



## Messages Listed by Severity Level

---

This appendix contains the following sections:

- [Alert Messages, Severity 1, page A-1](#)
- [Critical Messages, Severity 2, page A-3](#)
- [Error Messages, Severity 3, page A-5](#)
- [Warning Messages, Severity 4, page A-15](#)
- [Notification Messages, Severity 5, page A-23](#)
- [Informational Messages, Severity 6, page A-30](#)
- [Debugging Messages, Severity 7, page A-41](#)



**Note**

The Cisco ASA does not send severity 0, emergency messages to syslog. These are analogous to a UNIX panic message, and denote an unstable system.

---

### Alert Messages, Severity 1

The following messages appear at severity 1, alerts:

- %PIX|ASA-1-101001: (Primary) Failover cable OK.
- %PIX|ASA-1-101002: (Primary) Bad failover cable.
- %PIX|ASA-1-101003: (Primary) Failover cable not connected (this unit).
- %PIX|ASA-1-101004: (Primary) Failover cable not connected (other unit).
- %PIX|ASA-1-101005: (Primary) Error reading failover cable status.
- %PIX|ASA-1-102001: (Primary) Power failure/System reload other side.
- %PIX|ASA-1-103001: (Primary) No response from other firewall (reason code = code).
- %PIX|ASA-1-103002: (Primary) Other firewall network interface interface\_number OK.
- %PIX|ASA-1-103003: (Primary) Other firewall network interface interface\_number failed.
- %PIX|ASA-1-103004: (Primary) Other firewall reports this firewall failed.
- %PIX|ASA-1-103005: (Primary) Other firewall reporting failure.
- %PIX|ASA-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %PIX|ASA-1-104002: (Primary) Switching to STNDBY (cause: string).

- %PIXIASA-1-104003: (Primary) Switching to FAILED.
- %PIXIASA-1-104004: (Primary) Switching to OK.
- %PIXIASA-1-105001: (Primary) Disabling failover.
- %PIXIASA-1-105002: (Primary) Enabling failover.
- %PIXIASA-1-105003: (Primary) Monitoring on interface interface\_name waiting
- %PIXIASA-1-105004: (Primary) Monitoring on interface interface\_name normal
- %PIXIASA-1-105005: (Primary) Lost Failover communications with mate on interface interface\_name.
- %PIXIASA-1-105006: (Primary) Link status 'Up' on interface interface\_name.
- %PIXIASA-1-105007: (Primary) Link status 'Down' on interface interface\_name.
- %PIXIASA-1-105008: (Primary) Testing interface interface\_name.
- %PIXIASA-1-105009: (Primary) Testing on interface interface\_name {Passed|Failed}.
- %PIXIASA-1-105011: (Primary) Failover cable communication failure
- %PIXIASA-1-105020: (Primary) Incomplete/slow config replication
- %PIXIASA-1-105021: (failover\_unit) Standby unit failed to sync due to a locked context\_name config. Lock held by lock\_owner\_name
- %PIXIASA-1-105031: Failover LAN interface is up
- %PIXIASA-1-105032: LAN Failover interface is down
- %PIXIASA-1-105034: Receive a LAN\_FAILOVER\_UP message from peer.
- %PIXIASA-1-105035: Receive a LAN failover interface down msg from peer.
- %PIXIASA-1-105036: dropped a LAN Failover command message.
- %PIXIASA-1-105037: The primary and standby units are switching back and forth as the active unit.
- %PIXIASA-1-105038: (Primary) Interface count mismatch
- %PIXIASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %PIXIASA-1-105040: (Primary) Mate failover version is not compatible.
- %PIXIASA-1-105042: (Primary) Failover interface OK
- %PIXIASA-1-105043: (Primary) Failover interface failed
- %PIXIASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %PIXIASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %PIXIASA-1-105046 (Primary|Secondary) Mate has a different chassis
- %PIXIASA-1-105047: Mate has a io\_card\_name1 card in slot slot\_number which is different from my io\_card\_name2
- %ASA-1-105048: (unit) Mate's service module (application) is different from mine (application)
- %PIXIASA-1-106021: Deny protocol reverse path check from source\_address to dest\_address on interface interface\_name
- %PIXIASA-1-106022: Deny protocol connection spoof from source\_address to dest\_address on interface interface\_name

- %PIX|ASA-1-106101 The number of ACL log deny-flows has reached limit (number).
- %PIX|ASA-1-107001: RIP auth failed from IP\_address: version=number, type=string, mode=string, sequence=number on interface interface\_name
- %PIX|ASA-1-107002: RIP pkt failed from IP\_address: version=number on interface interface\_name
- %PIX|ASA-1-111111 error\_message
- %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error\_string).
- %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error\_string).
- %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error\_string).
- %ASA-n-216001: internal error in: function: message
- %ASA-1-216005: ERROR: Duplex-mismatch on interface\_name resulted in transmitter lockup. A soft reset of the switch was performed.
- %ASA|PIX-1-332004: Web Cache IP\_address/service\_ID lost
- %ASA-1-505015: SSM model Module in slot number, application up application, version version
- %PIX|ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %PIX|ASA-1-709004: (Primary) End Configuration Replication (ACT)
- %PIX|ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %PIX|ASA-1-709006: (Primary) End Configuration Replication (STB)

## Critical Messages, Severity 2

The following messages appear at severity 2, critical:

- %PIX|ASA-2-106001: Inbound TCP connection denied from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name
- %PIX|ASA-2-106002: protocol Connection denied by outbound list acl\_ID src inside\_address dest outside\_address
- %PIX|ASA-2-106006: Deny inbound UDP from outside\_address/outside\_port to inside\_address/inside\_port on interface interface\_name.
- %PIX|ASA-2-106007: Deny inbound UDP from outside\_address/outside\_port to inside\_address/inside\_port due to DNS {Response|Query}.
- %PIX|ASA-2-106013: Dropping echo request from IP\_address to PAT address IP\_address
- %PIX|ASA-2-106016: Deny IP spoof from (IP\_address) to IP\_address on interface interface\_name.
- %PIX|ASA-2-106017: Deny IP due to Land Attack from IP\_address to IP\_address
- %PIX|ASA-2-106018: ICMP packet type ICMP\_type denied by outbound list acl\_ID src inside\_address dest outside\_address
- %PIX|ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP\_address to IP\_address
- %PIX|ASA-2-106024: Access rules memory exhausted
- %PIX|ASA-2-108002: SMTP replaced string: out source\_address in inside\_address data: string

- %PIXIASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dset\_port. Data:string
- %PIXIASA-2-109011: Authen Session Start: user 'user', sid number
- %PIXIASA-2-112001: (string:dec) Clear complete.
- %ASA-2-113022: AAA Marking protocol server ip-addr in server group tag as FAILED
- %ASA-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
- %PIXIASA-2-201003: Embryonic limit exceeded nconns/elimit for outside\_address/outside\_port (global\_address) inside\_address/inside\_port on interface interface\_name
- %PIXIASA-2-214001: Terminating manager session from IP\_address on interface interface\_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %PIXIASA-2-215001:Bad route\_compress() call, sdb= number
- %ASA-n-216001: internal error in: function: message
- %PIXIASA-2-217001: No memory for string in string
- %PIXIASA-2-218001: Failed Identification Test in slot# [fail#/res].
- %PIXIASA-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %PIXIASA-2-218003: Module Version in <slot#> is obsolete. The module in slot = <slot#> is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.
- %PIXIASA-2-218004: Failed Identification Test in slot# [fail#/res]
- %PIXIASA-2-304007: URL Server IP\_address not responding, ENTERING ALLOW mode.
- %PIXIASA-2-304008: LEAVING ALLOW mode, URL Server is up.
- %PIXIASA-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src\_ifc:sip/sport to dest\_ifc:dip/dport
- %PIXIASA-2-709007: Configuration replication failed for command command
- %PIXIASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available\_size, used value
- %PIXIASA-2-713176: Device\_type memory resources are critical, IKE key acquire message on interface interface\_number, for Peer IP\_address ignored
- %ASA-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
- %ASA-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
- %ASA-2-716502: internal error in: function: Fiber library cannot allocate default arena
- %ASA-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
- %ASA-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
- %ASA-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
- %ASA-2-716507: internal error in: function: Fiber scheduler has reached unreachable code. Cannot continue terminating
- %ASA-2-716508: internal error in: function: Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating

- %ASA-2-716509: internal error in: function: Fiber scheduler is scheduling alien fiber. Cannot continue terminating
- %ASA-2-716510: internal error in: function: Fiber scheduler is scheduling finished fiber. Cannot continue terminating
- %ASA-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
- %ASA-2-716513: internal error in: function: Fiber in callback blocked on other channel
- %ASA-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
- %ASA-2-716516: internal error in: function: OCCAM has corrupted ROL array. Cannot continue terminating
- %ASA-2-716517: internal error in: function: OCCAM cached block has no associated arena
- %ASWA-2-716518: internal error in: function: OCCAM pool has no associated arena
- %ASA-2-716519: internal error in: function: OCCAM has corrupted pool list. Cannot continue terminating
- %ASA-2-716520: internal error in: function: OCCAM pool has no block list
- %ASA-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
- %ASA-2-716522: internal error in: function: OCCAM corrupted standalone block
- %ASA-2-716525: UNICORN\_SYSLOGID\_SAL\_CLOSE\_PRIVDATA\_CHANGED
- %ASA-2-716526: UNICORN\_SYSLOGID\_PERM\_STORAGE\_SERVER\_LOAD\_FAIL
- %ASA-2-716527: UNICORN\_SYSLOGID\_PERM\_STORAGE\_SERVER\_STORE\_FAIL
- %ASA-2-716528: Unexpected fiber scheduler error; possible out-of-memory condition
- %PIX|ASA-2-717008: Insufficient memory to process\_requiring\_memory.
- %PIX|ASA-2-717011: Unexpected event event event\_ID

## Error Messages, Severity 3

The following messages appear at severity 3, errors:

- %PIX|ASA-3-105010: (Primary) Failover message block alloc failed
- %PIX|ASA-3-106010: Deny inbound protocol src interface\_name:dest\_address/dest\_port dst interface\_name:source\_address/source\_port
- %PIX|ASA-3-106011: Deny inbound (No xlate) string
- %PIX|ASA-3-106014: Deny inbound icmp src interface\_name: IP\_address dst interface\_name: IP\_address (type dec, code dec)
- %PIX-3-107003: RIP: Attempted reference of stale data encountered in function, line: line\_num
- %PIX|ASA-3-109010: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (too many pending auths) on interface interface\_name.
- %PIX|ASA-3-109013: User must authenticate before using this service
- %PIX|ASA-3-109016: Can't find authorization ACL acl\_ID for user 'user'
- %PIX|ASA-3-109018: Downloaded ACL acl\_ID is empty
- %PIX|ASA-3-109019: Downloaded ACL acl\_ID has parsing error; ACE string
- %PIX|ASA-3-109020: Downloaded ACL has config error; ACE

- %PIXIASA-3-109023: User from source\_address/source\_port to dest\_address/dest\_port on interface outside\_interface must authenticate before using this service.
- %PIXIASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %PIXIASA-3-109032: Unable to install ACL access\_list, downloaded for user username; Error in ACE: ace.
- %PIXIASA-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %PIXIASA-3-113018: User: user, Unsupported downloaded ACL Entry: ACL\_entry, Action: action
- %PIXIASA-3-113020: Kerberos error : Clock skew with server ip\_address greater than 300 seconds
- %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error\_string).
- %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error\_string).
- %ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.
- %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error\_string).
- %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error\_string).
- %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error\_string).
- %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error\_string).
- %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error\_string).
- %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error\_string).
- %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %PIXIASA-3-201002: Too many TCP connections on {static|late} global\_address! econns nconns
- %PIXIASA-3-201004: Too many UDP connections on {static|late} global\_address! udp connections limit
- %PIXIASA-3-201005: FTP data connection failed for IP\_address IP\_address
- %PIXIASA-3-201006: RCMD backconnection failed for IP\_address/port
- %PIXIASA-3-201008: The security appliance is disallowing new connections.
- %PIXIASA-3-201009: TCP connection limit of number for host IP\_address on interface\_name exceeded
- %PIXIASA-3-201010: Embryonic connection limit exceeded econns/limit for dir packet from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name
- %PIXIASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if\_name
- %ASA-3-201013: Per-client connection limit exceeded curr num/limit for [input/output] packet from ip/port to ip/port on interface interface\_name

- %PIX|ASA-3-202005: Non-embryonic in embryonic list outside\_address/outside\_port inside\_address/inside\_port
- %PIX|ASA-3-202011: Connection limit exceeded econns/limit for dir packet from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name
- %PIX|ASA-3-208005: (function:line\_num) clear command return code
- %PIX|ASA-3-210001: LU sw\_module\_name error = number
- %PIX|ASA-3-210002: LU allocate block (bytes) failed.
- %PIX|ASA-3-210003: Unknown LU Object number
- %PIX|ASA-3-210005: LU allocate connection failed
- %PIX|ASA-3-210006: LU look NAT for IP\_address failed
- %PIX|ASA-3-210007: LU allocate xlate failed
- %PIX|ASA-3-210008: LU no xlate for inside\_address/inside\_port outside\_address/outside\_port
- %PIX|ASA-3-210010: LU make UDP connection for outside\_address:outside\_port inside\_address:inside\_port failed
- %PIX|ASA-3-210020: LU PAT port port reserve failed
- %PIX|ASA-3-210021: LU create static xlate global\_address ifc interface\_name failed
- %PIX|ASA-3-211001: Memory allocation Error
- %PIX|ASA-3-212001: Unable to open SNMP channel (UDP port port) on interface interface\_number, error code = code
- %PIX|ASA-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface\_number, error code = code
- %PIX|ASA-3-212003: Unable to receive an SNMP request on interface interface\_number, error code = code, will try again.
- %PIX|ASA-3-212004: Unable to send an SNMP response to IP Address IP\_address Port port interface interface\_number, error code = code
- %PIX|ASA-3-212005: incoming SNMP request (number bytes) on interface interface\_name exceeds data buffer size, discarding this SNMP request.
- %PIX|ASA-3-212006: Dropping SNMP request from source\_address/source\_port to interface\_name:dest\_address/dest\_port because: reason.
- %PIX|ASA-3-213001: PPTP control daemon socket io string, errno = number.
- %PIX|ASA-3-213002: PPTP tunnel hashtable insert failed, peer = IP\_address.
- %PIX|ASA-3-213003: PPP virtual interface interface\_number isn't opened.
- %PIX|ASA-3-213004: PPP virtual interface interface\_number client ip allocation failed.
- %ASA-n-216001: internal error in: function: message
- PIX|ASA-3-216002: Unexpected event (major: major\_id, minor: minor\_id) received by task\_string in function at line: line\_num
- %PIX|ASA-3-216003: Unrecognized timer timer\_ptr, timer\_id received by task\_string in function at line: line\_num
- %ASA-3-219002: I2C\_API\_name error, slot = slot\_number, device = device\_number, address = address, byte count = count. Reason: reason\_string
- %PIX|ASA-3-302019: H.323 library\_name ASN Library failed to initialize, error code number

- %PIXIASA-3-302302: ACL = deny; no sa created
- %PIXIASA-3-304003: URL Server IP\_address timed out URL url
- %PIXIASA-3-304006: URL Server IP\_address not responding
- %PIXIASA-3-305005: No translation group found for protocol src interface\_name:source\_address/source\_port dst interface\_name:dest\_address/dest\_port
- %PIXIASA-3-305006: {outbound staticidentity|portmap|regular} translation creation failed for protocol src interface\_name:source\_address/source\_port dst interface\_name:dest\_address/dest\_port
- %PIXIASA-3-305008: Free unallocated global IP address.
- %PIXIASA-3-313001: Denied ICMP type=number, code=code from IP\_address on interface interface\_name
- %PIXIASA-3-313008: Denied ICMPv6 type=number, code=code from IP\_address on interface interface\_name
- %PIXIASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
- %PIXIASA-3-316001: Denied new tunnel to IP\_address. VPN peer limit (platform\_vpn\_peer\_limit) exceeded
- %ASA-3-316002: VPN Handle error: protocol=protocol, src in\_if\_num:src\_addr, dst out\_if\_num:dst\_addr
- %PIXIASA-3-317001: No memory available for limit\_slow
- %PIXIASA-3-317002: Bad path index of number for IP\_address, number max
- %PIXIASA-3-317003: IP routing table creation failure - reason
- %PIXIASA-3-317004: IP routing table limit warning
- %PIXIASA-3-317005: IP routing table limit exceeded - reason, IP\_address netmask
- %PIXIASA-3-318001: Internal error: reason
- %PIXIASA-3-318002: Flagged as being an ABR without a backbone area
- %PIXIASA-3-318003: Reached unknown state in neighbor state machine
- %PIXIASA-3-318004: area string lsid IP\_address mask netmask adv IP\_address type number
- %PIXIASA-3-318005: lsid ip\_address adv IP\_address type number gateway gateway\_address metric number network IP\_address mask netmask protocol hex attr hex net-metric number
- %PIXIASA-3-318006: if interface\_name if\_state number
- %PIXIASA-3-318007: OSPF is enabled on interface\_name during idb initialization
- %PIXIASA-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %PIXIASA-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line\_num
- %PIXIASA-3-319001: Acknowledge for arp update for IP address dest\_address not received (number).
- %PIXIASA-3-319002: Acknowledge for route update for IP address dest\_address not received (number).
- %PIXIASA-3-319003: Arp update for IP address address to NPn failed.
- %PIXIASA-3-319004: Route update for IP address dest\_address failed (number).
- %PIXIASA-3-320001: The subject name of the peer cert is not allowed for connection

- %PIX|ASA-3-322001: Deny MAC address MAC\_address, possible spoof attempt on interface interface
- %PIX|ASA-3-322002: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is {statically|dynamically} bound to MAC Address MAC\_address\_2.
- %PIX|ASA-3-322003: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is not bound to any MAC Address.
- %ASA-3-323001: Module in slot slotnum experienced a control channel communications failure.
- %ASA-3-323002: Module in slot slotnum is not able to shut down, shut down request not answered.
- %ASA-3-323003: Module in slot slotnum is not able to reload, reload request not answered.
- %ASA-3-323004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Hw-module reset is required before further use.
- %ASA-3-323005: Module in slot slotnum can not be powered on completely
- %ASA-3-323006: Type Module in slot slot experienced a data channel communication failure, data channel is DOWN.
- %ASA-3-323007: Module in slot slot experienced a firmware failure and the recovery is in progress.
- %PIX|ASA-3-324000: Drop GTPv version message msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port Reason: reason
- %PIX|ASA-3-324001: GTPv0 packet parsing error from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port, TID: tid\_value, Reason: reason
- %PIX|ASA-3-324002: No PDP[MCB] exists to process GTPv0 msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port, TID: tid\_value
- %PIX|ASA-3-324003: No matching request to process GTPv version msg\_type from source\_interface:source\_address/source\_port to source\_interface:dest\_address/dest\_port
- %PIX|ASA-3-324004: GTP packet with version%d from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port is not supported
- %PIX|ASA-3-324005: Unable to create tunnel from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port
- %PIX|ASA-3-324006: GSN IP\_address tunnel limit tunnel\_limit exceeded, PDP Context TID tid failed
- %PIX|ASA-3-324007: Unable to create GTP connection for response from source\_interface:source\_address/0 to dest\_interface:dest\_address/dest\_port
- %PIX|ASA-3-324300: Radius Accounting Request from from\_addr has an incorrect request authenticator
- %PIX|ASA-3-324301: Radius Accounting Request has a bad header length hdr\_len, packet length pkt\_len
- %PIX|ASA-3-325001: Router ipv6\_address on interface has conflicting ND (Neighbor Discovery) settings

- %PIX-3-325003: EUI-64 source address check failed. Dropped packet from interface\_in:source\_address/source\_port to dest\_address/dest\_port with source MAC address MAC\_address.
- %PIXIASA-3-326001: Unexpected error in the timer library: error\_message
- %PIXIASA-3-326002: Error in error\_message : error\_message
- %PIXIASA-3-326004: An internal error occurred while processing a packet queue
- %PIXIASA-3-326005: Mrib notification failed for (IP\_address, IP\_address)
- %PIXIASA-3-326006: Entry-creation failed for (IP\_address, IP\_address)
- %PIXIASA-3-326007: Entry-update failed for (IP\_address, IP\_address)
- %PIXIASA-3-326008: MRIB registration failed
- %PIXIASA-3-326009: MRIB connection-open failed
- %PIXIASA-3-326010: MRIB unbind failed
- %PIXIASA-3-326011: MRIB table deletion failed
- %PIXIASA-3-326012: Initialization of string functionality failed
- %PIXIASA-3-326013: Internal error: string in string line %d (%s)
- %PIXIASA-3-326014: Initialization failed: error\_message error\_message
- %PIXIASA-3-326015: Communication error: error\_message error\_message
- %PIXIASA-3-326016: Failed to set un-numbered interface for interface\_name (string)
- %PIXIASA-3-326017: Interface Manager error - string in string : string
- %PIXIASA-3-326019: string in string : string
- %PIXIASA-3-326020: List error in string : string
- %PIXIASA-3-326021: Error in string : string
- %PIXIASA-3-326022: Error in string : string
- %PIXIASA-3-326023: string - IP\_address : string
- %PIXIASA-3-326024: An internal error occurred while processing a packet queue.
- %PIXIASA-3-326025: string
- %PIXIASA-3-326026: Server unexpected error: error\_message
- %PIXIASA-3-326027: Corrupted update: error\_message
- %PIXIASA-3-326028: Asynchronous error: error\_message
- %PIXIASA-3-327001: IP SLA Monitor: Cannot create a new process
- %PIXIASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
- %PIXIASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
- %PIXIASA-3-328001: Attempt made to overwrite a set stub function in string.
- %PIXIASA-3-329001: The string0 subblock named string1 was not removed
- ASAPIX-3-331001: Dynamic DNS Update for 'fqdn\_name' <=> ip\_address failed
- %PIXIASA-3-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number=0x7B) from 75.2.96.101 (user= user) to 85.2.96.10 with incorrect IPsec padding.

- %PIX|ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface\_name AC:ac\_name
- %PIX|ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface\_name AC:ac\_name
- %PIX|ASA-3-403503: PPPoE:PPP link down:reason
- %PIX|ASA-3-403504: PPPoE:No 'vpdn group group\_name' for PPPoE is created
- %PIX|ASA-3-403507:PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group\_name
- %PIX|ASA-3-404102: ISAKMP: Exceeded embryonic limit
- %PIX|ASA-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside\_address/outside\_port to global\_address (inside\_address)/inside\_port on interface interface\_name
- %PIX|ASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp\_server\_address on interface interface\_name: [fail\_reason]
- %PIX|ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail\_reason]
- %ASA-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)"
- %ASA-3-421001: TCPIUDP flow from interface\_name:ip/port to interface\_name:ip/port is dropped because application has failed.
- %ASA-3-421003: Invalid data plane encapsulation.
- %ASA-3-421007: TCPIUDP flow from interface\_name:IP\_address/port to interface\_name:IP\_address/port is skipped because application has failed.
- %ASA-3-500005: connection terminated for protocol from in\_ifc\_name:src\_address/src\_port to out\_ifc\_name:dest\_address/dest\_port due to invalid combination of inspections on same flow. Inspect inspect\_name is not compatible with inspect filter\_name.
- %PIX|ASA-3-610001: NTP daemon interface interface\_name: Packet denied from IP\_address
- %PIX|ASA-3-610002: NTP daemon interface interface\_name: Authentication failed for packet from IP\_address
- %PIX|ASA-3-611313: VPNClient: Backup Server List Error: reason
- %PIX|ASA-3-702305: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) is rekeying due to sequence number rollover.
- %PIX|ASA-3-702307: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) is rekeying due to data rollover.
- %PIX|ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %PIX|ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %PIX|ASA-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %PIX|ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %PIX|ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID\_Type
- %PIX|ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID\_Type
- %PIX|ASA-3-713018: Unknown ID type during find of group name for certs, Type ID\_Type
- %PIX|ASA-3-713020: No Group found by matching OU(s) from ID payload: OU\_value

- %PIXIASA-3-713022: No Group found matching peer\_ID or IP\_address for Pre-shared key peer IP\_address
- %PIXIASA-3-713032: Received invalid local Proxy Range IP\_address - IP\_address
- %PIXIASA-3-713033: Received invalid remote Proxy Range IP\_address - IP\_address
- %PIXIASA-3-713042: IKE Initiator unable to find policy: Intf interface\_number, Src: source\_address, Dst: dest\_address
- %PIXIASA-3-713043: Cookie/peer address IP\_address session already in progress
- %PIXIASA-3-713048: Error processing payload: Payload ID: id
- %PIXIASA-3-713051: Terminating connection attempt: IPSEC not permitted for group (group\_name)
- %PIXIASA-3-713056: Tunnel rejected: SA (SA\_name) not found for group (group\_name)!
- %PIXIASA-3-713059: Tunnel Rejected: User (user) matched with group name, group-lock check failed.
- %PIXIASA-3-713060: Tunnel Rejected: User (user) not member of group (group\_name), group-lock check failed.
- %PIXIASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source\_address, Dst: dest\_address!
- %PIXIASA-3-713062: IKE Peer address same as our interface address IP\_address
- %PIXIASA-3-713063: IKE Peer address not configured for destination IP\_address
- %PIXIASA-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %PIXIASA-3-713072: Password for user (user) too long, truncating to number characters
- %PIXIASA-3-713081: Unsupported certificate encoding type encoding\_type
- %PIXIASA-3-713082: Failed to retrieve identity certificate
- %PIXIASA-3-713083: Invalid certificate handle
- %PIXIASA-3-713084: Received invalid phase 1 port value (port) in ID payload
- %PIXIASA-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %PIXIASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %PIXIASA-3-713088: Set Cert filehandle failure: no IPSec SA in group group\_name
- %PIXIASA-3-713098: Aborting: No identity cert specified in IPSec SA (SA\_name)!
- %PIXIASA-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %PIXIASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %PIXIASA-3-713107: IP\_Address request attempt failed!
- %PIXIASA-3-713109: Unable to process the received peer certificate
- %PIXIASA-3-713112: Failed to process CONNECTED notify (SPI SPI\_value)!
- %PIXIASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %PIXIASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID\_Type
- %PIXIASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID\_Type
- %PIXIASA-3-713118: Detected invalid Diffie-Hellman group\_descriptor group\_number, in IKE area

- %PIX|ASA-3-713122: Keep-alives configured keepalive\_type but peer IP\_address support keep-alives (type = keepalive\_type)
- %PIX|ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive\_type)
- %PIX|ASA-3-713124: Received DPD sequence number rcv\_sequence\_# in DPD Action, description expected seq #
- %PIX|ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %PIX|ASA-3-713129: Received unexpected Transaction Exchange payload type: payload\_id
- %PIX|ASA-3-713132: Cannot obtain an IP\_address for remote peer
- %PIX|ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group\_id) with phase 1 group(DH group DH group\_number)
- %PIX|ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %PIX|ASA-3-713138: Group group\_name not found and BASE GROUP default preshared key not configured
- %PIX|ASA-3-713140: Split Tunneling Policy requires network list but none configured
- %PIX|ASA-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id), Product product(id), Caps: capability\_value. Expected -- Vendor: vendor(id), Product: product(id), Caps: capability\_value
- %PIX|ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability\_value
- %PIX|ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP\_address, mask: netmask
- %PIX|ASA-3-713149: Hardware client security attribute attribute\_name was enabled but not requested.
- %PIX|ASA-3-713152: Unable to obtain any rules from filter ACL\_tag to send to client for CPP, terminating connection.
- %PIX|ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %PIX|ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %PIX|ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %PIX|ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %PIX|ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %PIX|ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %PIX|ASA-3-713167: Remote peer has failed user authentication - check configured username and password
- %PIX|ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %PIX|ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!

- %PIXIASA-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %PIXIASA-3-713185: Error: Username too long - connection aborted
- %PIXIASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list\_text Character index (value) is illegal
- %PIXIASA-3-713189: Attempted to assign network or broadcast IP\_address, removing (IP\_address) from pool.
- %PIXIASA-3-713193: Received packet with missing payload, Expected payload: payload\_id
- %PIXIASA-3-713194: IKE/IPSec Delete With Reason message: termination\_reason
- %PIXIASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %PIXIASA-3-713198: User Authorization failed: user User authorization failed.
- %PIXIASA-3-713203: IKE Receiver: Error reading from socket.
- %PIXIASA-3-713205: Could not add static route for client address: IP\_address
- %PIXIASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %PIXIASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule\_id
- %PIXIASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %PIXIASA-3-713210: Cannot create dynamic map for Backup L2L entry rule\_id
- %PIXIASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP\_address, mask: netmask
- %PIXIASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP\_address, mask: netmask
- %PIXIASA-3-713217: Skipping unrecognized rule: action: action client type: client\_type client version: client\_version
- %PIXIASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %PIXIASA-3-713226: Connection failed with peer IP\_address, no trust-point defined in tunnel-group tunnel\_group
- %PIXIASA-3-713230 Internal Error, ike\_lock trying to lock bit that is already locked for type type
- %PIXIASA-3-713231 Internal Error, ike\_lock trying to unlock bit that is not locked for type type
- %PIXIASA-3-713232 SA lock refCnt = value, bitmask = hexvalue, pl\_decrypt\_cb = value, qm\_decrypt\_cb = value, qm\_hash\_cb = value, qm\_spi\_ok\_cb = value, qm\_dh\_cb = value, qm\_secret\_key\_cb = value, qm\_encrypt\_cb = value
- %PIXIASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %PIXIASA-3-713902 descriptive\_event\_string
- %ASA-3-716056: Group group-name User user-name IP IP\_address Authentication to SSO server name: name type type failed reason: reason
- %PIXIASA-3-717001: Querying keypair failed.
- %PIXIASA-3-717002: Certificate enrollment failed for trustpoint trustpoint\_name. Reason: reason\_string.
- %PIXIASA-3-717009: Certificate validation failed. Reason: reason\_string.
- %PIXIASA-3-717010: CRL polling failed for trustpoint trustpoint\_name.

- %PIX|ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint\_name at time\_of\_failure
- %PIX|ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl\_size, maximum CRL size = max\_crl\_size)
- %PIX|ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint\_name from enrollment\_url
- %PIX|ASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number\_of\_entries, maximum number allowed = max\_allowed)
- %PIX|ASA-3-717019: Failed to insert CRL for trustpoint trustpoint\_name. Reason: failure\_reason.
- %PIX|ASA-3-717021 Certificate data could not be verified. Locate Reason: reason\_string serial number: serial number, subject name: subject name, key length key length bits.
- %PIX|ASA-3-717023 SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason\_string.
- %PIX|ASA-3-717027 Certificate chain failed validation. reason\_string.
- %PIX-3-717032 OCSP status check failed. Reason: reason\_string.
- %ASA-3-719002: Email Proxy session pointer from source\_address has been terminated due to reason error.
- %ASA-3-719008: Email Proxy service is shutting down.
- %ASA-3-722007: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722008: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722009: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722020: Group group User user-name IP IP\_address No address available for SVC connection
- %ASA-3-722021: Group group User user-name IP IP\_address Unable to start compression due to lack of memory resources
- %ASA-3-722035: Group group User user-name IP IP\_address Transmitting large packet length (threshold threshold).
- %ASA-3-722036: Group group User user-name IP IP\_address Received large packet length (threshold threshold).

## Warning Messages, Severity 4

The following messages appear at severity 4, warning:

- %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
- %PIX|ASA-4-106027: Failed to determine the security context for the packet:vlan source Vlan#:ethertype src sourceMAC dst destMAC
- %PIX|ASA-4-108004: action\_class: action ESMTTP req\_resp from src\_ifc:siplsport to dest\_ifc:dipldport;further\_info
- %PIX|ASA-4-109017: User at IP\_address exceeded auth proxy connection limit (max)

- %PIXIASA-4-109022: exceeded HTTPS proxy process limit
- %PIXIASA-4-109027: [aaa protocol] Unable to decipher response message Server = server\_IP\_address, User = user
- %PIXIASA-4-109028: aaa bypassed for same-security traffic from ingress\_interface:source\_address/source\_port to egress\_interface:dest\_address/dest\_port
- %PIXIASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access\_list source | dest netmask netmask.
- %PIXIASA-4-109031: NT Domain Authentication Failed: rejecting guest login for username.
- %PIXIASA-4-109033: Authentication failed for admin user user from src\_IP. Interactive challenge processing is not supported for protocol connections
- %PIXIASA-4-109034: Authentication failed for network user user from src\_IP/port to dst\_IP/port. Interactive challenge processing is not supported for protocol connections
- %PIXIASA-4-113019: Group = group, Username = user, IP = peer\_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %PIXIASA-4-209003: Fragment database limit of number exceeded: src = source\_address, dest = dest\_address, proto = protocol, id = number
- %PIXIASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source\_address, dest = dest\_address, proto = protocol, id = number
- %PIXIASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %PIXIASA-4-308002: static global\_address inside\_address netmask netmask overlapped with global\_address inside\_address
- %PIXIASA-4-313004: Denied ICMP type=icmp\_type, from source\_address on interface interface\_name to dest\_address: no matching session
- %PIXIASA-4-313005: No matching connection for ICMP error message: icmp\_msg\_info on interface\_name interface. Original IP payload: embedded\_frame\_info icmp\_msg\_info = icmp src src\_interface\_name:src\_address dst dest\_interface\_name:dest\_address (type icmp\_type, code icmp\_code) embedded\_frame\_info = prot src source\_address/source\_port dst dest\_address/dest\_port
- %PIXIASA-4-325002: Duplicate address ipv6\_address/MAC\_address on interface
- %PIXIASA-4-335005: NAC Downloaded ACL parse failure - host-address
- %PIXIASA-4-4000nn: IPS:number string from IP\_address to IP\_address on interface interface\_name
- %PIXIASA-4-401001: Shuns cleared
- %PIXIASA-4-401002: Shun added: IP\_address IP\_address port port
- %PIXIASA-4-401003: Shun deleted: IP\_address
- %PIXIASA-4-401004: Shunned packet: IP\_address ==> IP\_address on interface interface\_name
- %PIXIASA-4-401005: Shun add failed: unable to allocate resources for IP\_address IP\_address port port
- %PIXIASA-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=dest\_address, prot=protocol, spi=number
- %PIXIASA-4-402102: decapsulate: packet missing {AH/ESP}, destaddr=dest\_address, actual prot=protocol

- %PIX|ASA-4-402103: identity doesn't match negotiated identity (ip) dest\_address= dest\_address, src\_addr= source\_address, prot= protocol, (ident) local=inside\_address, remote=remote\_address, local\_proxy=IP\_address/IP\_address/port/port, remote\_proxy=IP\_address/IP\_address/port/port
- %PIX|ASA-4-402106: Rec'd packet not an IPSEC packet (ip) dest\_address= dest\_address, src\_addr= source\_address, prot= protocol
- %PIX|ASA-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP to local\_IP with an invalid SPI.
- %PIX|ASA-4-402115: IPSEC: Received a packet from remote\_IP to local\_IP containing act\_prot data instead of exp\_prot data.
- %PIX|ASA-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP . The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt\_daddr, its source as pkt\_saddr, and its protocol as pkt\_prot . The SA specifies its local proxy as id\_daddr /id\_dmask /id\_dprot /id\_dport and its remote proxy as id\_saddr /id\_smask /id\_sprot /id\_sport .
- %PIX|ASA-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote\_IP to local\_IP.
- %PIX|ASA-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq\_num) from remote\_IP (username) to local\_IP containing an illegal IP fragment of length frag\_len with offset frag\_offset.
- %PIX|ASA-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP that failed anti-replay checking.
- %PIX|ASA-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP that failed authentication.
- %PIX|ASA-4-402123: CRYPTO: The accel\_type hardware accelerator encountered an error (code= error\_string) while executing crypto command command .
- %PIX|ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel\_id=number, session\_id=number
- %PIX|ASA-4-403102: PPP virtual interface interface\_name rcvd pkt with invalid protocol: protocol, reason: reason.
- %PIX|ASA-4-403103: PPP virtual interface max connections reached.
- %PIX|ASA-4-403104: PPP virtual interface interface\_name requires mschap for MPPE.
- %PIX|ASA-4-403106: PPP virtual interface interface\_name requires RADIUS for MPPE.
- %PIX|ASA-4-403107: PPP virtual interface interface\_name missing aaa server group info
- %PIX|ASA-4-403108: PPP virtual interface interface\_name missing client ip address option
- %PIX|ASA-4-403109: Rec'd packet not an PPTP packet. (ip) dest\_address= dest\_address, src\_addr= source\_address, data: string.
- %PIX|ASA-4-403110: PPP virtual interface interface\_name, user: user missing MPPE key from aaa server.
- %PIX|ASA-4-403505: PPPoE:PPP - Unable to set default route to IP\_address at interface\_name
- %PIX|ASA-4-403506: PPPoE:failed to assign PPP IP\_address netmask netmask at interface\_name
- %PIX|ASA-4-404101: ISAKMP: Failed to allocate address for client from pool string
- %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

- %PIXIASA-4-405002: Received mac mismatch collision from IP\_address/MAC\_address for authenticated host
- %PIXIASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign\_address outside\_address[/outside\_port] to local\_address inside\_address[/inside\_port]
- %PIXIASA-4-405102: Unable to Pre-allocate H245 Connection for foreign\_address outside\_address[/outside\_port] to local\_address inside\_address[/inside\_port]
- %PIXIASA-4-405103: H225 message from source\_address/source\_port to dest\_address/dest\_port contains bad protocol discriminator hex
- %PIXIASA-4-405104: H225 message received from outside\_address/outside\_port to inside\_address/inside\_port before SETUP
- %PIXIASA-4-405105: H323 RAS message AdmissionConfirm received from source\_address/source\_port to dest\_address/dest\_port without an AdmissionRequest
- %PIXIASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s\n
- %PIXIASA-4-405201: ILS ILS\_message\_type from inside\_interface:source\_IP\_address to outside\_interface:/destination\_IP\_address has wrong embedded address embedded\_IP\_address
- %PIXIASA-4-405300: Radius Accounting Request received from from\_addr is not allowed
- %PIXIASA-4-405301: Attribute attribute\_number does not match for user user\_ip
- %PIXIASA-4-406001: FTP port command low port: IP\_address/port to IP\_address on interface interface\_name
- %PIXIASA-4-406002: FTP port command different address: IP\_address(IP\_address) to IP\_address on interface interface\_name
- %PIXIASA-4-407001: Deny traffic for local-host interface\_name:inside\_address, license limit of number exceeded
- %PIXIASA-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside\_address/outside\_port to global\_address (inside\_address)/inside\_port on interface interface\_name
- %PIXIASA-4-407003: Established limit for RPC services exceeded number
- %PIXIASA-4-408001: IP route counter negative - reason, IP\_address Attempt: number
- %PIXIASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %PIXIASA-4-408003: can't track this type of object hex
- %PIXIASA-4-409001: Database scanner: external LSA IP\_address netmask is lost, reinstalls
- %PIXIASA-4-409002: db\_free: external LSA IP\_address netmask
- %PIXIASA-4-409003: Received invalid packet: reason from IP\_address, interface\_name
- %PIXIASA-4-409004: Received reason from unknown neighbor IP\_address
- %PIXIASA-4-409005: Invalid length number in OSPF packet from IP\_address (ID IP\_address), interface\_name
- %PIXIASA-4-409006: Invalid lsa: reason Type number, LSID IP\_address from IP\_address, IP\_address, interface\_name
- %PIXIASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP\_address netmask New: Destination IP\_address netmask
- %PIXIASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric : number area : string

- %PIX|ASA-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID
- %PIX|ASA-4-409010: Virtual link information found in non-backbone area: string
- %PIX|ASA-4-409011: OSPF detected duplicate router-id IP\_address from IP\_address on interface interface\_name
- %PIX|ASA-4-409012: Detected router with duplicate router ID IP\_address in area string
- %PIX|ASA-4-409013: Detected router with duplicate router ID IP\_address in Type-4 LSA advertised by IP\_address
- %PIX|ASA-4-409023: Attempting AAA Fallback method method\_name for request\_type request for user user :Auth-server group server\_tag unreachable
- %PIX|ASA-4-410001: UDP DNS request from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.
- %PIX|ASA-4-410003: action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %ASA-4-4108004: action\_class: action ESMTP req\_resp from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIX|ASA-4-411001: Line protocol on interface interface\_name changed state to up
- %PIX|ASA-4-411002: Line protocol on interface interface\_name changed state to down
- %PIX|ASA-4-411003: Configuration status on interface interface\_name changed state to downup
- %PIX|ASA-4-411004: Configuration status on interface interface\_name changed state to up
- %ASA-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.
- %PIX|ASA-4-412001: MAC MAC\_address moved from interface\_1 to interface\_2
- %PIX|ASA-4-412002: Detected bridge table full while inserting MAC MAC\_address on interface interface. Number of entries = num
- %ASA-4-413001: Module in slot slotnum is not able to shut down. Module Error: errnum message
- %ASA-4-413002: Module in slot slotnum is not able to reload. Module Error: errnum message
- %ASA-4-413003: Module in slot slotnum is not a recognized type
- %ASA-4-413004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Trying again.
- %PIX|ASA-4-415016: policy-map map\_name: Maximum number of unanswered HTTP requests exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-4-416001: Dropped UDP SNMP packet from source\_interface :source\_IP/source\_port to dest\_interface:dest\_address/dest\_port; version (prot\_version) is not allowed through the firewall
- %PIX|ASA-4-417001: Unexpected event received: number
- %PIX|ASA-4-417004: Filter violation error: conn number (string:string) in string
- %PIX|ASA-4-417006: No memory for string) in string. Handling: string
- %PIX-4-417008 AutoRP: removed string embedded group address1/mask1 on interface interface-name from address2 due to overlap address3/mask2
- %PIX-4-417009 AutoRp: discarded string on interface interface-name from address due to malformed packet

- %PIXIASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol\_string from interface\_name IP\_address (port) to interface\_name IP\_address (port)
- %PIXIASA-4-419001: Dropping TCP packet from src\_ifc:src\_IP/src\_port to dest\_ifc:dest\_IP/dest\_port, reason: MSS exceeded, MSS size, data size
- %ASA-4-419002: Received duplicate TCP SYN from in\_interface:src\_address/src\_port to out\_interface:dest\_address/dest\_port with different initial sequence number.
- %ASA-4-419003:Cleared TCP urgent flag from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port.
- %ASA-3-420001 : IPS card not up and fail-close mode used, dropping ICMP packet ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)"
- %ASA-4-420002 : IPS requested to drop ICMP packets ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)"
- %ASA-4-420003 : IPS requested to reset TCP connection from ifc\_in:SIP/SPORT to ifc\_out:DIP/DPORT"
- %PIXIASA-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1
- %PIXIASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %PIXIASA-4-422006: IP SLA Monitor Probe number: string
- %ASA-4-423001: { Allowed | Dropped } invalid NBNS pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423002: { Allowed | Dropped } mismatched NBNS pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423003: { Allowed | Dropped } invalid NBDGM pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423004: { Allowed | Dropped } mismatched NBDGM pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423005: { Allowed | Dropped } NBDGM pkt\_type\_name fragment with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-424001: Packet denied protocol\_string intf\_in:src\_ip/src\_port intf\_out:dst\_ip/dst\_port. [Ingress|Egress] interface is in a backup state.
- %ASA-4-424002: Connection to the backup interface is denied: protocol\_string intf:src\_ip/src\_port intf:dst\_ip/dst\_port
- %PIXIASA-4-431001: RTP conformance: Dropping RTP packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, Drop reason: drop\_reason value
- %PIXIASA-4-431002: RTCP conformance: Dropping RTCP packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, Drop reason: drop\_reason value
- ASA-4-450001: Deny traffic for protocol protocol\_id src interface\_name:IP\_address/port dst interface\_name:IP\_address/port, licensed host limit of num exceeded.
- %PIXIASA-4-500004: Invalid transport field for protocol=protocol, from source\_address/source\_port to dest\_address/dest\_port
- %PIXIASA-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %PIXIASA-4-607002: action\_class: action SIP req\_resp req\_resp\_info from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIXIASA-4-608002: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, SCCPPrefix length value too small

- %PIX|ASA-4-608003: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, SCCPPrefix length value too large
- %PIX|ASA-4-608004: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, message id value not allowed
- %PIX|ASA-4-608005: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, message id value registration not complete
- %PIX|ASA-4-612002: Auto Update failed:filename, version:number, reason:reason
- %PIX|ASA-4-612003:Auto Update failed to contact:url, reason:reason
- %PIX|ASA-4-620002: Unsupported CTIQBE version: hex: from interface\_name:IP\_address/port to interface\_name:IP\_address/port
- %PIX|ASA-4-713154: DNS lookup for peer\_description Server [server\_name] failed!
- %PIX|ASA-4-713157: Timed out on initial contact to server [server\_name or IP\_address] Tunnel could not be established.
- %ASA-4-713239: IP\_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %ASA-4-713240: Received DH key with bad length: received length=rlength expected length=length
- %ASA-4-713241: IE Browser Proxy Method setting\_number is Invalid
- %ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
- %ASA-4-713243: META-DATA Unable to find the requested certificate
- %ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %ASA-4-713249: META-DATA Received unsupported authentication results: result
- %ASA-4-713251: META-DATA Received authentication failure message
- %ASA-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name 'group-name'
- %PIX|ASA-4-713903:descriptive\_event\_string.
- %ASA-4-716007: Group group User user WebVPN Unable to create session.
- %ASA-4-716022: Unable to connect to proxy server reason.
- %ASA-4-716023: Group name User user Session could not be established: session limit of maximum\_sessions reached.
- %ASA-4-716044: Group group-name User user-name IP IP\_address AAA parameter param-name value param-value out of range.
- %ASA-4-716045: Group group-name User user-name IP IP\_address AAA parameter param-name value invalid.

- %ASA-4-716046: Group group-name-name User user-name IP IP\_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.
- %ASA-4-716047: Group group-name User user-name IP IP\_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
- %ASA-4-716048: Group group-name User user-name IP IP\_address No memory to parse ACL.
- %ASA-4-716052: Group group-name User user-name IP IP\_address Pending session terminated.
- %PIXIASA-4-717026 Name lookup failed for hostname hostname during PKI operation.
- %PIXIASA-4-717031 Failed to find a suitable trustpoint for the issuer: issuer Reason: reason\_string
- %PIXIASA-4-717035 OCSP status is being checked for certificate. certificate\_identifier.
- %PIXIASA-4-717037 Tunnel group search using certificate maps failed for peer certificate: certificate\_identifier.
- %ASA-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %ASA-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %ASA-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %ASA-4-720009: (VPN-unit) Failed to create version control block.
- %ASA-4-720011: (VPN-unit) Failed to allocate memory
- %ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint\_name
- %ASA-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %ASA-4-720033: (VPN-unit) Failed to queue add to message queue.
- %ASA-4-720038: (VPN-unit) Corrupted message from active unit.
- %ASA-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %ASA-4-720044: (VPN-unit) Failed to receive message from active unit
- %ASA-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP\_address on the standby unit.
- %ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %ASA-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP\_address, port=port
- %ASA-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP\_address, port=port.
- %ASA-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %ASA-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP\_address, port=port during bulk sync.
- %ASA-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %ASA-4-720066: (VPN-unit) Failed to activate IKE database.
- %ASA-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %ASA-4-720068: (VPN-unit) Failed to parse peer message.
- %ASA-4-720069: (VPN-unit) Failed to activate cTCP database.
- %ASA-4-720070: (VPN-unit) Failed to deactivate cTCP database.

- %ASA-4-720073: (VPN-unit) Fail to insert certificate in trust point trustpoint on the standby unit.
- %ASA-4-722001: IP IP\_address Error parsing SVC connect request.
- %ASA-4-722002: IP IP\_address Error consolidating SVC connect request.
- %ASA-4-722003: IP IP\_address Error authenticating SVC connect request.
- %ASA-4-722004: Group group User user-name IP IP\_address Error responding to SVC connect request.
- %ASA-4-722015: Group group User user-name IP IP\_address Unknown SVC frame type: type-num
- %ASA-4-722016: Group group User user-name IP IP\_address Bad SVC frame length: length expected: expected-length
- %ASA-4-722017: Group group User user-name IP IP\_address Bad SVC framing: 525446, reserved: 0
- %ASA-4-722018: Group group User user-name IP IP\_address Bad SVC protocol version: version, expected: expected-version
- %ASA-4-722019: Group group User user-name IP IP\_address Not enough data for an SVC header: length
- %ASA-4-724001: Group group-name User user-name IP IP\_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.
- %ASA-4-724002: Group group-name User user-name IP IP\_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.
- %ASA-4-733104: TD\_SYSLOG\_TCP\_INTERCEPT\_AVERAGE\_RATE\_EXCEED
- %ASA-4-733105: TD\_SYSLOG\_TCP\_INTERCEPT\_BURST\_RATE\_EXCEED

## Notification Messages, Severity 5

The following messages appear at severity 5, notifications:

- %PIX|ASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %PIX|ASA-5-109029: Parsing downloaded ACL: string
- %PIX|ASA-5-111002: Begin configuration: IP\_address reading from device
- %PIX|ASA-5-111003: IP\_address Erase configuration
- %PIX|ASA-5-111004: IP\_address end configuration: {FAILED|OK}
- %PIX|ASA-5-111005: IP\_address end configuration: OK
- %PIX|ASA-5-111007: Begin configuration: IP\_address reading from device.
- %PIX|ASA-5-111008: User user executed the command string
- %PIX|ASA-5-199001: Reload command executed from telnet (remote IP\_address).
- %PIX|ASA-5-199006: Orderly reload started at when by whom. Reload reason: reason
- %PIX|ASA-5-199007: Reload scheduled for when by whom at when-command-issued. Reload reason: reason
- %PIX|ASA-5-199008: Scheduled reload for when-reload-is-supposed-to-happen cancelled by whom at when.

- %PIXIASA-5-303004: FTP cmd\_string command unsupported - failed strict inspection, terminating connection from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_interface
- %PIXIASA-5-303005: Strict FTP inspection matched match\_string in policy-map policy-name, action\_string from src\_ifc:sip/sport to dest\_ifc:dip/dport
- %PIXIASA-5-304001: user@source\_address Accessed {JAVA URL|URL} dest\_address: url
- %PIXIASA-5-304002: Access denied URL chars SRC IP\_address DEST IP\_address: chars
- %PIX/ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface\_name:source\_address/source\_port dest interface\_name: dest\_address/dest\_port denied due to NAT reverse path failure.
- %PIXIASA-5-321001: Resource var1 limit of var2 reached.
- %PIXIASA-5-321002: Resource var1 rate limit of var2 reached.
- ASA/PIX-5-331002: Dynamic DNS type RR for ip\_address -> 'fqdn\_name' successfully updated in DNS server dns\_server\_ip
- %ASA/PIX-5-332003: Web Cache IP\_address/service\_ID acquired
- %PIXIASA-5-333002: Timeout waiting for EAP response - context:EAP-context
- %PIXIASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %PIXIASA-5-334002: EAPoUDP association successfully established - host-address
- %PIXIASA-5-334003: EAPoUDP association failed to establish - host-address
- %PIXIASA-5-334005: Host put into NAC Hold state - host-address
- %PIXIASA-5-334006: EAPoUDP failed to get a response from host - host-address
- %PIXIASA-5-335002: Host is on the NAC Exception List - host-address, OS:oper-sys
- %PIXIASA-5-335003: NAC Default ACL applied, ACL:ACL-name - host-address
- %PIXIASA-5-335008: NAC IPsec terminate from dynamic ACL:ACL-name - host-address
- %ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit
- %PIXIASA-5-415004: HTTP - matched matched\_string in policy-map map\_name, content-type verification failed connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415005: HTTP - matched matched\_string in policy-map map\_name, URI length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415006: HTTP - matched matched\_string in policy-map map\_name, URI matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415007: HTTP - matched matched\_string in policy-map map\_name, Body matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415008: HTTP - matched matched\_string in policy-map map\_name, header matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415009: HTTP - matched matched\_string in policy-map map\_name, method matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-5-415010: matched matched\_string in policy-map map\_name, transfer encoding matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num

- %PIX|ASA-5-415011: HTTP - policy-map map\_name:Protocol violation connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415012: HTTP - matched matched\_string in policy-map map\_name, Unknown mime-type connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415013: HTTP - policy-map map\_name:Malformed chunked encoding connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415014: HTTP - matched matched\_string in policy-map map\_name, Mime-type in response wasn't found in the accept-types of the request connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415015: HTTP - matched matched\_string in policy-map map\_name, transfer-encoding unknown connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415018: HTTP - matched matched\_string in policy-map map\_name, Header length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415019: HTTP - matched matched\_string in policy-map map\_name, status line matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-415020: HTTP - matched matched\_string in policy-map map\_name, a non-ASCII character was matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIX|ASA-5-500001: ActiveX content modified src IP\_address dest IP\_address on interface interface\_name.
- %PIX|ASA-5-500002: Java content modified src IP\_address dest IP\_address on interface interface\_name.
- %PIX|ASA-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source\_address/source\_port to dest\_address/dest\_port, flags: tcp\_flags, on interface interface\_name
- %PIX|ASA-5-501101: User transitioning priv level
- %PIX|ASA-5-502101: New user added to local dbase: Uname: user Priv: privilege\_level Encpass: string
- %PIX|ASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege\_level Encpass: string
- %PIX|ASA-5-502103: User priv level changed: Uname: user From: privilege\_level To: privilege\_level
- %PIX|ASA-5-502111: New group policy added: name: policy\_name Type: policy\_type
- %PIX|ASA-5-502112: Group policy deleted: name: policy\_name Type: policy\_type
- %PIX|ASA-5-503001: Process number, Nbr IP\_address on interface\_name from string to string, reason
- %PIX|ASA-5-504001: Security context context\_name was added to the system
- %PIX|ASA-5-504002: Security context context\_name was removed from the system
- %ASA-5-505001: Module in slot slotnum is shutting down. Please wait...
- %ASA-5-505002: Module in slot slotnum is reloading. Please wait...
- %ASA-5-505003: Module in slot slotnum is resetting. Please wait...
- %ASA-5-505004: Module in slot slotnum shutdown is complete.
- %ASA-5-505005: Module in slot slotnum is initializing control communication. Please wait...

- %ASA-5-505006: Module in slot slotnum is Up.
- %ASA-5-505007: Module in slot slotnum is recovering. Please wait...
- %ASA-5-505008: Module in slot slotnum software is being updated to vnewver (currently vver)
- %ASA-5-505009: Module in slot slotnum software was updated to vnewver (previously vver)
- %ASA-5-505010: Module in slot slot removed.
- %ASA-5-505011: Type Module in slot slot, data channel communication is UP.
- %ASA-5-505012: Module in slot slot, application stopped application, version version
- %ASA-5-505013: Module in slot slot application changed from: application version version to: newapplication version newversion.
- %ASA-5-506001: event\_source\_string event\_string
- %PIXIASA-5-507001: Terminating TCP-Proxy connection from interface\_inside:source\_address/source\_port to interface\_outside:dest\_address/dest\_port - reassembly limit of limit bytes exceeded
- %PIXIASA-5-508001: DCERPC message\_type non-standard version\_type version version\_number from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port, terminating connection.
- %PIXIASA-5-508002: DCERPC response has low endpoint port port\_number from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port, terminating connection.
- %ASA-5-509001: Connection attempt from src\_intf:src\_ip/src\_port to dst\_intf:dst\_ip/dst\_port was prevented by “no forward” command.
- %PIXIASA-5-611103: User logged out: Uname: user
- %PIXIASA-5-611104: Serial console idle timeout exceeded
- %PIXIASA-5-612001: Auto Update succeeded:filename, version:number
- %PIXIASA-5-713006: Failed to obtain state for message Id message\_number, Peer Address: IP\_address
- %PIXIASA-5-713010: IKE area: failed to find centry for message Id message\_number
- %PIXIASA-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface\_number, IKE Peer IP\_address local Proxy Address IP\_address, remote Proxy Address IP\_address, Crypto map (crypto map tag)
- %PIXIASA-5-713049: Security negotiation complete for tunnel\_type type (group\_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %PIXIASA-5-713050: Connection terminated for peer IP\_address. Reason: termination reason Remote Proxy IP\_address, Local Proxy IP\_address
- %PIXIASA-5-713068: Received non-routine Notify message: notify\_type (notify\_value)
- %PIXIASA-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger\_value to smaller\_value seconds
- %PIXIASA-5-713074: Responder forcing change of IPSec rekeying duration from larger\_value to smaller\_value Kbs
- %PIXIASA-5-713075: Overriding Initiator's IPSec rekeying duration from larger\_value to smaller\_value seconds
- %PIXIASA-5-713076: Overriding Initiator's IPSec rekeying duration from larger\_value to smaller\_value Kbs
- %PIXIASA-5-713092: Failure during phase 1 rekeying attempt due to collision

- %PIX|ASA-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec
- %PIX|ASA-5-713119: PHASE 1 COMPLETED
- %PIX|ASA-5-713120: PHASE 2 COMPLETED (msgid=msg\_id)
- %PIX|ASA-5-713130: Received unsupported transaction mode attribute: attribute id
- %PIX|ASA-5-713131: Received unknown transaction mode attribute: attribute\_id
- %PIX|ASA-5-713135: message received, redirecting tunnel to IP\_address.
- %PIX|ASA-5-713136: IKE session establishment timed out [IKE\_state\_name], aborting!
- %PIX|ASA-5-713137: Reaper overriding refCnt [ref\_count] and tunnelCnt [tunnel\_count] -- deleting SA!
- %PIX|ASA-5-713139: group\_name not found, using BASE GROUP default preshared key
- %PIX|ASA-5-713144: Ignoring received malformed firewall record; reason - error\_reason TLV type attribute\_value correction
- %PIX|ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP\_address, mask: netmask
- %PIX|ASA-5-713155: DNS lookup for Primary VPN Server [server\_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %PIX|ASA-5-713156: Initializing Backup Server [server\_name or IP\_address]
- %PIX|ASA-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP
- %PIX|ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %PIX|ASA-5-713179: IKE AM Initiator received a packet from its peer without a payload\_type payload
- %PIX|ASA-5-713196: Remote L2L Peer IP\_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!
- %PIX|ASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel\_type connection. Enforcing the second default.
- %PIX|ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter\_value)!
- %PIX-5-713201: Duplicate (Phase 1/Phase 2) packet detected. (Retransmitting test packet/No last packet to retransmit.)
- %PIX|ASA-5-713216: Rule: action Client type : version Client: type version is/is not allowed
- %PIX|ASA-5-713229: Auto Update - Notification to client client\_ip of update string: message\_string.
- %PIX|ASA-5-713237: ACL update (access\_list) received during re-key re-authentication will not be applied to the tunnel.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute
- %ASA-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.
- %ASA-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.

- %ASA-5-713257: Phase var1 failure: Mismatched attribute types for class var2: Rcv'd: var3 Cfg'd: var4
- %PIXIASA-5-713904:descriptive\_event\_string.
- %ASA-5-716053: New SSO Server added: name: name Type: type
- %ASA-5-716054: SSO Server deleted: name: name Type: type
- %PIXIASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
- %PIXIASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %PIXIASA-5-718002: Create peer IP\_address failure, already at maximum of number\_of\_peers
- %PIXIASA-5-718005: Fail to send to IP\_address, port port
- %PIXIASA-5-718006: Invalid load balancing state transition [cur=state\_number][event=event\_number]
- %PIXIASA-5-718007: Socket open failure failure\_code
- %PIXIASA-5-718008: Socket bind failure failure\_code
- %PIXIASA-5-718009: Send HELLO response failure to IP\_address
- %PIXIASA-5-718010: Sent HELLO response to IP\_address
- %PIXIASA-5-718011: Send HELLO request failure to IP\_address
- %PIXIASA-5-718012: Sent HELLO request to IP\_address
- %PIXIASA-5-718014: Master peer IP\_address is not answering HELLO
- %PIXIASA-5-718015: Received HELLO request from IP\_address
- %PIXIASA-5-718016: Received HELLO response from IP\_address
- %PIXIASA-5-718024: Send CFG UPDATE failure to IP\_address
- %PIXIASA-5-718028: Send OOS indicator failure to IP\_address
- %PIXIASA-5-718031: Received OOS obituary for IP\_address
- %PIXIASA-5-718032: Received OOS indicator from IP\_address
- %PIXIASA-5-718033: Send TOPOLOGY indicator failure to IP\_address
- %PIXIASA-5-718042: Unable to ARP for IP\_address
- %PIXIASA-5-718043: Updating/removing duplicate peer entry IP\_address
- %PIXIASA-5-718044: Deleted peer IP\_address
- %PIXIASA-5-718045: Created peer IP\_address
- %PIXIASA-5-718048: Create of secure tunnel failure for peer IP\_address
- %PIXIASA-5-718050: Delete of secure tunnel failure for peer IP\_address
- %PIXIASA-5-718052: Received GRAT-ARP from duplicate master MAC\_address
- %PIXIASA-5-718053: Detected duplicate master, mastership stolen MAC\_address
- %PIXIASA-5-718054: Detected duplicate master MAC\_address and going to SLAVE
- %PIXIASA-5-718055: Detected duplicate master MAC\_address and staying MASTER
- %PIXIASA-5-718057: Queue send failure from ISR, msg type failure\_code
- %PIXIASA-5-718060: Inbound socket select fail: context=context\_ID.

- %PIX|ASA-5-718061: Inbound socket read fail: context=context\_ID.
- %PIX|ASA-5-718062: Inbound thread is awake (context=context\_ID).
- %PIX|ASA-5-718063: Interface interface\_name is down.
- %PIX|ASA-5-718064: Admin. interface interface\_name is down.
- %PIX|ASA-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB\_state, master=IP\_address, session=Enable/Disable).
- %PIX|ASA-5-718066: Cannot add secondary address to interface interface\_name, ip IP\_address.
- %PIX|ASA-5-718067: Cannot delete secondary address to interface interface\_name, ip IP\_address.
- %PIX|ASA-5-718068: Start VPN Load Balancing in context context\_ID.
- %PIX|ASA-5-718069: Stop VPN Load Balancing in context context\_ID.
- %PIX|ASA-5-718070: Reset VPN Load Balancing in context context\_ID.
- %PIX|ASA-5-718071: Terminate VPN Load Balancing in context context\_ID.
- %PIX|ASA-5-718072: Becoming master of Load Balancing in context context\_ID.
- %PIX|ASA-5-718073: Becoming slave of Load Balancing in context context\_ID.
- %PIX|ASA-5-718074: Fail to create access list for peer context\_ID.
- %PIX|ASA-5-718075: Peer IP\_address access list not set.
- %PIX|ASA-5-718076: Fail to create tunnel group for peer IP\_address.
- %PIX|ASA-5-718077: Fail to delete tunnel group for peer IP\_address.
- %PIX|ASA-5-718078: Fail to create crypto map for peer IP\_address.
- %PIX|ASA-5-718079: Fail to delete crypto map for peer IP\_address.
- %PIX|ASA-5-718080: Fail to create crypto policy for peer IP\_address.
- %PIX|ASA-5-718081: Fail to delete crypto policy for peer IP\_address.
- %PIX|ASA-5-718084: Public/cluster IP not on the same subnet: public IP\_address, mask netmask, cluster IP\_address
- %PIX|ASA-5-718085: Interface interface\_name has no IP address defined.
- %PIX|ASA-5-718086: Fail to install LB NP rules: type rule\_type, dst interface\_name, port port.
- %PIX|ASA-5-718087: Fail to delete LB NP rules: type rule\_type, rule rule\_ID.
- %ASA-5-719014: Email Proxy is changing listen port from old\_port to new\_port for mail protocol protocol.
- %ASA-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %ASA-5-720017: (VPN-unit) Failed to update LB runtime data
- %ASA-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %ASA-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %ASA-5-720020: (VPN-unit) Failed to send type timer message.
- %ASA-5-720021: (VPN-unit) HA non-block send failed for peer msg message\_number. HA error code.
- %ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle
- %ASA-5-720036: (VPN-unit) Failed to process state update message from the active peer.

- %ASA-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %ASA-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %ASA-5-722037: Group group User user-name IP IP\_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP\_address SVC terminating session: reason.
- %ASA-5-722005: Group group User user-name IP IP\_address Unable to update session information for SVC connection.
- %ASA-5-722006: Group group User user-name IP IP\_address Invalid address IP\_address assigned to SVC connection.
- %ASA-5-722010: Group group User user-name IP IP\_address SVC Message: type-num/NOTICE: message
- %ASA-5-722011: Group group User user-name IP IP\_address SVC Message: type-num/NOTICE: message
- %ASA-5-722012: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-5-722028: Group group User user-name IP IP\_address Stale SVC connection closed.
- %ASA-5-722032: Group group User user-name IP IP\_address New SVC connection replacing old connection.
- %ASA-5-722033: Group group User user-name IP IP\_address First SVC connection established for SVC session.
- %ASA-5-722034: Group group User user-name IP IP\_address New SVC connection, no existing connection.
- %ASA-5-722037: Group group User user-name IP IP\_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP\_address SVC terminating session: reason.

## Informational Messages, Severity 6

The following messages appear at severity 6, informational:

- %PIXIASA-6-106012: Deny IP from IP\_address to IP\_address, IP options hex.
- %PIXIASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.
- %PIXIASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol
- %PIXIASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol
- %PIXIASA-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})
- %PIXIASA-6-108005: action\_class: Received ESMTTP req\_resp from src\_ifc:siplsport to dest\_ifc:dipldport;further\_info
- %ASA-6-108007: TLS started on ESMTTP session between client client-side interface-name: clientIP address/client port and server server-side interface-name: server IP address/server port

- %PIX|ASA-6-109001: Auth start for user user from inside\_address/inside\_port to outside\_address/outside\_port
- %PIX|ASA-6-109002: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (server IP\_address failed) on interface interface\_name.
- %PIX|ASA-6-109003: Auth from inside\_address to outside\_address/outside\_port failed (all servers failed) on interface interface\_name.
- %PIX|ASA-6-109005: Authentication succeeded for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %PIX|ASA-6-109006: Authentication failed for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %PIX|ASA-6-109007: Authorization permitted for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %PIX|ASA-6-109008: Authorization denied for user user from outside\_address/outside\_port to inside\_address/ inside\_port on interface interface\_name.
- %PIX|ASA-6-109024: Authorization denied from source\_address/source\_port to dest\_address/dest\_port (not authenticated) on interface interface\_name using protocol
- %PIX|ASA-6-109025: Authorization denied (acl=acl\_ID) for user 'user' from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name using protocol
- %PIX|ASA-6-110001: No route to dest\_address from source\_address
- %PIX|ASA-6-113003: AAA group policy for user user is being set to policy\_name.
- %PIX|ASA-6-113004: AAA user aaa\_type Successful: server = server\_IP\_address, User = user
- %PIX|ASA-6-113005: AAA user authentication Rejected: reason = string: server = server\_IP\_address, User = user
- %PIX|ASA-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %PIX|ASA-6-113007: User user unlocked by administrator
- %PIX|ASA-6-113008: AAA transaction status ACCEPT: user = user
- %PIX|ASA-6-113009: AAA retrieved default group policy policy for user user
- %PIX|ASA-6-113010: AAA challenge received for user user from server server\_IP\_address
- %PIX|ASA-6-113011: AAA retrieved user specific group policy policy for user user
- %PIX|ASA-6-113012: AAA user authentication Successful: local database : user = user
- %PIX|ASA-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %PIX|ASA-6-113014: AAA authentication server not accessible: server = server\_IP\_address: user = user
- %PIX|ASA-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user
- %PIX|ASA-6-113016: AAA credentials rejected: reason = reason: server = server\_IP\_address: user = user
- %PIX|ASA-6-113017: AAA credentials rejected: reason = reason: local database: user = user\
- %ASA-6-114004: 4GE SSM I/O Initialization start.
- %ASA-6-114005: 4GE SSM I/O Initialization end.
- %PIX|ASA-6-199002: startup completed. Beginning operation.

- %PIXIASA-6-199003: Reducing link MTU dec.
- %PIXIASA-6-199005: Startup begin
- %ASA-6-201012: Per-client embryonic connection limit exceeded curr num/limit for [input/output] packet from IP\_address/ port to ip/port on interface interface\_name
- %PIXIASA-6-210022: LU missed number updates
- %PIXIASA-6-302003: Built H245 connection for foreign\_address outside\_address/outside\_port local\_address inside\_address/inside\_port
- %PIXIASA-6-302004: Pre-allocate H323 UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port
- %PIXIASA-6-302009: Rebuilt TCP connection number for foreign\_address outside\_address/outside\_port global\_address global\_address/global\_port local\_address inside\_address/inside\_port
- %PIXIASA-6-302010: connections in use, connections most used
- %PIXIASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP\_address/port to laddr IP\_address
- %PIXIASA-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)]
- %PIXIASA-6-302014: Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason] [(user)]
- %PIXIASA-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)]
- %PIXIASA-6-302016: Teardown UDP connection number for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [(user)]
- %PIXIASA-6-302017: Built {inbound/outbound} GRE connection id from interface:real\_address (translated\_address) to interface:real\_address/real\_cid (translated\_address/translated\_cid)[(user)]
- %PIXIASA-6-302018: Teardown GRE connection id from interface:real\_address (translated\_address) to interface:real\_address/real\_cid (translated\_address/translated\_cid) duration hh:mm:ss bytes bytes [(user)]
- %PIXIASA-6-302020: Built {in | out}bound ICMP connection for faddr {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr
- %PIXIASA-6-302021: Teardown ICMP connection for faddr {faddr | icmp\_seq\_num} gaddr {gaddr | cmp\_type} laddr laddr
- PIX-6-303002: FTP connection from src\_ifc:src\_ip/src\_port to
- %PIXIASA-6-304004: URL Server IP\_address request failed URL url
- %PIXIASA-6-305007: addrpool\_free(): Orphan IP IP\_address on interface interface\_number
- %PIXIASA-6-305009: Built {dynamic/static} translation from interface\_name [(acl-name)]:real\_address to interface\_name:mapped\_address
- %PIXIASA-6-305010: Teardown {dynamic/static} translation from interface\_name:real\_address to interface\_name:mapped\_address duration time
- %PIXIASA-6-305011: Built {dynamic/static} {TCPI/UDP/ICMP} translation from interface\_name:real\_address/real\_port to interface\_name:mapped\_address/mapped\_port

- %PIX|ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface\_name [(acl-name)];real\_address/{real\_port|real\_ICMP\_ID}to interface\_name:mapped\_address/{mapped\_port|mapped\_ICMP\_ID} duration time
- %PIX|ASA-6-308001: console enable password incorrect for number tries (from IP\_address)
- %PIX|ASA-6-311001: LU loading standby start
- %PIX|ASA-6-311002: LU loading standby end
- %PIX|ASA-6-311003: LU recv thread up
- %PIX|ASA-6-311004: LU xmit thread up
- %PIX|ASA-6-312001: RIP hdr failed from IP\_address: cmd=string, version=number domain=string on interface interface\_name
- %PIX|ASA-6-314001: Pre-allocate RTSP UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port
- %PIX|ASA-6-315011: SSH session from IP\_address on interface interface\_name for user user disconnected by SSH server, reason: reason
- %PIX|ASA-6-321003: Resource var1 log level of var2 reached.
- %PIX|ASA-6-321004: Resource var1 rate log level of var2 reached
- %PIX|ASA-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface\_in:source\_address/source\_port to interface\_out:dest\_address/dest\_port
- %PIX|ASA-6-333001: EAP association initiated - context:EAP-context
- %PIX|ASA-6-333003: EAP association terminated - context:EAP-context
- %PIX|ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
- %PIX|ASA-6-334001: EAPoUDP association initiated - <host-address>
- %PIX|ASA-6-334004: Authentication request for NAC Clientless host - host-address
- %PIX|ASA-6-334007: EAPoUDP association terminated - host-address
- %PIX|ASA-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
- %PIX|ASA-6-335001: NAC session initialized - host-address
- %PIX|ASA-6-335004: NAC is disabled for host - host-address
- %PIX|ASA-6-335006: NAC Applying ACL:ACL-name - host-address
- %PIX|ASA-6-335009: NAC 'Revalidate' request by administrative action - host-address
- %PIX|ASA-6-335010: NAC 'Revalidate All' request by administrative action - num sessions
- %PIX|ASA-6-335011: NAC 'Revalidate Group' request by administrative action for group-name group - num sessions
- %PIX|ASA-6-335012: NAC 'Initialize' request by administrative action - host-address
- %PIX|ASA-6-335013: NAC 'Initialize All' request by administrative action - num sessions
- %PIX|ASA-6-335014: NAC 'Initialize Group' request by administrative action for group-name group - num sessions
- %ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
- %PIX|ASA-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface\_name AC:ac\_name.

- %ASA-6-410004: action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIXIASA-6-415001: HTTP - matched matched\_string in policy-map map\_name, header field count exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-6-415002: HTTP - matched matched\_string in policy-map map\_name, header field length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-6-415003: HTTP - matched matched\_string in policy-map map\_name, body length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %PIXIASA-6-415017: HTTP - matched\_string in policy-map map\_name, arguments matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-6-421002: TCPIUDP flow from interface\_name:IP\_address/port to interface\_name:IP\_address/port bypassed application checking because the protocol is not supported.
- %ASA-6-421005: interface\_name:IP\_address is counted as a user of application
- %ASA-6-421006: There are number users of application accounted during the past 24 hours.
- %ASA-6-428001: WAAS confirmed from in\_interface:src\_ip\_addr/src\_port to out\_interface:dest\_ip\_addr/dest\_port, inspection services bypassed on this connection.
- %PIXIASA-6-602101: PMTU-D packet number bytes greater than effective mtu number dest\_addr=dest\_address, src\_addr=source\_address, prot=protocol
- %PIXIASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from src\_addr with suggested PMTU of rcvd\_mtu; PMTU updated for SA with peer peer\_addr, SPI spi, tunnel name username, old PMTU old\_mtu, new PMTU new\_mtu.%PIXIASA-7-703001: H.225 message received from interface\_name:IP\_address/port to interface\_name:IP\_address/port is using an unsupported version number
- %PIXIASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from src\_addr, PMTU is unchanged because suggested PMTU of rcvd\_mtu is equal to or greater than the current PMTU of curr\_mtu, for SA with peer peer\_addr, SPI spi, tunnel name username.
- %PIXIASA-6-602303: IPSEC: An direction tunnel\_type SA (SPI=spi ) between local\_IP and remote\_IP (username) has been created.
- %PIXIASA-6-602304: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) has been deleted.
- %PIXIASA-6-603101: PPTP received out of seq or duplicate pkt, tnl\_id=number, sess\_id=number, seq=number.
- %PIXIASA-6-603102: PPP virtual interface interface\_name - user: user aaa authentication started.
- %PIXIASA-6-603103: PPP virtual interface interface\_name - user: user aaa authentication status
- %PIXIASA-6-603104: PPTP Tunnel created, tunnel\_id is number, remote\_peer\_ip is remote\_address, ppp\_virtual\_interface\_id is number, client\_dynamic\_ip is IP\_address, username is user, MPPE\_key\_strength is string
- %PIXIASA-6-603105: PPTP Tunnel deleted, tunnel\_id = number, remote\_peer\_ip= remote\_address
- %PIXIASA-6-603106: L2TP Tunnel created, tunnel\_id is number, remote\_peer\_ip is remote\_address, ppp\_virtual\_interface\_id is number, client\_dynamic\_ip is IP\_address, username is user

- %PIX|ASA-6-603107: L2TP Tunnel deleted, tunnel\_id = number, remote\_peer\_ip = remote\_address
- %PIX|ASA-6-603108: Built PPTP Tunnel at interface\_name, tunnel-id = number, remote-peer = IP\_address, virtual-interface = number, client-dynamic-ip = IP\_address, username = user, MPPE-key-strength = number
- %PIX|ASA-6-603109: Teardown PPPOE Tunnel at interface\_name, tunnel-id = number, remote-peer = IP\_address
- %PIX|ASA-6-604101: DHCP client interface interface\_name: Allocated ip = IP\_address, mask = netmask, gw = gateway\_address
- %PIX|ASA-6-604102: DHCP client interface interface\_name: address released
- %PIX|ASA-6-604103: DHCP daemon interface interface\_name: address granted MAC\_address (IP\_address)
- %PIX|ASA-6-604104: DHCP daemon interface interface\_name: address released
- %PIX|ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"
- %PIX|ASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"
- %PIX|ASA-6-606001: ASDM session number number from IP\_address started
- %PIX|ASA-6-606002: ASDM session number number from IP\_address ended
- %PIX|ASA-6-606003: ASDM logging session number id from IP\_address started id session ID assigned
- %PIX|ASA-6-606004: ASDM logging session number id from IP\_address ended
- %PIX|ASA-6-607001: Pre-allocate SIP connection\_type secondary channel for interface\_name:IP\_address/port to interface\_name:IP\_address from string message
- %PIX|ASA-6-607003: action\_class: Received SIP req\_resp req\_resp\_info from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %PIX|ASA-6-608001: Pre-allocate Skinny connection\_type secondary channel for interface\_name:IP\_address to interface\_name:IP\_address/port from string message
- %PIX|ASA-6-610101: Authorization failed: Cmd: command Cmdtype: command\_modifier
- %ASA-6-6108005: action\_class: Received ESMTP req\_resp from src\_ifc:sip/sport to dest\_ifc:dip/dport;further\_info
- %PIX|ASA-6-611101: User authentication succeeded: Uname: user
- %PIX|ASA-6-611102: User authentication failed: Uname: user
- %PIX|ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped\_address
- %PIX|ASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling
- %PIX|ASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped\_address Split Tunnel Networks: IP\_address/netmask IP\_address/netmask ...
- %PIX|ASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP\_address/netmask IP\_address/netmask ...
- %PIX|ASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP\_address Secondary DNS: IP\_address Primary WINS: IP\_address Secondary WINS: IP\_address

- %PIXIASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed
- %PIXIASA-6-611307: VPNClient: Head end : IP\_address
- %PIXIASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string ...
- %PIXIASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP\_address
- %PIXIASA-6-611310: VNPClient: XAUTH Succeeded: Peer: IP\_address
- %PIXIASA-6-611311: VNPClient: XAUTH Failed: Peer: IP\_address
- %PIXIASA-6-611312: VPNClient: Backup Server List: reason
- %PIXIASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP\_address has redirected the to server IP\_address
- %PIXIASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP\_address
- %PIXIASA-6-611316: VPNClient: Secure Unit Authentication Enabled
- %PIXIASA-6-611317: VPNClient: Secure Unit Authentication Disabled
- %PIXIASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP\_address Auth Server Port: port Idle Timeout: time
- %PIXIASA-6-611319: VPNClient: User Authentication Disabled
- %PIXIASA-6-611320: VPNClient: Device Pass Thru Enabled
- %PIXIASA-6-611321: VPNClient: Device Pass Thru Disabled
- %PIXIASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled
- %PIXIASA-6-611323: VPNClient: Duplicate split nw entry
- %PIXIASA-6-613001: Checksum Failure in database in area string Link State Id IP\_address Old Checksum number New Checksum number
- %PIXIASA-6-613002: interface interface\_name has zero bandwidth
- %PIXIASA-6-613003: IP\_address netmask changed from area string to area string
- %PIXIASA-6-614001: Split DNS: request patched from server: IP\_address to server: IP\_address
- %PIXIASA-6-614002: Split DNS: reply from server:IP\_address reverse patched back to original server:IP\_address
- %PIXIASA-6-615001: vlan number not available for firewall interface
- %PIXIASA-6-615002: vlan number available for firewall interface
- %PIXIASA-6-616001:Pre-allocate MGCP data\_channel connection for inside\_interface:inside\_address to outside\_interface:outside\_address/port from message\_type message
- %PIXIASA-6-617001: GTPv version msg\_type from source\_interface:source\_address/source\_port not accepted by source\_interface:dest\_address/dest\_port
- %PIXIASA-6-617002: Removing v1 PDP Context with TID tid from GGSN IP\_address and SGSN IP\_address, Reason: reason or Removing v1 primary/secondary PDP Context with TID tid from GGSN IP\_address and SGSN IP\_address, Reason: reason
- %PIXIASA-6-617003: GTP Tunnel created from source\_interface:source\_address/source\_port to source\_interface:dest\_address/dest\_port

- %PIX|ASA-6-617004: GTP connection created for response from source\_interface:source\_address/0 to source\_interface:dest\_address/dest\_port
- PIX|ASA-6-617100: Teardown num\_conns connection(s) for user user\_ip
- %PIX|ASA-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for interface\_name:outside\_address[/outside\_port] to interface\_name:inside\_address[/inside\_port] from CTIQBE\_message\_name message
- %PIX|ASA-6-621001: Interface interface\_name does not support multicast, not enabled
- %PIX|ASA-6-621002: Interface interface\_name does not support multicast, not enabled
- %PIX|ASA-6-621003: The event queue size has exceeded number
- %PIX|ASA-6-621006: Mrib disconnected, (IP\_address,IP\_address) event cancelled
- %PIX|ASA-6-621007: Bad register from interface\_name:IP\_address to IP\_address for (IP\_address, IP\_address)
- %PIX-6-621008 AutoRP: discard string on interface interface-name from address due to incorrect version.
- %PIX-6-621009 AutoRP: discard string on interface interface-name from address due to incorrect type number
- %PIX-6-621010 AutoRP: discard string on interface interface-name from address due to zero RP count
- %PIX|ASA-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %PIX|ASA-6-622101: Starting regex table compilation for match\_command; table entries = regex\_num entries
- %PIX|ASA-6-622102: Completed regex table compilation for match\_command; table size = num bytes
- %PIX|ASA-6-713128: Connection attempt to VCPIP redirected to VCA peer IP\_address via load balancing
- %PIX|ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP\_address, mask: netmask
- %PIX|ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP\_address, mask: netmask
- %PIX|ASA-6-713172: Automatic NAT Detection Status: Remote end is/is not behind a NAT device This end is/is not behind a NAT device
- %PIX|ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host\_name Address IP\_address, Protocol protocol, Port port
- %PIX|ASA-6-713184: Client Type: Client\_type Client Application Version: Application\_version\_string
- %PIX|ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: IP\_address, mask: netmask
- %PIX|ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP\_address, mask: netmask
- %PIX|ASA-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default

- %PIXIASA-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %PIXIASA-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.
- %PIXIASA-6-713228: Group = group, Username = uname, IP = remote\_IP\_address Assigned private IP address assigned\_private\_IP to remote user
- %ASA-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.
- %PIXIASA-6-713905:descriptive\_event\_string.
- %ASA-6-716001: Group group User user IP ip WebVPN session started.
- %ASA-6-716002: Group group User user IP ip WebVPN session terminated: User requested.
- %ASA-6-716003: Group group User user IP ip WebVPN access “GRANTED:: url”
- %ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %ASA-6-716006: Group name User user WebVPN session terminated. Idle timeout.
- %ASA-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
- %PIXIASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint\_name.
- %ASA-6-716038: Group group User user IP ip Authentication: successful, Session Type: WebVPN.
- %ASA-6-716039: Authentication: rejected, group = name user = user, Session Type: WebVPN
- %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.
- %ASA-6-716041: access-list acl\_ID action url url hit\_cnt count
- %ASA-6-716042: access-list acl\_ID action tcp source\_interface/source\_address (source\_port) -> dest\_interface/dest\_address(dest\_port) hit-cnt count
- %ASA-6-716043 Group group-name, User user-name, IP IP\_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings.
- %ASA-6-716049: Group group-name User user-name IP IP\_address Empty SVC ACL.
- %ASA-6-716050: Error adding to ACL: ace\_command\_line
- %ASA-6-716051: Group group-name User user-name IP IP\_address Error adding dynamic ACL for user.
- %ASA-6-716055: Group group-name User user-name IP IP\_address Authentication to SSO server name: name type type succeeded
- %ASA-6-724004: Group group-policy, User user-name, IP IP\_address: Secure Desktop Results: WEB\_ACCESS = effective\_permission == secure\_desktop\_permission & group-policy permission, FILE\_ACCESS = effective\_permission == secure\_desktop\_permission & group-policy permission, PORT\_FORWARDING == effective\_permission == secure\_desktop\_permission & group-policy permission, SSL\_VPN\_CLIENT = effective\_permission == secure\_desktop\_permission & group-policy permission, GROUP\_POLICY = results
- %PIXIASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint\_name.
- %PIXIASA-6-717004: PKCS #12 export failed for trustpoint trustpoint\_name.
- %PIXIASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint\_name.
- %PIXIASA-6-717006: PKCS #12 import failed for trustpoint trustpoint\_name.

- %PIX|ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint\_name.
- %PIX|ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %PIX|ASA-6-717022 Certificate was successfully validated. certificate\_identifiers
- %PIX|ASA-6-717028 Certificate chain was successfully validated additional info.
- %PIX|ASA-6-717033 OCSP response status - Successful.
- %PIX|ASA-6-718003: Got unknown peer message message\_number from IP\_address, local version version\_number, remote version version\_number
- %PIX|ASA-6-718004: Got unknown internal message message\_number
- %PIX|ASA-6-718013: Peer IP\_address is not answering HELLO
- %PIX|ASA-6-718027: Received unexpected KEEPALIVE request from IP\_address
- %PIX|ASA-6-718030: Received planned OOS from IP\_address
- %PIX|ASA-6-718037: Master processed number\_of\_timeouts timeouts
- %PIX|ASA-6-718038: Slave processed number\_of\_timeouts timeouts
- %PIX|ASA-6-718039: Process dead peer IP\_address
- %PIX|ASA-6-718040: Timed-out exchange ID exchange\_ID not found
- %PIX|ASA-6-718051: Deleted secure tunnel to peer IP\_address
- %ASA-6-719001: Email Proxy session could not be established: session limit of maximum\_sessions has been reached.
- %ASA-6-719003: Email Proxy session pointer resources have been freed for source\_address.
- %ASA-6-719004: Email Proxy session pointer has been successfully established for source\_address.
- %ASA-6-719010: protocol Email Proxy feature is disabled on interface interface\_name.
- %ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface\_name.
- %ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %ASA-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %ASA-6-719018: WebVPN user: vpnuser ACL ID acl\_ID not found
- %ASA-6-719019: WebVPN user: vpnuser authorization failed.
- %ASA-6-719020: WebVPN user vpnuser authorization completed successfully.
- %ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.
- %ASA-6-719022: WebVPN user vpnuser has been authenticated.
- %ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
- %ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source\_address
- %ASA-6-719025: Email Proxy DNS name resolution failed for hostname.
- %ASA-6-719026: Email Proxy DNS name hostname resolved to IP\_address.
- %ASA-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %ASA-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully

- %ASA-6-720004: (VPN-unit) VPN failover main thread started.
- %ASA-6-720005: (VPN-unit) VPN failover timer thread started.
- %ASA-6-720006: (VPN-unit) VPN failover sync thread started.
- %ASA-6-720010: (VPN-unit) VPN failover client is being disabled
- %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
- %ASA-6-722013: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-720014: (VPN-unit) Phase 2 connection entry (msg\_id=message\_number, my cookie=mine, his cookie=his) contains no SA list.
- %ASA-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg\_id=message\_number,my cookie=mine, his cookie=his).
- %ASA-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %ASA-6-720024: (VPN-unit) HA status callback: Control channel is status.
- %ASA-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %ASA-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %ASA-6-720027: (VPN-unit) HA status callback: My state state.
- %ASA-6-720028: (VPN-unit) HA status callback: Peer state state.
- %ASA-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %ASA-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %ASA-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence\_#, grp=group, event=event, op=operand, my=my\_state, peer=peer\_state.
- %ASA-6-720037: (VPN-unit) HA progression callback: id=id,seq=sequence\_number,grp=group,event=event,op=operand, my=my\_state,peer=peer\_state.
- %ASA-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %ASA-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %ASA-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %ASA-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %ASA-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %ASA-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %ASA-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %ASA-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %ASA-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %ASA-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %ASA-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %ASA-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %ASA-6-722013: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-722014: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message

- %ASA-6-722022: TunnelGroup tunnel\_group GroupPolicy group\_policy User user-name IP IP\_address No address available for SVC connection
- %ASA-6-722023: Group group User user-name IP IP\_address SVC connection terminated {with/without} compression
- %ASA-6-722024: SVC Global Compression Enabled
- %ASA-6-722025: SVC Global Compression Disabled
- %ASA-6-722026: Group group User user-name IP IP\_address SVC compression history reset
- %ASA-6-722027: Group group User user-name IP IP\_address SVC decompression history reset
- %ASA-6-723001: Group group-name, User user-name, IP IP\_address: WebVPN Citrix ICA connection connection is up.
- %ASA-6-723002: Group group-name, User user-name, IP IP\_address: WebVPN Citrix ICA connection SG\_ID is down, reason reason\_string.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-6-725001 Starting SSL handshake with remote\_device interface\_name:IP\_address/port for SSL\_version session.
- %ASA-6-725002 Device completed SSL handshake with remote\_device interface\_name:IP\_address/port
- %ASA-6-725003 SSL client interface\_name: IP\_address/port requesting to resume previous session.
- %ASA-6-725004 Device requesting certificate from SSL client interface\_name:IP\_address/port for authentication.
- %ASA-6-725005 SSL server interface\_name:IP\_address/port requesting our device certificate for authentication.
- %ASA-6-725006 Device failed SSL handshake with remote\_device interface\_name:IP\_address/port
- %ASA-6-725007 SSL session with remote\_device interface\_name:IP\_address/port terminated.
- %PIX|ASA-6-726001: Inspected im\_protocol im\_service Session between Client im\_client\_1 and im\_client\_2 Packet flow from src\_ifc:/sip/sport to dest\_ifc:/dip/dport Action: action Matched Class class\_map\_id class\_map\_name
- %ASA-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names

## Debugging Messages, Severity 7

The following messages appear at severity 7, debugging:

- %PIX|ASA-7-108006: Detected ESMTTP size violation from src\_ifc:sip/sport to dest\_ifc:dip/dport;declared size is: decl\_size, actual size is act\_size.
- %PIX|ASA-7-109014: A non-Telnet connection was denied to the configured virtual Telnet IP address.
- %PIX|ASA-7-109021: Uauth null proxy error
- %PIX|ASA-7-111009:User user executed cmd:string
- %PIX|ASA-7-199009: Reloaded at when by whom. Reload reason: reason

- %PIXIASA-7-304005: URL Server IP\_address request pending URL url
- %PIXIASA-7-304009: Ran out of buffer blocks specified by url-block command
- %PIXIASA-7-333004: EAP-SQ response invalid - context:EAP-context
- %PIXIASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %PIXIASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %PIXIASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %PIXIASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
- %PIXIASA-7-335007: NAC Default ACL not configured - host-address
- %ASA-7-421004: Failed to inject {TCPIUDP} packet from IP\_address/port to IP\_address/port
- %PIXIASA-7-609001: Built local-host interface\_name:IP\_address
- %PIXIASA-7-609002: Teardown local-host interface\_name:IP\_address duration time
- %PIXIASA-7-701001: alloc\_user() out of Tcp\_user objects
- %PIXIASA-7-701002: alloc\_user() out of Tcp\_proxy objects
- %PIXIASA-7-702201: ISAKMP Phase 1 delete received (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702202: ISAKMP Phase 1 delete sent (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702203: ISAKMP DPD timed out (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702204: ISAKMP Phase 1 retransmission (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702205: ISAKMP Phase 2 retransmission (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702206: ISAKMP malformed payload received (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702207: ISAKMP duplicate packet detected (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702208: ISAKMP Phase 1 exchange started (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702209: ISAKMP Phase 2 exchange started (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702210: ISAKMP Phase 1 exchange completed(local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702211: ISAKMP Phase 2 exchange completed(local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-702212: ISAKMP Phase 1 initiating rekey (local IP\_address (initiator/responder), remote IP\_address)
- %PIXIASA-7-703001: H.225 message received from interface\_name:IP\_address/port to interface\_name:IP\_address/port is using an unsupported version number
- %PIXIASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface\_name:IP\_address to interface\_name:IP\_address/port
- %PIXIASA-7-709001: FO replication failed: cmd=command returned=code

- %PIX|ASA-7-709002: FO unreplicable: cmd=command
- %PIX|ASA-7-710001: TCP access requested from source\_address/source\_port to interface\_name:dest\_address/service
- %PIX|ASA-7-710002: {TCPIUDP} access permitted from source\_address/source\_port to interface\_name:dest\_address/service
- %PIX|ASA-7-710004: TCP connection limit exceeded from Src\_ip/Src\_port to In\_name:Dest\_ip/Dest\_port (current connections/connection limit = Curr\_conn/Conn\_lmt)
- %PIX|ASA-7-710005: {TCPIUDP} request discarded from source\_address/source\_port to interface\_name:dest\_address/service
- %PIX|ASA-7-710006: protocol request discarded from source\_address to interface\_name:dest\_address
- %PIX|ASA-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86.1.129.1/4500
- %PIX|ASA-7-711001: debug\_trace\_msg
- %PIX|ASA-7-711002: Task ran for elapsed\_time msecs, process = process\_name, PC = PC Tracebeback = traceback
- %PIX|ASA-7-713024: Received local Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713026: Transmitted local Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713027: Transmitted remote Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713030: Transmitted local Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713031: Transmitted remote Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %PIX|ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %PIX|ASA-7-713039: Send failure: Bytes (number), Peer: IP\_address
- %PIX|ASA-7-713040: Could not find connection entry and can not encrypt: msgid message\_number
- %PIX|ASA-7-713052: User (user) authenticated.

- %PIXIASA-7-713066: IKE Remote Peer configured for SA: SA\_name
- %PIXIASA-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %PIXIASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %PIXIASA-7-713103: Invalid (NULL) secret key detected while computing hash
- %PIXIASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %PIXIASA-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP\_address, SA address: internal\_SA\_address, tunnel count: count
- %PIXIASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA\_internal\_address) for peer IP\_address, but cookies don't match
- %PIXIASA-7-713117: Received Invalid SPI notify (SPI SPI\_Value)!
- %PIXIASA-7-713121: Keep-alive type for this connection: keepalive\_type
- %PIXIASA-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability\_value, Version Number: version\_number, Version String: version\_text
- %PIXIASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %PIXIASA-7-713164: The Firewall Server has requested a list of active user sessions
- %PIXIASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP\_address, SA address: internal\_SA\_address, tunnelCnt: tunnel\_count
- %PIXIASA-7-713170: IKE Received delete for rekeyed centry IKE peer: IP\_address, centry address: internal\_address, msgid: id
- %PIXIASA-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %PIXIASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP\_address, Remote peer address: IP\_address
- %PIXIASA-7-713190: Got bad refCnt (ref\_count\_value) assigning IP\_address (IP\_address)
- %PIXIASA-7-713204: Adding static route for client address: IP\_address
- %PIXIASA-7-713221: Static Crypto Map check, checking map = crypto\_map\_tag, seq = seq\_number...
- %PIXIASA-7-713222: Static Crypto Map check, map = crypto\_map\_tag, seq = seq\_number, ACL does not match proxy IDs src:source\_address dst:dest\_address
- %PIXIASA-7-713223: Static Crypto Map check, map = crypto\_map\_tag, seq = seq\_number, no ACL configured
- %PIXIASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %PIXIASA-7-713225: [IKEv1], Static Crypto Map check, map map\_name, seq = sequence\_number is a successful match
- %PIXIASA-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %PIXIASA-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %PIXIASA-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %PIXIASA-7-713236: IKE\_DECODE tx/rx Message (msgid=msgid) with payloads :payload1 (payload1\_len) + payload2 (payload2\_len)...total length : tlen
- %PIXIASA-7-713900:Descriptive\_event\_string.

- %PIX|ASA-7-713901:Descriptive\_event\_string.
- %PIX|ASA-7-713906:descriptive\_event\_string.
- %PIX|ASA-7-714001: description\_of\_event\_or\_packet
- %PIX|ASA-7-714002: IKE Initiator starting QM: msg id = message\_number
- %PIX|ASA-7-714003: IKE Responder starting QM: msg id = message\_number
- %PIX|ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message\_number
- %PIX|ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message\_number
- %PIX|ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message\_number
- %PIX|ASA-7-714007: IKE Initiator sending Initial Contact
- %PIX|ASA-7-714011: Description of received ID values
- %PIX|ASA-7-715001: Descriptive statement
- %PIX|ASA-7-715004: subroutine name() Q Send failure: RetCode (return\_code)
- %PIX|ASA-7-715005: subroutine name() Bad message code: Code (message\_code)
- %PIX|ASA-7-715006: IKE got SPI from key engine: SPI = SPI\_value
- %PIX|ASA-7-715007: IKE got a KEY\_ADD msg for SA: SPI = SPI\_value
- %PIX|ASA-7-715008: Could not delete SA SA\_address, refCnt = number, caller = calling\_subroutine\_address
- %PIX|ASA-7-715009: IKE Deleting SA: Remote Proxy IP\_address, Local Proxy IP\_address
- %PIX|ASA-7-715013: Tunnel negotiation in progress for destination IP\_address, discarding data
- %PIX|ASA-7-715019: IKEGetUserAttributes: Attribute name = name
- %PIX|ASA-7-715020: construct\_cfg\_set: Attribute name = name
- %PIX|ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %PIX|ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %PIX|ASA-7-715027: IPSec SA Proposal # chosen\_proposal, Transform # chosen\_transform acceptable Matches global IPSec SA entry # crypto\_map\_index
- %PIX|ASA-7-715028: IKE SA Proposal # 1, Transform # chosen\_transform acceptable Matches global IKE entry # crypto\_map\_index
- %PIX|ASA-7-715033: Processing CONNECTED notify (MsgId message\_number)
- %PIX|ASA-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.
- %PIX|ASA-7-715035: Starting IOS keepalive monitor: seconds sec.
- %PIX|ASA-7-715036: Sending keep-alive of type notify\_type (seq number number)
- %PIX|ASA-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %PIX|ASA-7-715038: action Spoofing\_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %PIX|ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %PIX|ASA-7-715040: Deleting active auth handle during SA deletion: handle = internal\_authentication\_handle
- %PIX|ASA-7-715041: Received keep-alive of type keepalive\_type, not the negotiated type

- %PIXIASA-7-715042: IKE received response of type failure\_type to a request from the IP\_address utility
- %PIXIASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %PIXIASA-7-715045: ERROR: malformed Keepalive payload
- %PIXIASA-7-715046: Group = groupname, Username = username, IP = IP\_address, constructing payload\_description payload
- %PIXIASA-7-715047: processing payload\_description payload
- %PIXIASA-7-715048: Send VID\_type VID
- %PIXIASA-7-715049: Received VID\_type VID
- %PIXIASA-7-715050: Claims to be IOS but failed authentication
- %PIXIASA-7-715051: Received unexpected TLV type TLV\_type while processing FWTYPE ModeCfg Reply
- %PIXIASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %PIXIASA-7-715053: MODE\_CFG: Received request for attribute\_info!
- %PIXIASA-7-715054: MODE\_CFG: Received attribute\_name reply: value
- %PIXIASA-7-715055: Send attribute\_name
- %PIXIASA-7-715056: Client is configured for TCP\_transparency
- %PIXIASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %PIXIASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %PIXIASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %PIXIASA-7-715060: Dropped received IKE fragment. Reason: reason
- %PIXIASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %PIXIASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
- %PIXIASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %PIXIASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %PIXIASA-7-715065: IKE state\_machine subtype FSM error history (struct data\_structure\_address) state, event: state/event pairs
- %PIXIASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %PIXIASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %PIXIASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %PIXIASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %PIXIASA-7-715069: Invalid ESP SPI size of SPI\_size
- %PIXIASA-7-715070: Invalid IPComp SPI size of SPI\_size
- %PIXIASA-7-715071: AH proposal not supported
- %PIXIASA-7-715072: Received proposal with unknown protocol ID protocol\_ID
- %PIXIASA-7-715074: Could not retrieve authentication attributes for peer IP\_address

- %PIX|ASA-7-715075: Group = group\_name, Username = client, IP = IP\_address Received keep-alive of type message\_type (seq number number)
- %PIX|ASA-7-715076: Computing hash for ISAKMP
- %PIX|ASA-7-715077: Pitcher: msg string, spi spi
- %PIX-7-715078: META-DATA Received type LAM attribute.
- %PIX-7-715079: META-DATA INTERNAL\_ADDRESS: Received request for type.
- %ASA-7-715080: Starting P2 rekey timer: 28800 seconds.
- %ASA-7-716008: WebVPN ACL: action
- %ASA-7-716010: Group group User user Browse network.
- %ASA-7-716011: Group group User user Browse domain domain.
- %ASA-7-716012: Group group User user Browse directory directory.
- %ASA-7-716013: Group group User user Close file filename.
- %ASA-7-716014: Group group User user View file filename.
- %ASA-7-716015: Group group User user Remove file filename.
- %ASA-7-716016: Group group User user Rename file old\_filename to new\_filename.
- %ASA-7-716017: Group group User user Modify file filename.
- %ASA-7-716018: Group group User user Create file filename.
- %ASA-7-716019: Group group User user Create directory directory.
- %ASA-7-716020: Group group User user Remove directory directory.
- %ASA-7-716021: File access DENIED, filename.
- %ASA-7-716024: Group name User user Unable to browse the network.Error: description
- %ASA-7-716025: Group name User user Unable to browse domain domain. Error: description
- %ASA-7-716026: Group name User user Unable to browse directory directory. Error: description
- %ASA-7-716027: Group name User user Unable to view file filename. Error: description
- %ASA-7-716028: Group name User user Unable to remove file filename. Error: description
- %ASA-7-716029: Group name User user Unable to rename file filename. Error: description
- %ASA-7-716030: Group name User user Unable to modify file filename. Error: description
- %ASA-7-716031: Group name User user Unable to create file filename. Error: description
- %ASA-7-716032: Group name User user Unable to create folder folder. Error: description
- %ASA-7-716033: Group name User user Unable to remove folder folder. Error: description
- %ASA-7-716034: Group name User user Unable to write to file filename.
- %ASA-7-716035: Group name User user Unable to read file filename.
- %ASA-7-716036: Group name User user File Access: User user logged into the server server.
- %ASA-7-716037: Group name User user File Access: User user failed to login into the server server.
- %PIX|ASA-7-717024 Checking CRL from trustpoint: trustpoint name for purpose
- %PIX|ASA-7-717025 Validating certificate chain containing number of certs certificate(s).
- %PIX|ASA-7-717029 Identified client certificate within certificate chain. serial number: serial\_number, subject name: subject\_name.

- %PIXIASA-7-717030 Found a suitable trustpoint trustpoint name to validate certificate.
- %PIXIASA-7-717034 No-check extension found in certificate. OCSP check bypassed.
- PIXIASA-7-717036 Looking for a tunnel group match based on certificate maps for peer certificate with certificate\_identifier.
- %PIXIASA-7-717038 Tunnel group match found. Tunnel Group: tunnel\_group\_name, Peer certificate: certificate\_identifier.
- %PIXIASA-7-718001: Internal interprocess communication queue send failure: code error\_code
- %PIXIASA-7-718017: Got timeout for unknown peer IP\_address msg type message\_type
- %PIXIASA-7-718018: Send KEEPALIVE request failure to IP\_address
- %PIXIASA-7-718019: Sent KEEPALIVE request to IP\_address
- %PIXIASA-7-718020: Send KEEPALIVE response failure to IP\_address
- %PIXIASA-7-718021: Sent KEEPALIVE response to IP\_address
- %PIXIASA-7-718022: Received KEEPALIVE request from IP\_address
- %PIXIASA-7-718023: Received KEEPALIVE response from IP\_address
- %PIXIASA-7-718025: Sent CFG UPDATE to IP\_address
- %PIXIASA-7-718026: Received CFG UPDATE from IP\_address
- %PIXIASA-7-718029: Sent OOS indicator to IP\_address
- %PIXIASA-7-718034: Sent TOPOLOGY indicator to IP\_address
- %PIXIASA-7-718035: Received TOPOLOGY indicator from IP\_address
- %PIXIASA-7-718036: Process timeout for req-type type\_value, exid exchange\_ID, peer IP\_address
- %PIXIASA-7-718041: Timeout [msgType=type] processed with no callback
- %PIXIASA-7-718046: Create group policy policy\_name
- %PIXIASA-7-718047: Fail to create group policy policy\_name
- %PIXIASA-7-718049: Created secure tunnel to peer IP\_address
- %PIXIASA-7-718056: Deleted Master peer, IP IP\_address
- %PIXIASA-7-718058: State machine return code: action\_routine, return\_code
- %PIXIASA-7-718059: State machine function trace: state=state\_name, event=event\_name, func=action\_routine
- %PIXIASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC\_address.
- %ASA-7-719005: FSM NAME has been created using protocol for session pointer from source\_address.
- %ASA-7-719006: Email Proxy session pointer has timed out for source\_address because of network congestion.
- %ASA-7-719007: Email Proxy session pointer cannot be found for source\_address.
- %ASA-7-719009: Email Proxy service is starting.
- %ASA-7-719015: Parsed emailproxy session pointer from source\_address username: mailuser = mail\_user, vpnuser = VPN\_user, mailserver = server
- %ASA-7-719016: Parsed emailproxy session pointer from source\_address password: mailpass = \*\*\*\*\* , vpnpass= \*\*\*\*\*
- %ASA-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event\_ID.

- %ASA-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %ASA-7-720041: (VPN-unit) Sending type message id to standby unit
- %ASA-7-720042: (VPN-unit) Receiving type message id from active unit
- %ASA-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %ASA-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %ASA-7-720050: (VPN-unit) Failed to remove timer. ID = id.
- %ASA-7-722029: Group group User user-name IP IP\_address SVC Session Termination: Conns: connections, DPD Conns: DPD\_conns, Comp resets: compression\_resets, Dcmp resets: decompression\_resets
- %ASA-7-722030: Group group User user-name IP IP\_address SVC Session Termination: In: data\_bytes (+ctrl\_bytes) bytes, data\_pkts (+ctrl\_pkts) packets, drop\_pkts drops
- %ASA-7-722031: Group group User user-name IP IP\_address SVC Session Termination: Out: data\_bytes (+ctrl\_bytes) bytes, data\_pkts (+ctrl\_pkts) packets, drop\_pkts drops.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-7-723004: WebVPN Citrix encountered bad flow control flow.
- %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %ASA-7-723006: WebVPN Citrix SOCKS errors.
- %ASA-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %ASA-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %ASA-7-723009: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received data on invalid connection connection.
- %ASA-7-723010: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %ASA-7-723011: Group group-name, User user-name, IP IP\_address: WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.
- %ASA-7-723012: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received bad SOCKS socks message format.
- %ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
- %ASA-7-723014: Group group-name, User user-name, IP IP\_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %ASA-7-725008 SSL client interface\_name:IP\_address/port proposes the following number cipher(s).
- %ASA-7-725009 Device proposes the following number cipher(s) to SSL server interface\_name:IP\_address/port.
- %ASA-7-725010 Device supports the following number cipher(s).
- %ASA-7-725011 Cipher[order] : cipher\_name
- %ASA-7-725012 Device chooses cipher : cipher\_name for SSL session with client interface\_name:IP\_address/port
- %ASA-7-725013 SSL Server interface\_name:IP\_address/port chooses cipher : cipher\_name
- %ASA-7-725014 SSL lib error. Function: function Reason: reason

