

# PIX/ASA Security Appliance FAQ

Document ID: 68330

## Questions

**Introduction**

**Compatibility with Software Version**

**Configuration Issues**

**Software Upgrade Issues**

**Connectivity issues**

**ASDM Related**

**Supported Features**

**Failover**

**Error Messages**

**Related Information**

## Introduction

This document provides answers to the most frequently asked questions (FAQs) related to Cisco Security Appliances, such as the PIX 500 series and the ASA 5500 series appliances.

The target audience for this document is a security appliance administrator who understands CLI commands and features and has experience with the configuration of earlier PIX software versions.

## Compatibility with Software Version

### Q. Which devices support PIX 7.x?

A. PIX 515, PIX 515E, PIX 525, PIX 535 and all of the Cisco ASA 5500 Series Adaptive Security Appliances (ASA 5510, ASA 5520, and ASA 5540) support software version 7.x and later.

The PIX 501, PIX 506E, and PIX 520 Security Appliances are not supported in software version 7.x.

### Q. I have a PIX 515/515E model that runs on software version 6.x, and I want to upgrade to 7.x. Is this possible?

A. Yes, it is possible provided you have the necessary memory modules. Refer to Cisco PIX 515/515E Security Appliance Memory Upgrade for PIX Software version 7.0 for the exact memory requirements before you upgrade PIX 515/515E.

### Q. What are the changes and new features in PIX 7.0? When I upgrade from version 6.x to 7.x, are the old features taken care of automatically?

A. Refer to Changes in PIX Security Appliance Version 7.0 for details related to the changes and new features in PIX 7.0.

Most changed and deprecated features and commands are converted automatically when PIX Security Appliance 7.x boots on your system. A few features and commands require manual intervention before or during the upgrade. Refer to Changed and Deprecated Features and Commands for more information.

## Configuration Issues

### Q. How do you perform a basic configuration for Security Appliances running 7.x?

A. Refer to the Configuring Basic Settings section of Cisco Security Appliance Command Line Configuration Guide, Version 7.1.

### Q. How do I configure the interfaces in PIX 7.x?

A. PIX/ASA 7.0 is set up to resemble the router and switch Cisco IOS<sup>®</sup> as closely as possible. In PIX/ASA 7.0, the configuration reads like this:

```
interface Ethernet0
  description Outside Interface
  speed 100
  duplex full
  nameif outside
  security-level 0
  ip address 10.10.80.4 255.255.255.0 standby 10.10.80.6
```

Refer to Configuring Interface Parameters on PIX 7.0. for more information.

### Q. How do I create an access list (ACL) on the ASA or PIX?

A. An access list is made up of one or more Access Control Entries (ACE) with the same access list ID. Access lists are used to control network access or to specify traffic for many features to act upon. In order to add an ACE, use the command **access-list <ID> extended** in global configuration mode. In order to remove an ACE, use the **no** form of this command. In order to remove the entire access list, use the **clear configure access-list** command.

This **access-list** command allows all hosts (on the interface to which you apply the access list) to go through the security appliance:

```
hostname(config)#access-list ACL_IN extended permit ip any any
```

If an access list is configured to control traffic through the security appliance, it must be applied to an interface with the **access-group** command before it takes effect. Only one access list can be applied to each interface in each direction.

Enter this command in order to apply an extended access list to the inbound or outbound direction of an interface:

```
hostname(config)#access-group access_list_name {in | out} interface interface_name
[per-user-override]
```

This example shows an inbound access list applied to the inside interface that allows the network 10.0.0.0 /24 through the security appliance:

```
hostname(config)#access-list INSIDE extended permit ip 10.0.0.0 255.255.255.0 any
```

```
hostname(config)#access-group INSIDE in interface inside
```

This example shows an inbound access list applied to the outside interface that allows all hosts on the outside of the security appliance to have web access through the security appliance to the server at 172.20.1.10:

```
hostname(config)#access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www
hostname(config)#access-group OUTSIDE in interface outside
```

**Note:** Access lists contain an implicit "deny" at the end. This means that once an ACL is applied, all traffic not explicitly permitted by an ACE in the ACL is denied.

## Q. Can I use the management 0/0 interface on the ASA in order to pass traffic like any other interface?

A. Yes. Refer to the **management-only** command for more information.

## Q. What does Security Context in Security Appliance mean?

A. You can partition a single hardware PIX into multiple virtual devices, known as Security Contexts. Each context becomes an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode and include routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

## Q. How do I configure the VPN user group-lock feature on the ASA or PIX?

A. In order to configure group lock, send the group policy name in the class attribute 25 on the Remote Authentication Dial-In User Service (RADIUS) server and choose the group in order to lock the user within the policy.

For example, in order to lock the **Cisco 123** user into the **RemoteGroup** group, define the Internet Engineering Task Force (IETF) attribute 25 class *OU=RemotePolicy* for this user on the RADIUS server.

Refer to this configuration example in order to configure group lock on an Adaptive Security Appliance (ASA)/PIX:

```
group-policy RemotePolicy internal
group-policy RemotePolicy attributes
dns-server value x.x.x.x
group-lock value RemoteGroup

tunnel-group RemoteGroup type ipsec-ra
tunnel-group RemoteGroup general-attributes
address-pool cisco
authentication-server-group RADIUS-Group
default-group-policy RemotePolicy
```

**Note:** *OU* sets the group policy, and the group policy locks the user into the preferred tunnel-group.

In order to set up your Cisco Secure ACS for Windows, RADIUS server to lock a user into a particular group configured on the ASA.

## Q. How can I capture packets in PIX/ASA?

A. Packets can be captured in PIX/ASA if you use the Packet Capture feature. Refer to ASA/PIX/FWSM: Packet Capturing using CLI and ASDM Configuration Example for more information on how to configure the Packet Capture feature.

## Q. How can I redirect HTTP traffic to HTTPS on ASA?

A. Issue the **http redirect** command in global configuration mode in order specify that the security appliance redirect HTTP connections to HTTPS.

```
hostname(config)#http redirect interface [port]
```

## Q. How does an ASA learn about the MAC address of the host?

A. An ASA issues an ARP request for the host in a directly connected subnet even if it issues a SYN packet to the ASA, which has the ARP information in the layer 2 header. The firewall does not learn the MAC address of the host from the SYN packet and has to issue an ARP request for it. If the host is not replying for the ARP request, then the ASA drops the packet.

## Software Upgrade Issues

### Q. I upgraded my PIX from 6.x to 7.x. After the upgrade I noticed 8–10% higher CPU usage for the same amount of traffic? Is this increase normal?

A. PIX 7.0 has three times more syslogs and new features than the 6.x versions. Increased CPU usage compared to 6.x is normal.

## Connectivity issues

### Q. I am unable to ping outside of the outside interface while using Security Appliance 7.0. How do I fix this?

A. There are two options in PIX 7.x that allow inside users to ping outside. The first option is to setup a specific rule for each type of echo message. For example:

```
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any source-quench
access-list 101 permit icmp any any unreachable
access-list 101 permit icmp any any time-exceeded
access-group 101 in interface outside
```

This allows only these return messages through the firewall when an inside user pings to an outside host. The other types of ICMP status messages might be hostile and the firewall blocks all other ICMP messages.

Another option is to configure **icmp inspection**. This allows a trusted IP address to traverse the firewall and allows replies back to the trusted address only. This way, all inside interfaces

can ping outside and the firewall allows the replies to return. This also gives you the advantage of monitoring the ICMP traffic that traverses the firewall.

For example:

```
policy-map global_policy
  class inspection_default
    inspect icmp
```

## Q. I am unable to access the inside interface of the Security Appliance when connected via a VPN tunnel. How can I do this?

A. The inside interface of the Security Appliance cannot be accessed from the outside, and vice-versa, unless the **management-access** is configured in global configuration mode. Once **management-access** is enabled, Telnet, SSH, or HTTP access must still be configured for the desired hosts.

```
pix(config)#management-access inside
pix(config)#show running-config management-access
management-access inside
```

## Q. Why am I unable to connect IP Phone through VPN Tunnel with ASA?

A. It can be an authentication issue. Verify that the IP phone user group has authentication (X-auth) enabled.

## ASDM Related

### Q. How do I enable/access the ASDM on ASA/PIX?

A. You need to enable the HTTPS server and allow HTTPS connections to the security appliance in order to use ASDM. All of these tasks are completed if you use the **setup** command.

Refer to Allowing HTTPS Access for ASDM for more information.

## Supported Features

### Q. What are the two modes of operations in Security Appliance?

A. The PIX Security Appliance can operate in two different firewall modes:

1. **Routed mode** In routed mode, the PIX has IP addresses assigned to its interfaces and acts as a router hop for packets that pass through it. All traffic inspection and forwarding decisions are based on Layer 3 parameters. This is how PIX Firewall versions earlier than 7.0 operate.
2. **Transparent mode** In transparent mode the PIX does not have IP addresses assigned to its interfaces. Instead it acts as a Layer 2 bridge that maintains a MAC address table and makes forwarding decisions based on that. The use of full extended IP access lists is still available and the firewall can inspect IP activity at any layer. In this mode of operation the PIX is often referred to as a "bump in the wire" or "stealth firewall". There are other significant differences as to how transparent mode operates in comparison to routed mode:

- ◇ Only two interfaces are supported *inside* and *outside*
- ◇ NAT is not supported or required since the PIX is no longer a hop.

**Note:** NAT and PAT is supported in the transparent firewall for ASA/PIX releases 8.0(2) and later.

Refer to PIX/ASA: Transparent Firewall Configuration Example for more information on how to configure the Security Appliance in Transparent Mode. Refer to NAT in Transparent Mode for more information.

**Note:** Because transparent and routed modes use different approaches to security, the running configuration is cleared when the PIX is switched to transparent mode. Be sure to save your routed mode running configuration to Flash or an external server.

## **Q. Does ASA support ISP load balancing?**

**A.** No. Load balancing must be handled by a router that passes traffic to the security appliance.

## **Q. Is MD5 authentication with BGP supported through ASA?**

**A.** No, MD5 authentication is not supported through ASA, but a workaround can be to disable it. Refer to ASA/PIX: BGP through ASA Configuration Example for more information.

## **Q. Does PIX/ASA support EtherChannel/PortChannel interfaces?**

**A.** Yes, support for EtherChannel is introduced in ASA software version 8.4. You can configure up to 48 802.3ad EtherChannels of eight active interfaces each. For more information, refer to Release Notes of ASA Version 8.4.

## **Q. Can Anyconnect and Cisco VPN Client work together on ASA?**

**A.** Yes, because they are not interrelated. Anyconnect works on SSL and Cisco VPN Client works on IPSEC.

## **Q. Is ASA/PIX is able to block Skype?**

**A.** Unfortunately, the PIX/ASA is not able to block the skype traffic. Skype has the capability to negotiate dynamic ports and to use encrypted traffic. With encrypted traffic, it is virtually impossible to detect it as there are no patterns to look for.

You could eventually use a Cisco Intrusion Prevention System (IPS). It has some signatures that are able to detect a Windows Skype Client that connects to the Skype server to synchronize its version. This is usually done when the client is initiated the connection. When the sensor picks up the initial Skype connection, you can be able to find the person who use the service, and block all connections initiated from their IP address.

## **Q. Does ASA support SNMPv3?**

**A.** Yes. Cisco ASA Software Release 8.2 supports Simple Network Management Protocol (SNMP) version 3, the newest version of SNMP, and adds authentication and privacy options in order to secure protocol operations.

## **Q. Is there a way to log entries with a name instead of an IP address?**

**A.** Use the **names** command in order to enable the association of a name with an IP address. You can associate only one name with an IP address. You must first use the **names** command before you use the **name** command. Use the **name** command immediately after you use the **names** command and before you use the **write memory** command.

The **name** command allows you to identify a host by a text name and map text strings to IP addresses. Use the **clear configure name** command in order to clear the list of names from the configuration. Use the **no names** command in order to disable logging name values. Both the **name** and **names** commands are saved in the configuration.

## **Q. Is the ip accounting command available in PIX/ASA 7.x?**

**A.** No.

## **Q. Does Security Appliance 7.0 support the Are You There (AYT) feature?**

**A.** Yes. In an AYT scenario, a remote user has a personal firewall installed on the PC. The VPN Client enforces the firewall policy defined on the local firewall, and it monitors that firewall to make sure that it runs. If the firewall stops running, the VPN Client drops the connection to the PIX or ASA. This firewall enforcement mechanism is called Are You There (AYT), because the VPN Client monitors the firewall by sending it periodic "are you there?" messages. If no reply comes, the VPN Client knows the firewall is down and terminates its connection to the PIX Security Appliance. The network administrator might configure these PC firewalls originally, but with this approach, users can customize their own configurations.

## **Q. Is FTP with TLS/SSL supported through the Security Appliance?**

**A.** No. In a typical FTP connection, either the client or the server must tell the other what port to use for data transfer. The PIX is able to inspect this conversation and open that port. However, with FTP with TLS/SSL, this conversation is encrypted and the PIX is unable to determine what ports to open. Thus, the FTP with TLS/SSL connection ultimately fails.

One possible workaround in this situation is to use an FTP client that supports the use of a "clear command channel" while still using TLS/SSL to encrypt the data channel. With this option enabled, the PIX should be able to determine what port needs to be opened.

## **Q. Does the Security Appliance support DDNS?**

**A.** Yes, the Security Appliance support DDNS. Refer to Configuring Dynamic DNS for more information.

## **Q. Does the PIX support WebVPN/SSL VPN?**

**A.** No, but it is supported in the Cisco 5500 Series Adaptive Security Appliance (ASA).

## **Q. Does the PIX support Cisco AnyConnect VPN Client?**

**A.** No, it is supported only in the Cisco 5500 Series Adaptive Security Appliance (ASA).

**Q. Does the PIX support any services modules like AIP-SSM and CSC-SSM?**

A. No.

**Q. Does the Cisco Security Appliance support IPsec Manual Keying (manual encryption)?**

A. No.

**Q. Does the ASA support password management with NT?**

A. ASA does not support password management with NT.

**Note:** Security appliance supports password management for the RADIUS and LDAP protocols.

**Q. Can Cisco 5500 Series ASA do a Policy Based Routing (PBR) like Cisco Router? For example, mail traffic should be routed to first ISP while http traffic should be routed to the second one.**

A. Unfortunately, there is no way to do policy-based routing on the ASA at this time. It can be a feature that is added to the ASA in the future.

**Note:** The **route-map** command is used to redistribute routes between routing protocols, such as OSPF and RIP, with the use of metrics and not to policy route regular traffic as in routers.

**Q. Can I use ASA 5510 as an Easy VPN Client?**

A. No. Easy VPN client configuration is only supported on ASA 5505.

**Q. Does ASA supports Asymmetric routing ?**

A. ASA supports Asymmetric routing in version 8.2(1) and later. It is not supported in ASA versions before 8.2(1).

**Q. Can I configure dynamic routing over VPN tunnel on ASA?**

A. No. This is possible only by using tunnel interfaces, which are not yet supported on ASA.

**Q. Does ASA support PPTP client?**

A. No.

**Q. Does ASA support QOS marking the packet with DSCP value?**

A. No, it supports only matching the DSCP traffic and pass it to next hop devices without changing the DSCP values. Refer to DSCP and DiffServ Preservation for more information.

**Q. Which IPsec transforms (ESP, AH) are supported on the ASA/PIX versions 7.0 and later?**

A. Only IPsec Encapsulating Security Payload (ESP) encryption and authentication is supported. Authentication Header (AH) transforms are not supported on the ASA/PIX versions 7.0 and later.

**Q. Does ASA support Universal Plug and Play (UPnP) feature?**

A. No, ASA does not support Universal Plug and Play (UPnP) feature as of now.

**Q. Does ASA support source-based routing?**

A. No.

**Q. Does H.329 traffic pass through PIX/ASA 8.1 and later?**

A. No.

**Q. Does ASA support H.460 protocol inspection?**

A. No.

**Q. Does ASA support EXEC Authorization, which logs the user directly into enable mode after authentication?**

A. No, EXEC Authorization feature is not supported in ASA.

**Q. Does ASA allow Broadcast traffic to pass through its interface?**

A. No.

**Q. Is it possible to configure two-factor L2L VPN authentication between 5505 ASAs?**

A. Two-factor authentication can be configured beginning with ASA version 8.2.x only for AnyConnect and SSL VPN. You cannot configure two-factor authentication for L2L VPN.

**Q. Is it possible to add two phone proxies on the same ASA?**

A. No. It is not possible to add two phone proxies on the same ASA as ASA does not support this.

**Q. Does the ASA support the NetFlow configuration?**

A. Yes, this feature is supported in Cisco ASA version 8.1.x and later. For complete implementation details, refer to the Cisco NetFlow Implementation Guides. For a complete configuration summary, refer to the *Configuration Examples for NewFlow Secure Event Logging* section of Configuring NetFlow Secure Event Logging.

## **Q. Does ASA support Sharepoint?**

**A.** ASA 7.1 and 7.2 do not support Sharepoint. Support for Sharepoint 2003 (2.0 and 3.0) starts with ASA version 8.x. Editing Office documents for Sharepoint 2.0 and 3.0 in a pureclientless mode (no smarttunnels, no port forwarder) is also supported. Smart-tunnels can be used as well, as of ASA 8.0.4. All basic features supported for Sharepoint 2003 in 8.0 are supported for 2007 in ASA version 8.2 5.

## **Q. Does the ASA support the native L2TP/IPsec Client on Android devices?**

**A.** The Android is not fully RFC compliant and supported by Cisco ASA starting with version 8.4.1. For more information, refer to Supported Clients.

## **Q. What is the maximum number of ACLs that can be configured on the ASA?**

**A.** There is no defined limit for the number of ACLs that can be configured on the ASA. It depends on the memory present in the ASA.

## **Q. Can I backup the ASA configuration through SNMP?**

**A.** No. In order to achieve this, you need to use SNMP writenet, which requires **Cisco Config Copy MIB**. Currently, this is not supported because this specific MIB is not supported by Cisco ASA.

## **Q. I cannot initiate a laptop presentation during a video conference call between Cisco Video Units. The video call works fine, but the video presentation from the laptop does not work. How is this issue resolved?**

**A.** A video conference with a laptop presentation works on the H.239 protocol, which is not supported in Cisco ASA software versions before 8.2. In order to ensure a data presentation works in a video conference, the Cisco ASA should support proper negotiation of H.239 between the video end points. This support is available from Cisco ASA software release 8.2 and later. An upgrade to a stable version in a software release, such as 8.2.4, will resolve this issue.

## **Q. Is it possible to configure 802.1x Authentication on the ASA 5505?**

**A.** No. It is not possible to configure 802.1x Authentication on the ASA 5505.

## **Q. Does Cisco ASA support multicast traffic to be sent on an IPsec VPN tunnel?**

**A.** No. It is not possible because this is not supported by Cisco ASA. As a workaround, you can have the multicast traffic encapsulated using GRE before that gets encrypted. Initially, the multicast packet has to be encapsulated using GRE on a Cisco router, then this GRE packet will be forwarded further to the Cisco ASA for IPsec encryption.

**Q. Cisco ASA is running in Active/Active mode. I want to configure the Cisco ASA as a VPN gateway. Is this possible?**

A. This is not possible because multiple contexts and VPN cannot run simultaneously. Cisco ASA can be configured for VPN when only in Active/Standby mode.

**Q. When using Cisco ASA as a VPN server, is it possible to send information about the client type (AnyConnect or IPsec) to a RADIUS database through accounting records?**

A. This is not possible because there is no such attribute to send the type of service that the client is using.

**Q. ASA Botnet Filter: How do you check for reports about dynamic blocks on the ASA?**

A. The reports about the dynamic blocks on the ASA can be checked with the **show dynamic-filter reports top** command. For more information, refer to Combating Botnets Using the Cisco ASA Botnet Traffic Filter.

**Q. Is Cisco Discovery Protocol (CDP) supported on PIX/ASA?**

A. Because PIX/ASA is a security device, it does not support CDP.

**Q. Can I manage ASA using Cisco Network Assistant (CNA)?**

A. Yes, the latest version of the CNA supports ASA. Refer to the Devices Supported list for more information.

**Q. Is it possible to configure ASA to act as Certification Authority (CA) and issue a certificate to VPN clients?**

A. Yes, with ASA 8.x and later you can configure the ASA to act as a local CA. Currently, ASA only allows authentication for the SSL VPN clients with the certificates issued by this CA. IPsec clients are not supported yet. Refer to The Local CA for more information.

**Note:** The Local CA feature is not supported if you use active/active failover or VPN load balancing. The Local CA cannot be subordinate to another CA; it can act only as the Root CA.

## **Failover**

**Q. Can a Security Appliance with a failover license be part of an active-active failover?**

A. Security Appliance failover units can be used in an active/active failover pair once they have a new failover active/active license upgrade installed (active/active requires one UR model and one "FO active/active" model). Refer to Feature Licenses and Specifications for more information on licensing.

## Q. Does the ASA support SSL VPN when configured for failover?

A. ASA supports SSL VPN only when configured for Active/Standby Failover and not in Active/Active Failover. For more information, refer to ASA Failover handling of SSL VPN application traffic and configurations.

## Error Messages

**Q. I am unable to configure failover when EZVPN is enabled on ASA 5505. Why does this error message appear: error :- ERROR]] vpnclient enable \* Disable failover CONFIG CONFLICT: Configuration that would prevent successful Cisco Easy VPN Remote operation has been detected, and is listed above. Please resolve the above configuration conflict(s) and re-enable?**

A. If ASA 5505 uses EasyVPN for remote users (Client mode), failover works, but if you have the ASA configured to use it with **Easy VPN Client** (Network-Extension Mode-NEM mode), then it does not work when Failover is configured. So Failover works only when ASA uses EZVPN for remote users (Client mode), and so this error occurs.

**Q. I receive this error message when I configure the third VLAN: :- ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured. How can I resolve this error?**

A. This error has occurred due to a license limitation on ASA. You must obtain the Security Plus license in order to configure more VLANs as in routed mode. Only three active VLANs can be configured with the Base license, and up to 20 active VLANs with the Security Plus license. You can create a third VLAN with the Base license, but this VLAN only has communication either to the outside or to the inside but not in both directions. If you need to have the communication in both directions, then you need to upgrade the license. Also, if you use the Base license, allow this interface to be the third VLAN and limit it from initiating contact to one other VLAN with the **hostname(config-if)# no forward interface vlan number** command. Thus the third VLAN can be configured.

**Q. How can I resolve this error message: %ASA-6-110002: Failed to locate egress interface for UDP from outside:x.x.x.x/xxxx to x.x.x.x/xxxx?**

A. ASA gives this error message when VPN Client tries to use peer-to-peer program and that traffic goes into the tunnel, where the peer-to-peer server does not reside. Configure the split tunnel in order to resolve this issue so that the traffic that needs to go out to the internet does not travel through the Tunnel and the packet is not dropped by the firewall. Refer to ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example for more information on Split Tunneling configuration in ASA.

**Q. How can I resolve this error message: Error : execUpgradeSoftware: operation timed out with 0 out of 1 bytes received?**

A. When you attempt to upgrade the AIP-SSM with the FTP, it can timeout. Increase the FTP Timeout value in order to resolve the issue.

**For Example:**

```
configure terminal
service host
network-settings
ftp-timeout 2700
exit
```

Save Changes.

**Q. How can I resolve this error message: %ASA-4-402123: CRYPTO: The ASA hardware accelerator encountered an error?**

A. In order to resolve this issue, try one of these workarounds:

- ◆ Disable the DTLS on ASA interfaces on which it is enabled.

In order to complete this solution, go to the Anyconnect profile on the ASDM, and remove the tick beside the interface working for the Anyconnect. For more information, refer to Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections.

- ◆ Reload the ASA.

This problem arises due to an error in the hardware accelerator of ASA. There are two bugs filed regarding this behavior. For more information, refer to CSCsd43563 (registered customers only) and CSCsc64621" (registered customers only) .

**Q. How can I resolve this error message: unable to send authentication message?**

A. The ASA does not support password management when you use LOCAL (internal) authentication. Remove the password management if configured in order to resolve this issue.

**Q. How can I resolve this error message that is received when testing the authentication on the ASA: ERROR: Authentication Server not responding: No error?**

```
ASA# test aaa-server authentication TAC_SRVR_GRP username test password test123 Server IP Address
```

A. Use any of these points to resolve this problem:

- ◆ Verify the connectivity from the ASA to the AAA server through ping test and ensure that the AAA server is reachable from the ASA.
- ◆ Verify the AAA related configuration on the ASA and check whether the AAA server is mentioned properly or not.

```
ASA# show run aaa-server
```

```
aaa-server RAD_SRVR_GRP protocol radius
aaa-server RAD_SRVR_GRP host ACS-SERVER
key *
aaa-server TAC_SRVR_GRP protocol tacacs+
aaa-server TAC_SRVR_GRP host ACS-SERVER
key *
```

- ◆ Verify if the Radius is TACACS ports are blocked by any firewall in the path between the AAA server and ASA. Ensure that corresponding ports are opened based on the protocol used.
- ◆ Verify the parameters on the AAA server.
- ◆ Reload the AAA server.

A successful test of the authentication looks like this:

```
ASA(config)# test aaa authentication topix host 10.24.10.10 username test password t
INFO: Attempting Authentication test to IP address <10.24.0.10> (timeout: 12 seconds
INFO: Authentication Successful
```

### **Q. How can I resolve this error message: %Error opening disk0:/.private/startup-config (Read-only file system) Error executing command [FAILED]?**

A. Format the **flash** or **FSCK** command in ASA/PIX in order to resolve this issue.

### **Q. How can I resolve this ASDM error message: Unconnected sockets not implemented?**

A. This issue occurs when ASDM version 5.0 or later runs on the ASA, PIX, or FWSM, and uses Java 6 Update 10 or later. While loading ASDM, this message appears:

```
ASDM cannot be loaded. Click OK to exit ASDM.
Unconnected sockets not implemented.
```

In order to resolve this issue, uninstall Java 6 Update 10, and install Java 6 Update 7. For more information, refer to **CSCsv12681 (registered customers only)** .

In order to get ASDM to load correctly with Java 6 Update 10, update ASDM to ASDM 6.1(5)51. For detailed information, refer to the **ASDM Client Operating System and Browser Requirements** section of the *Cisco ASDM Release Notes Version 6.1(5)*.

### **Q. How can I resolve this error message: %ASA-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0?**

A. This issue might be caused when ASDM is used to access the ASA or when there is high CPU utilization on the ASA. This message usually appears when the error recovery mechanism prevents system from crashing.

If there is no other issue with this message, it can be ignored. It is a recoverable error that does not impact performance.

## Q. Oracle traffic does not pass through the firewall. How can I resolve this issue?

A. This issue is caused by the sqlnet inspection feature of the firewall. When it occurs, the connections are torn out. The TCP proxy for sqlnet inspection engine was designed to handle multiple TNS frames in one TCP segment. The sqlnet inspection handles many TNS frames in one packet rendering the code complex.

In order to resolve this issue, the inspection engine should not handle multiple TNS frames in one packet. It is assumed that each TNS frame to be a different TCP packet and is inspected individually.

Software bugs have been filed for this behavior; for more information, refer to **CSCsr27940** (registered customers only) and **CSCsr14351** (registered customers only) .

The solution for this problem is given below.

Use the **no inspect sqlnet** command in class configuration mode in order to disable the inspection for sqlnet.

```
ASA(config)#class-map sqlnet-port
ASA(config-cmap)#match port tcp eq 1521
ASA(config-cmap)#exit
ASA(config)#policy-map sqlnet_policy
ASA(config-pmap)#class sqlnet-port
ASA(config-pmap-c)#no inspect sqlnet
ASA(config-pmap-c)#exit
ASA(config)#service-policy sqlnet_policy interface outside
```

For more information, refer to the **SQLNet inspection** section of the *Cisco Security Appliance Command Reference, Version 8.0*.

## Q. I am unable to copy the software image to the flash of the ASA, and I receive an error message similar to this message: Error writing disk0:/asa8XX-XX.bin (Cannot allocate memory)

A. This issue might occur if the firewall is unable to allocate memory (RAM) to load the software image.

ASA buffers the entire image in RAM while it is transferred to the ASA. Until it completes writing to flash, there must be an available free memory block large enough to hold the entire software image. One full memory block must be available to buffer the entire image before the ASA writes it to flash.

Memory usage is directly related to the features enabled on your ASA; these features are loaded each time your ASA is booted, regardless of how the image is loaded (via network or flash). You can disable features that you are not currently using in order to reduce memory usage. Note that WebVPN, SSLVPN, and threat detection tend to consume a lot of memory.

You can also use ROM monitor (ROMmon) to copy the image, or you can set your boot parameter to boot via tftp and then copy the image after the ASA has booted over the network. Since ROMmon does not load the configuration, it does not load these features; therefore, you should not experience the issue when you use this method to copy the file.

Try these workarounds.

- ◆ Disable threat detection on the firewall.

Enter these commands in order to disable threat detection:

```
conf t
!
no threat-detection basic-threat

no threat-detection statistics tcp-intercept
no threat-detection statistics

!
wr mem
```

- ◆ Disable the WebVPN-related processes.
- ◆ Use the ROMmon to copy the image.

For detailed information on how to use the ROM monitor to load a software image, refer to [Using the ROM Monitor to Load a Software Image](#).

**Q. How can I resolve this error message: [ERROR] threat-detection statistics host number-of-rate 0 threat-detection statistics host number-of-rate 0 ^ % Invalid input detected at '^' marker?**

A. This error can occur while you use the threat detection feature in ASDM. Either use CLI to send the command or downgrade the ASDM in order to resolve this issue.

**Q. How can I resolve this error message: %ERROR: copying 'disk0:/cisco\_config/97/customization/index.ini' to a temporary ramfs file failed?**

A. This issue is due to the Cisco bug ID CSCsy77628 (registered customers only). In order to resolve this issue the command **revert webvpn all** command in privileged EXEC mode to clear all WebVPN configurations. Reconfigure from scratch and then reload the ASA.

**Q. How can I resolve this error message on the ASA: ERROR: mount: Mounting /dev/hda1 on /mnt/disk0 failed: Invalid argument?**

A. Reformat the flash in order to resolve this issue. If this does not resolve the issue then contact TAC for further assistance.

**Q. I receive this error message on the ASA when I try to add non-English characters in a banner: The CLI generated has unsupported characters. ASA does not accept such characters. The following line(s) has unsupported characters. How can I resolve this error?**

A. This issue is due to Cisco bug ID CSCsz32125 (registered customers only). In order to resolve this issue, upgrade the ASA with software version 8.0(4.34).

**Q. How can I resolve this error message on the ASA: %ASA-1-216005: ERROR: Duplex-mismatch on Et0/0 resulted in transmitter lockup. A soft reset of the switch was performed?**

A. This error message is seen when a duplex-mismatch exists between the specified port and the device that is connected to it. Set both devices to either **auto** or **hard-coding the duplex** on both sides to be the same in order to correct the duplex-mismatch. This resolves the issue.

**Note:** Cisco bug ID CSCsm87892 has been filed regarding this problem, and the bug is moved to **Resolved** state now. For more information, refer to CSCsm87892 ( registered customers only) .

**Q. When I perform the recovery process on the AIP-SSM module and then the module repeatedly reboots, I receive this error message: Bad magic number (0x-682a2af). How can I resolve this error message?**

A. This issue happens when you use the wrong file for recovery or reimaging. If you use the **.pkg** file instead of the **.img**, then this action causes this error. This error also occurs when **.img** file is good, but ASA is stuck in boot loop. The only way to resolve this issue is to reimage the sensor.

**Q. Why does this error message appear when I download Global Correlations updates for AIP-SSM: collaborationApp[530] rep/E A global correlation update failed: Failed download of ibrs/1.1/config/default/1236210407 : HTTP connection failed collaborationApp[459] rep/E A global correlation update failed: Failed download of ibrs/1.1/drop/default/1296529950 : URI does not contain a valid ip address?**

A. This issue might occur due to URL filtering that is configured, which affects the traffic flow, and also due to the management interface of the AIP-SSM module that can go through the ASA to get out to the Internet. Make sure that the URL filtering configured does not block the devices (AIP-SSM) from reaching the Global Correlations, which resolves the issue. This issue occurs when there is corruption in a previous GC update. This can usually be corrected by turning off the GC service and then turning it back on. In IDM, choose **Configuration > Policies > Global Correlation > Inspection/Reputation**. Then, set Global Correlation Inspection (and **Reputation Filtering** if **On**) to **Off**. Apply the changes and wait for 10 minutes. Turn the features back on and monitor.

**Q. How can I resolve this error message on the ASA: Secure Connection Failed. An error occurred during a connection to x.x.x.x. Cannot communicate securely with peer: no common encryption algorithm(s). (Error code: ssl\_error\_no\_cypher\_overlap)?**

A. This issue is due to Cisco bug ID CSCtc37947 ( registered customers only) . In order to resolve this issue, remove the temporary files created for auto update from the root account on CSC, and then restart the services.

**Q. How can I resolve this error message on the ASA for Grayware: GraywarePattern : Pattern Update: The download file was unsuccessful for ActiveUpdate was unable to unzip the downloaded patch packages. The zip file may be corrupted. This can happen due to an unstable network connection. Please try downloading the file again.. The error code is 24?**

A. In order to resolve this issue, enter the 3DES activation key or use this command on the ASA: `ciscoasa(config)# ssl encryption aes256-sha1 aes128-sha1 3des-sha1 des-sha1 rc4-md5` . This command is used to specify the encryption algorithms that the SSL/TLS protocol uses.

**Q. How can I resolve this error message that I received while configuring the interfaces on ASA 5505: ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s)?**

A. This issue is due to the number of interfaces allowed to communicate based on the license present in the ASA. For models with a built-in switch, such as the ASA 5505, use the **forward interface** command in interface configuration mode in order to restore connectivity for one VLAN from initiating contact to another VLAN. In order to restrict one VLAN from initiating contact to another VLAN, use the **no** form of this command. You might need to restrict one VLAN depending on how many VLANs your license supports.

**Q. How can I resolve this error message on the ASA: %Error opening system:/running-config (No such device)?**

A. Reload the ASA in order to resolve this error message.

**Q. I received this error: [ERR-PAT-0003] The update system cannot find the required files in the decompressed set of update files, and cannot continue. This message is for diagnostic purpose only. Customers - please contact Technical Support. while upgrading to the latest pkg file on CSC-SSM. Why does this error occur?**

A. This issue is due to Cisco bug ID CSCta99320 ( registered customers only) . Refer to this bug for more information.

**Q. I receive this error message on the ASA, and the ASA does not reboot: mempool: error 12 creating global shared pool. Why does this issue occur, and how can it be resolved?**

A. This problem might occur when you try to install more RAM than is appropriate for a particular platform. For example, if you try to install 4 GB of RAM in an ASA5540, you might receive this error because the ASA5540 should not run more than 2 GB of RAM.

Keep these items in mind when you install the new RAM:

- ◆ Only the new RAM is installed in the ASA. The old RAM should be removed and NOT loaded in the extra RAM slots.
- ◆ The new RAM should be installed in alternating slot. For optimum performance, install the DIMMs in slots P13 and P15.

**Q. I receive this error: %ASA-4-402125: CRYPTO: The ASA hardware accelerator Ipsec ring timed out (Desc= 0xD6AF25E0, CtrlStat= 0xA000, ResultP= 0xD2D10A00, ResultVal= 186, Cmd= 0x10, CmdSize= 0, Param= 0x0, Dlen= 152, DataP= 0xD2D10974, CtxtP= 0xD46E6B10, SWReset= 21), when the ASA drops packet exhibiting severely degraded performance. Why does this issue occur?**

A. This issue is due to Cisco bug ID CSCti17266 ( registered customers only) . Refer to this bug for more information.

Another bug related to this behavior is CSCtn56501 ( registered customers only) .

**Q. This error message is received on the ASA: 418001: Through-the-device packet to/from management-only network is denied: icmp src In-DMZ:192.168.145.53 dst Mgt-Net:10.40.10.1 (type 8, code 0). How do I resolve this?**

A. Remove the **management-only** command from the interface where it is configured. In this specific case, from the above error message, remove the **management-only** command from the Mgt-Net interface.

**Q. How can I resolve this error message: %PIX|ASA-5-713137: Reaper overriding refCnt [ref\_count] and tunnelCnt [tunnel\_count] -- deleting SA!?**

A. This issue is due to Cisco bug ID CSCsq91271 ( registered customers only) . Refer to this bug for more information.

**Q. How can I resolve this error message: "CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files ( 2 ) allowed have been written to < disk0:/crypto\_archive >. Please archive & remove files from < disk0:/crypto\_archive > if you want more Crypto Archive Files saved"?**

A. This can be caused due to malfunctionalities of the crypto engine. This behavior has been logged in Cisco bug IDs CSCtg58074 ( registered customers only) and CSCsm77854 ( registered customers only) . A temporary workaround is to delete the crypto archive files from the flash and reload the device. This error does not seem to affect the existing traffic. If you need a permanent solution to this, contact Cisco TAC to receive an engineering build image.

## Related Information

- [Cisco PIX 500 Series Security Appliances](#)
  - [Cisco ASA 5500 Series Adaptive Security Appliances](#)
  - [AnyConnect VPN Client FAQ](#)
  - [Cisco Secure Desktop \(CSD\) FAQ](#)
  - [Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions](#)
  - [Cisco VPN Client FAQ](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 02, 2008

Document ID: 68330

---