

PIX/ASA: Security Appliance FAQ

Document ID: 68330

Questions

Introduction

Which devices support PIX 7.x?

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?

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?

What are the two modes of operations in Security Appliance?

What does Security Context in Security Appliance mean?

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

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

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

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

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?

I am unable to ping outside of the outside interface while using Security Appliance 7.0.

How do I fix this?

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

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

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

Does ASA support ISP load balancing?

Does PIX/ASA support EtherChannel/PortChannel interfaces?

Is ASA/PIX is able to block Skype?

Does ASA support SNMPv3?

Is there a way to log entries with a name instead of an IP address?

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

Can a Security Appliance with a failover license be part of an active–active failover?

Does Security Appliance 7.0 support the Are You There (AYT) feature?

How do I configure the VPN user group–lock feature on the ASA or PIX?

Is FTP with TLS/SSL supported through the Security Appliance?

Does the Security Appliance support DDNS?

Does the PIX support WebVPN/SSL VPN?

Does the PIX support Cisco AnyConnect VPN Client?

Does the PIX support any services modules like AIP–SSM and CSC–SSM?

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

Does the ASA support password management with NT?

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.

Can I use ASA 5510 as an Easy VPN Client?

Does ASA supports Asymmetric routing ?

Does ASA support PPTP client?

Does ASA support QOS marking the packet with DSCP value?

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

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

I am unable to configure Failover when EZVPN is enabled on ASA 5505. Why does the 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 error message appear?

I get the :- 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. error message when I configure the third VLAN. How can this error be resolved?

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

How can I resolve the "Error: execUpgradeSoftware: operation timed out with 0 out of 1 bytes received" error message?

How can I resolve the unable to send authentication message error message?

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

How can I resolve the issue with the "Unconnected sockets not implemented" ASDM error message?

Does ASA support source-based routing?

Does H329 traffic pass through PIX/ASA 8.1 and later?

How can I resolve the ERROR] threat-detection statistics host number-of-rate 0 threat-detection statistics host number-of-rate 0 ^ % Invalid input detected at '^' marker error message?

How can I capture packets in PIX/ASA?

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

How can I resolve the %ERROR: copying 'disk0:/cisco_config/97/customization/index.ini' to a temporary ramfs file failed error message?

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

Does ASA allow Broadcast traffic to pass through its interface?

How can I redirect HTTP traffic to HTTPS on ASA?

Related Information

Introduction

The document addresses the most frequently asked questions (FAQs) related to Cisco Security Appliances like PIX 500 Series and ASA 5500 Series..

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.

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.

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.

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: 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. 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 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® 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 interface management 0/0 on the ASA in order to pass traffic like any other interface?

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

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.

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.

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.

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. Does PIX/ASA support EtherChannel/PortChannel interfaces?

A. No.

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 capacity 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 IPS (Intrusion Prevention System). 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. 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 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. 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. 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 in order to control how routes are redistributed between routing protocols like OSPF with the use of metrics and to not to redistribute regular traffic.

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 prior to 8.2(1).

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. I am unable to configure Failover when EZVPN is enabled on ASA 5505. Why does the 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 error message appear?

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 get the :- 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. error message when I configure the third VLAN. How can this error be resolved?

A. This error has occurred due to a license limitation on ASA. You need to 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 the %ASA-6-110002: Failed to locate egress interface for UDP from outside:x.x.x.x/xxxx to x.x.x.x/xxxx error message?

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 the "Error: execUpgradeSoftware: operation timed out with 0 out of 1 bytes received" error message?

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 the unable to send authentication message error 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 the %Error opening disk0:/.private/startup-config (Read-only file system) Error executing command [FAILED] error message?

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

Q. How can I resolve the issue with the "Unconnected sockets not implemented" ASDM error message?

A. ASDM is not compatible with Java 6 update 10/11, so downgrade to Java 6 Update 7 with which ASDM works fine.

Q. Does ASA support source-based routing?

A. No.

Q. Does H329 traffic pass through PIX/ASA 8.1 and later?

A. No.

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

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 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. 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. How can I resolve the %ERROR: copying 'disk0:/cisco_config/97/customization/index.ini' to a temporary ramfs file failed error message?

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 the ERROR: mount: Mounting /dev/hda1 on /mnt/disk0 failed: Invalid argument error message on ASA?

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

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

A. No.

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]
```

Related Information

- [Cisco PIX Firewall Software](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 02, 2008

Document ID: 68330
