanation** Informational message to the user that hardware bypass is manually enabled.

**Recommended Action** None required.

## 803003

**Error Message** %ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2.

**Explanation** Informational message to the user that hardware bypass is manually disabled.

**Recommended Action** None required.

**Error Message** %ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/3-1/4.

**Explanation** Informational message to the user that hardware bypass is manually disabled.

**Recommended Action** None required.

## 804001

**Error Message** %ASA-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted

**Explanation** Informational message to the user about the online insertion of the supported SFP module.

**Recommended Action** None required.

## 804002

**Error Message** %ASA-6-804002: Interface GigabitEthernet1/3 SFP has been removed

**Explanation** Informational message to the user about removal of the supported SFP module.

**Recommended Action** None required.

## 805001

**Error Message** %ASA-6-805001: Flow offloaded: connection conn\_id  
outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port)  
inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol

**Explanation** Indicates flow is offloaded to the super-fast path.

**Recommended Action** None required.

## 805002

**Error Message** %ASA-6-805002: Flow is no longer offloaded: connection conn\_id  
outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port)  
inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol

**Explanation** Indicates flow offloading is disabled on a flow which was offloaded to the super-fast path.

**Recommended Action** None required.

## 805003

**Error Message** %ASA-6-805003: TCP Flow could not be offloaded for connection conn\_id from outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port) to inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) reason

**Explanation** Indicates flow could not be offloaded. For example, due to flow entry collision on the offload flow table.

**Recommended Action** None required.

## 806001

**Error Message** %ASA-6-806001: Primary alarm CPU temperature is High temperature

**Explanation** The CPU has reached temperature over primary alarm temperature setting for high temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806002

**Error Message** %ASA-6-806002: Primary alarm for CPU high temperature is cleared

**Explanation** The CPU temperature goes down to under primary alarm temperature setting for high temperature.

**Recommended Action** None required.

## 806003

**Error Message** %ASA-6-806003: Primary alarm CPU temperature is Low temperature

**Explanation** The CPU has reached temperature under primary alarm temperature setting for low temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806004

**Error Message** %ASA-6-806004: Primary alarm for CPU Low temperature is cleared

**Explanation** The CPU temperature goes up to over primary alarm temperature setting for low temperature.

**Recommended Action** None required.

## 806005

**Error Message** %ASA-6-806005: Secondary alarm CPU temperature is High temperature

**Explanation** The CPU has reached temperature over secondary alarm temperature setting for high temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806006

**Error Message** %ASA-6-806006: Secondary alarm for CPU high temperature is cleared

**Explanation** The CPU temperature goes down to under secondary alarm temperature setting for high temperature.

**Recommended Action** None required.

## 806007

**Error Message** %ASA-6-806007: Secondary alarm CPU temperature is Low temperature

**Explanation** The CPU has reached temperature under secondary alarm temperature setting for low temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806008

**Error Message** %ASA-6-806008: Secondary alarm for CPU Low temperature is cleared

**Explanation** The CPU temperature goes up to over secondary alarm temperature setting for low temperature.

**Recommended Action** None required.

## 806009

**Error Message** %ASA-6-806009: Alarm asserted for ALARM\_IN\_1 description

**Explanation** Alarm input port 1 is triggered.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806010

**Error Message** %ASA-6-806010: Alarm cleared for ALARM\_IN\_1 alarm\_1\_description

**Explanation** Alarm input port 1 is cleared.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** None required.

## 806011

**Error Message** %ASA-6-806011: Alarm asserted for ALARM\_IN\_2 description

**Explanation** Alarm input port 2 is triggered.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806012

**Error Message** %ASA-6-806012: Alarm cleared for ALARM\_IN\_2 alarm\_2\_description

**Explanation** Alarm input port 2 is cleared.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** None required.

## 812005

**Error Message** %ASA-4-812005: Link-State-Propagation activated on inline-pair due to failure of interface *interface-name* bringing down pair interface *interface-name*

**Explanation** This message is generated when the link state propagation is activated on the inline pair due to failure of an interface.

**Recommended Action** None.

## 812006

**Error Message** %ASA-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery of interface *interface-name* bringing up pair interface *interface-name*

**Explanation** This message is generated when the link state propagation is deactivated on the inline pair due to recovery of failed interface.

**Recommended Action** None.

## 812007

**Error Message** %ASA-6-812007: Inline-set hardware-bypass mode configuration *status*

**Explanation** This message is generated when the state (succeeded or failed) of hardware and software bypass modes for the IPS inline interfaces changes.

**Recommended Action** None.

## 815002

**Error Message** %ASA-2-815002: Denied packet, hard limit, 10000, for object-group search exceeded for UDP from source *IP address/port* to destination *IP address/port*

**Explanation** When object-group-search threshold (by default threshold is 10K) is configured in ASA, and if any OGS search crosses 10k limit, packets are dropped and this message is generated.

**Recommended Action** None.

## 815003

**Error Message** %ASA-4-815003: Object-Group-Search threshold exceeded *current value* threshold (10000) for packet UDP from *source IP address/port* to *destination IP address/port*

**Explanation** When object-group-search threshold is not configured in ASA, and if any OGS search crosses 10000 limit, packets are dropped and this message is generated.

**Recommended Action** None.

## 815004

**Error Message** %ASA-7-815004: OGS: Packet *protocol* from *source IP address/port* to *destination IP address/port* matched *number of source network objects* source network objects and *number of source network objects* destination network objects *total search entries* total number of entries. Resultant key-set has *number of entries* entries

**Explanation** This message is generated to provide a detailed information on the object group search entries:

- Source network object count
- Destination network object count
- Total search (product of source and destination count)
- Resultant Key-set value (to be queried in the ACL Lookup)

**Recommended Action** None.

## 840001

**Error Message** %ASA-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>

**Explanation** In the high-availability setup of distributed site-to-site VPN, an attempt to create a backup session is made when a IKEv2 session is established or when the cluster membership changes. However, the attempt may fail for reasons such as capacity limit. Hence this message is generated on the unit of a session owner whenever it is notified of failing to create a backup.

**Recommended Action** None.

## 850001

**Error Message** %ASA-3-850001: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to delay of <delay>ms (threshold <AAB-threshold>ms) with <connection-info>

**Explanation** The Automatic-Application-Bypass (AAB) event is triggered due to packet delay exceeding the AAB threshold.

**Recommended Action** Collect troubleshoot archive, snort core files and contact Cisco TAC.

## 850002

**Error Message** %ASA-3-850002: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to SNORT not responding to traffics for <timeout-delay>ms (threshold <AAB-threshold>ms)

**Explanation** The Automatic-Application-Bypass (AAB) event is triggered due to SNORT not responding to traffics for a period exceeding the AAB threshold.

**Recommended Action** Collect troubleshoot archive, snort core files and contact Cisco TAC.

## 870001

**Error Message** %ASA-4-870001: policy-route path-monitoring, remote peer *interface\_name:IP\_Address reachable\_status*

**Explanation** This message appears to display whether the interface on the policy based route identified through path monitoring is reachable or not:

- *reachable\_status*—reachable or unreachable

**Recommended Action** None required.

## 880001

**Error Message** %ASA-6-880001: *Ingress interface, for traffic source ipaddress to destination ipaddress, PBR picked outside interface 1 as its metric-type became better than outside interface 2*

**Explanation** This message is generated whenever the interface chosen is different from previous while forwarding the traffic. Where, metric-types are jitter, cost, mos, packet loss, rtt.

**Recommended Action** None.

## 8300001

**Error Message** %ASA-6-8300001: VPN session redistribution <variable 1>

**Explanation** These events notify the administrator that the operation related to ‘cluster redistribute vpn-sessiondb’ has started or completed. Where,

- <variable 1>—Action: started or completed

**Recommended Action** None.

## 8300002

**Error Message** %ASA-6-8300002: Moved <variable 1> sessions to <variable 2>

**Explanation** Provides details on how many active sessions were moved to another member of the cluster.



- <variable 1>— number of active sessions moved (this can be less than the number requested)
- <variable 2>—name of the cluster member the sessions where moved to

**Recommended Action** None.

## 8300003

**Error Message** %ASA-3-8300003: Failed to send session redistribution message to <variable 1>

**Explanation** There was an error sending a request to another cluster member. This could be due to an internal error or the cluster member the message was destined for is not available.

- <variable 1>— name of the cluster member the message was destined for

**Recommended Action** If this message is persistent contact customer support.

## 8300004

**Error Message** %ASA-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

**Explanation** This event is displayed when a member receives a request from the director to move a specific number of active sessions to another member in the group.

- <variable 1>—Action: Received, Sent
- <variable 2>—number of active sessions to move
- <variable 3>—name of member receiving the move session request
- <variable 4>—name of the member to receive the active sessions

**Recommended Action** None.

## 8300005

**Error Message** %ASA-3-8300005: Failed to receive session move response from <variable 1>

**Explanation** The director has requested a member to move active sessions to another member. If the director has not received a response to this request within a defined period, it will display this event and terminate the redistribution process.

- <variable 1>—name of member which failed to send a move response within timeout period

**Recommended Action** Re-issue the “cluster redistribute vpn-sessiondb” and if the problem persists, contact support.

## 8300006

**Error Message** %ASA-5-8300006: Cluster topology change detected. VPN session redistribution aborted.

**Explanation** The VPN session redistribution move calculations are based on the active members at the time the process is started. If a member joins or leaves during this process, the director will terminate the session redistribution.

**Recommended Action** Retry the operation when all of the members have joined or left the group.