PIX/ASA 7.x and later: Connecting Multiple Internal Networks with Internet Configuration Example

Contents

Introduction **Prerequisites** Requirements **Components Used Related Products Conventions** Configure Background Information Network Diagram Configurations PIX Configuration using ASDM PIX Configuration using CLI Verify Troubleshoot **Troubleshooting Commands** Troubleshooting Procedure Unable to Access Websites by Name **Related Information**

Introduction

This document provides a sample configuration for PIX/ASA Security Appliance version 7.x and later with multiple internal networks that connect to the Internet (or an external network) using the command line interface (CLI) or Adaptive Security Device Manager (ASDM) 5.x and later.

Refer to <u>Establish and Troubleshoot Connectivity through the Cisco Security Appliance</u> for information on how to establish and troubleshoot connectivity through PIX/ASA.

Refer to <u>Using nat, global, static, conduit, and access-list Commands and Port</u> <u>Redirection(Forwarding) on PIX</u> for information about common PIX commands.

Note: Some options in other ASDM versions can appear different from the options in ASDM 5.1. Refer to the <u>ASDM documentation</u> for more information.

Prerequisites

Requirements

When you add more than one internal network behind a PIX Firewall, keep these points in mind:

• The PIX does not support secondary addressing.

- A router has to be used behind the PIX in order to achieve routing between the existing network and the newly added network.
- The default gateway of all the hosts needs to point to the inside router.
- Add a default route on the inside router that points to the PIX.
- Clear the Address Resolution Protocol (ARP) cache on the inside router.

Refer to <u>Allowing HTTPS Access for ASDM</u> in order to allow the device to be configured by the ASDM.

Components Used

The information in this document is based on these software and hardware versions:

- PIX Security Appliance 515E with software version 7.1
- ASDM 5.1
- Cisco routers with Cisco IOS® Software Release 12.3(7)T

Note: This document has been recertified with PIX/ASA software version 8.x and Cisco IOS Software Release 12.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco ASA Security Appliance version 7.x and later.

Conventions

Refer to the <u>Cisco Technical Tips Conventions</u> for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the <u>Command Lookup Tool</u> (<u>registered</u> customers only) to obtain more information on the commands used in this section.

The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Background Information

In this scenario, there are three internal networks (10.1.1.0/24, 10.2.1.0/24 and 10.3.1.0/24) to be connected to the Internet (or an External network) through PIX. The internal networks are connected to the inside interface of PIX. The Internet connectivity is through a router which is connected to the outside interface of the PIX. The PIX has the IP address 172.16.1.1/24.

The static routes are used to route the packets from the internal networks to the Internet and vice

versa. Instead of using the static routes, you can also use a dynamic routing protocol such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).

The internal hosts communicate with the Internet by translating the internal networks on PIX using dynamic NAT (pool of IP addresses - 172.16.1.5 to 172.16.1.10). If the pool of IP addresses is exhausted, the PIX will PAT (using IP address 172.16.1.4) the internal hosts to reach the Internet.

Refer to <u>PIX/ASA 7.x NAT and PAT Statements</u> for more information on NAT/PAT.

Note: If the static NAT uses the outside IP (global_IP) address to translate, then this might cause a translation. Therefore, use the keyword interface instead of the IP address in the static translation.

Network Diagram

This document uses this network setup:



The default gateway of the hosts on the 10.1.1.0 network points to RouterA. A default route on RouterB is added that points to RouterA. RouterA has a default route that points to the PIX inside interface.

Configurations

This document uses these configurations:

- RouterA Configuration
- <u>RouterB Configuration</u>
- <u>PIX Security Appliance 7.1 ConfigurationPIX Configuration using ASDMPIX Security</u> <u>Appliance CLI Configuration</u>





If you want to use the ASDM for the configuration of the PIX Security Appliance, but have not bootstrapped the device, complete these steps:

- 1. Console into the PIX.
- 2. From a cleared configuration, use the interactive prompts in order to enable ASDM for the management of the PIX from workstation 10.1.1.5.

```
PIX Security Appliance 7.1 Configuration
Pre-configure Firewall now through interactive prompts [yes]?
yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
 Year [2005]:
 Month [Mar]:
 Day [15]:
 Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5
The following configuration will be used:
        Enable password: cisco
        Allow password recovery: yes
        Clock (UTC): 14:45:00 Mar 15 2005
        Firewall Mode: Routed
        Inside IP address: 10.1.1.1
        Inside network mask: 255.255.255.0
         Host name: OZ-PIX
         Domain name: cisco.com
         IP address of host running Device Manager: 10.1.1.5
Use this configuration and write to flash? yes
        INFO: Security level for "inside" set to 100 by
default.
        Cryptochecksum: a0bff9bb aa3d815f c9fd269a 3f67fef5
965 bytes copied in 0.880 secs
        INFO: converting 'fixup protocol dns maximum-length
512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF
```

commands INFO: converting 'fixup protocol h323_h225 1720' to MPF commands INFO: converting 'fixup protocol h323_ras 1718-1719' to MPF commands INFO: converting 'fixup protocol netbios 137-138' to MPF commands INFO: converting 'fixup protocol rsh 514' to MPF commands INFO: converting 'fixup protocol rtsp 554' to MPF commands INFO: converting 'fixup protocol sip 5060' to MPF commands INFO: converting 'fixup protocol skinny 2000' to MPF commands INFO: converting 'fixup protocol smtp 25' to MPF commands INFO: converting 'fixup protocol sqlnet 1521' to MPF commands INFO: converting 'fixup protocol sunrpc_udp 111' to MPF commands INFO: converting 'fixup protocol tftp 69' to MPF commands INFO: converting 'fixup protocol sip udp 5060' to MPF commands INFO: converting 'fixup protocol xdmcp 177' to MPF commands Type help or '?' for a list of available commands. OZ-PIX>

PIX Configuration using ASDM

Complete these steps in order to configure via the ASDM GUI:

- 1. From workstation 10.1.1.5, open a web browser to use ADSM (in this example, https://10.1.1.1).
- 2. Click yes on the certificate prompts.
- 3. Log in with the enable password, as previously configured.
- 4. If this is the first time ASDM is run on the PC, you are prompted to use ASDM Launcher or ASDM as a Java App. In this example, the ASDM Launcher is selected and installed.
- 5. Go to the ASDM Home window and click **Configuration**.

		Interrace Status	
General License		Interface IP Address/Mask Line Link	Current Kb
Host Name: pixfirew	all.default.domain.invalid	inside 10.1.1.1/24 O up O up	1
PIX Version: 7.1(1)	Device Uptime: 14d 6h 4m 4s		
ASDM Version: 5.1(1)	Device Type: PIX 515E		
Firewall Mode: Routed	Context Mode: Single		
Total Flash: 16 MB	Total Memory: 64 MB	Select an interface to view input and output Kbps	
VPN Status IKE Tunnels: 0	IPSec Tunnels: 0	Connections Per Second Usage	
System Resources Statu	s	-1	
CPU CPU Usage	percent)	0.0	
96		201	je sa sj er
1% 32		UDP: 0 Total: 0	
17:58:50 17:58:10		'inside' Interface Traffic Usage (Kbps)	
Memory Memory Usa	ge (MB)		
a distantia di sul di		0.5	
0.44		10 1 10 10 10 10 10 10 10 10 10 10 10 10 10	
36M0 32			
38M0 17.58.50 17.58.50		Input Kbps: 0 Output Kbps: 1	DM Codes File

6. Choose **Interface > Edit** in order to configure the outside interface.

Cisco ASDM	5.1 for PIX - 10.1.1.1				2 B. 200	
File Rules S	Bearch Options Tools Wizard	is Help				
S Home	Configuration Monitoring	Back Forward	Q Q Search Retresh	Save Help		CISCO SYSTEMS
	Configuration > Interfaces					
Interfaces	⊕ <u>≞</u> ≆ ≌ ĝ ŝ	e il <u>6</u> ii 4				
Security Policy	Interface	Name Enabl	ed Security IP Addr	ess Subnet Mask	Management MTU Only	Add
2 de	EthernetD	No			No	Edit
NAT	Ethemet1	inside Yes	10010.1.1.1	255.255.255.0	No 1500	Delete
9						
VPN						
Routing						
Global Objects						
Properties						
	🗖 Enable traffic between t	wo or more interfaces	s which are configured w	ith same security levels	1	
		Ĺ	Apply	Reset		
-	,		<admin></admin>	NA (15)	a 7/11/08	5:59:49 PM UTC

7. Enter the interface details and click **OK** when you are done.

lardware Port:	Ethernet0	Configure Hardware Propertie
Z Enable Interface	Dedicate this interface	to management only
iterface Name:	outside	
ecurity Level:	0	
IP Address	- 275	
Ose Static IP	C Obtain Address via DH	CP
IP Address:	172.16.1.1	
Subnet Mask:	255.255.255.0	-
ITU:	1500	
escription:		
		Holp

box.

8.



9. Click Apply to accept the interface configuration. The configuration also gets pushed onto the

PIX.

Cisco ASDM 5	1 for PIX - 10.1.1.1 arch Options Tools Wizards	Help							<u>_ 0 ×</u>
Home (Configuration Monitoring	Back For	onward s	Q	Refresh :	Save Help			CISCO SYSTEMS
Interfaces	Configuration > Interfaces ♥: ① ▼ ■ ▼ ■ ■ 1 ⑧ = ※ P	- 6 6 6	9						
Security Policy	Interface	Name	Enabled S	ecurity evel	IP Address	Subnet Mask	Management Only	MTU	Add
340	Ethernet0	outside	Yes	017	2.16.1.1	255.255.255.0	No	1500	Edit
NAT	Ethernet1	inside	Yes	10010	1.1.1	255.255.255.0	No:	1500	Delete
A Counting Routing Global Objects Properties									
	Enable traffic between tw	ro ar more inte	rfaces whic	h are conf	igured with sa	me security levels		•	
ļ,),		-	Kar	imin> NA		A CONTRACTOR	7/11/06	8-01-09 PM LTC

10. Choose **Security Policy** on the Features tab in order to review the security policy rule used. In this example, the default inside rule is used.

Cisco ASDM 5.1	for PIX - 10.1.1.1			
Home C	onfiguration Montoring Es	ck Forward Search Refresh	Save Help	Cisco Systems
Home C	enfiguration Monitoring Es Configuration > Security Policy > Ac Access Rules C AAA Rule Show Rules for Interface: All Intu Rule Action H C Access Rules C AAA Rule Show Rules for Interface: All Intu C ACCESS Rule Action H C ACTION H	ick Forward Search Refresh icess Rules Rules Row All is Filter Rules Service Policy is is Show All isource IostiNetwork Destination Host/Network any	Save Help Rules Rule Applied To Traffic Interface (outbound)	Service Add Edit Delete
	🖌 Allow traffic 🛛 🥹 Der	Ny traffic Apply Reset	Show Summary Advanced	C Show Detail
		<admin></admin>	NA (15)	🔒 7/11/06 6:01:49 PM UTC

11. In this example, NAT is used. Uncheck the **Enable traffic through the firewall without** address translation check box and click **Add** in order to configure the NAT rule.

Eisco ASDM 5.1 f	or PIX - 10.1 h Options	.1.1 Tools Wizar	ds Help					×
Home Con	anguration	Monitoring	Back Forward	Q Search	Refresh	Save He	q	CISCO SYSTEMS
Interfaces Security Policy	ontiguration • 👷 🐨 Filenable • Transla	× NAT > Transl ■	ation Rules Point Robert Robe	ress franslatio cemption Rules	0	_		
NAT	Show Rul	les for Interface	All Interfaces		Show All	1	Translated	Add
SFN VPN	Туре	Interface	Source Network	Destina	tion Network	Interface	Address	Edit
Routing Global Objects Properties	• • • Static	NAT 📲	Dynamic NAT 🖓	Static Policy N Appl	ат 👘	Dynamic Policy Reset	NAT <u>Manage Pools</u>	

12. Configure the Source Network. In this example, 10.0.0.0 is used for the IP address, and 255.0.0.0 is used for the mask.Click **Manage Pools** in order to define the NAT pool addresses.

OBC HAN	CU	Ise Policy NAT				
Source Host/	Network-					
		Interface: IP Address:	inside 10.0.0.0		-	
		maon.	[266.0.0.0] Browse	: 		
						NAT Options
anslate Addre	ess on Inte	rface: outs	ide 🗾			
inslate Addre	ess on Inte dress To	rface: outs	ide 🗾			
ranslate Addre	ess on Inte dress To –	rface: Jouts				
ranslate Addre Translate Ad ۲ ان ۲ ۲	ess on Inte dress To — tatic "Redirect r	IP Address;		*		
Inslate Addre Franslate Ad C 1 8	ess on Inte dress To – itatic Redirect p © TCP © UDP	IP Address; Fort Original port	ide Tr	• anslated pr	ort:	
Inslate Addre Franslate Ad I S I S I S I S I S I S I S I S I S I S	ess on Inte dress To – itatic Redirect p O TOP O UDP	IP Address; oort Original port Address Pool:	Ide	anslated pr	ort: T Manage P	
Inslate Addre Franslate Ad I I I I I I I I I I I I I I I I I I I	ess on Inte dress To – itatic Redirect p C UDP Dynamic Pool ID	rface: outs IP Address; Fort Original port Address Pool:	Ide	anslated pr	ort: T Manage P	ools
rranslate Addre Corio S	ess on Inte dress To – itatic Redirect p C UDP Dynamic Pool ID N/A	rface: outs IP Address; Fort Original port Address Pool: No address po	Ide	anslated pr	ort: Manage P	001s
rranslate Addre Criti S	ess on Inte dress To – itatic Redirect p © TCP © UDP bynamic Pool ID N/A	rface: outs IP Address; Fort Original port Address Pool: No address po	Ide	anslated pr s	nt: Manage P	00IS

13. Select the outside interface and click Add.

side	Pool ID	IP Address(es)	Add
itside			Edit
			Delete

14. In this example, a Range and PAT address pool are configured. Configure the range NAT pool address and click **OK**.

C Denve					
● Range C Dout Adv	dua a a Tuan alatian (
PortAdo	oress Translation ((PAT)			
Port Add	ress Translation ((PAT) using t	he IP addres	s of the interf	ace
IP Ad	dress: 172161	5		72.16110	
1.00	172.10.1	.9		72.10.1.10	
		3			
Netwi	ork Mask (optional)	: 255.2	255.255.0		

15. Select the outside interface in step 13 in order to configure the PAT address. Click **OK**

		Pool ID:	1	
C Range				
Port Address	Translation (PAT)			
C Port Address	Translation (PAT) us	sing the IP addres	s of the interface	
IP Address	1721614	r		
in Address.	1172.10.1.4			
	isk (optional):	255 255 255 0		
Network Ma				
Network Ma				

Click OK in order to

Interface	Pool ID	IP Address(es)	
nside	1 1721	614	Add
			Delete

 On the Edit Address Translation Rule window, select the Pool ID to be used by the source network configured. Click OK.

• USE NAT	O U	se Policy NAT					
Source Host/N	letwork						
		Interface: IP Address: Mask:	inside 10.0.0.0 255.0.0.0		¥		
anslate Addre	ss on Inte	rface: outsi	ide •	1			NAT Options
Translate Add	ress To –			-			
Translate Add C 1 Sta	ress To — atic Redirect p	IP Address: ort	_	-, 	2		
Translate Add Translate Add	ress To – atic Redirect p © TCP © UDP	IP Address: ort Original port		Translated	port.		
Translate Add Translate Add Sta Translate Add Sta Sta Sta Sta Sta Sta Sta Sta	ress To — atic Redirect p © TCP © UDP namic	IP Address: ort Original port Address Pool:	1	Translated	port Manag	e Pools	
Translate Add Translate Add Sta Translate Add	ress To — atic Redirect p TCP C UDP namic Pool ID	IP Address: ort Original port Address Pool:		Translated	port.	e Pools	
Translate Add	ress To — atic Redirect p © UDP namic Pool ID 1	IP Address: ort Original port Address Pool: 172.16.1.4 172.16.1.5-177		Translated	port Manag	e Pools	

17. Click **Apply** in order to push the configured NAT rule to the PIX.



18. In this example, static routes are used. Click **Routing**, choose **Static Route** and click **Add**.

Cisco ASDM 5.1 for Pl	12 - 10.1.1.1							
File Rules Search (Options Tools Wizards	Help						
Home Configu	ination Monitoring	Back Forw	ard Seard	Retres	h Save	? Help		CISCO SYSTEMS
Interfaces Interfaces Security Policy Image: Security Policy I	guration > Routing > Pouter	Ig > Static Rout Re Route Specify static Interface	e Coutes. IP Address	Netmask	Gateway IP	Metric	Tunneled	Add Edit Defete
				<admin></admin>	NA (15)		7/1	1/06 7:45:00 PM UTC

19. Configure the default gateway and click

Add Static Route	
Interface Name:	outside 💌
IP Address:	0.0.0.0
Mask:	0.0.0.0
Gateway IP:	172.16.1.2
Metric	1
C Tunneled (Used	only for default route)
ок	Cancel Help

20. Click Add and add the routes to the inside

F	Add Static R	oute			×
	Interface	Name:	inside	-	
	IP Addre	ss:	10.2.1.0		
	Mask:		255.255.255.	0 💌	
	Gateway	IP:	10.1.1.2		
	 Metric 		1		
	C Tunnel	ed (Used	only for default r	oute)	
networks.	ОK		Cancel	Help	
🔂 Add Stat	ic Route	- 12		×	
Interf	ace Name:	inside			
IP Ad	dress:	10.3.1	.0		
Mask	c	255.25	5.255.0		
Gate	way IP:	10.1.1	.2		
	tric	1			
C Tur	nneled (Used	only for de	efault route)		
ОК		Cancel	Hel	p	

21. Confirm that the correct routes are configured and click **Apply**.

Eisco ASDM File Rules S	5.1 for PIX - 10.1.1.1 earch Options Tools Wizard	ts Help						_ 🗆 X
San Home	Configuration Monitoring	Back Form	and Sear	ch Refresh	Save	? Help		CISCO SYSTEMS
Interfaces Security Policy NAT Security Policy NAT Security VPN Security Routing Global Objects Properties	Contiguration > Routing > Ro	Uting > Static Rou Static Route Specify static Interface outside Inside Inside Inside	te Coutes. IP Address 0.0.0. 10.2.1.0 10.3.1.0	Netmask 0.0.0.0 265.255.255.0 255.255.255.0	Gateway IP 172.16.1.2 10.1.1.2	Metric 1 1	Tunneler No N/A N/A	Add Edit Delete
5	·			<admin></admin>	NA (15)	i 🖓 🔂	1/11	/06 7:48:40 PM UTC

PIX Configuration using CLI

Configuration via the ASDM GUI is now complete.

You can see this configuration via the CLI:

PIX Security Appliance CLI

<pre>pixfirewall(config)#write terminal PIX Version 7.0(0)102</pre>
names ! interface Ethernet0 nameif outside security-level 0
ip address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! Assign name and IP address to the
interfaces enable password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image flash:/asdmfile.50073
no asdm history enable arp timeout 14400 nat-control !
Enforce a strict NAT for all the traffic through the Security
appliance global (outside) 1 172.16.1.5-172.16.1.10 netmask
255.255.255.0 ! Define a pool of global addresses
172.16.1.5 to 172.16.1.10 with ! NAT ID 1 to be used for
NAT global (outside) 1 172.16.1.4 netmask 255.255.255.0 !
Define a single IP address 172.16.1.4 with NAT ID 1 to be
used for PAT nat (inside) 1 10.0.0.0 255.0.0.0 ! Define
the inside networks with same NAT ID 1 used in the global
command for NAT route inside 10.3.1.0 255.255.255.0 10.1.1.3
1 route inside 10.2.1.0 255.255.255.0 10.1.1.2 1 !
Configure static routes for routing the packets towards the
internal network route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
<pre>! Configure static route for routing the packets towards</pre>
the Internet (or External network) timeout xlate 3:00:00

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute http server enable !--- Enable the HTTP
server on PIX for ASDM access http 10.1.1.5 255.255.255
inside !--- Enable HTTP access from host 10.1.1.5 to
configure PIX using ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

Choose **File > Show Running Configuration in New Window** in order to view the CLI configuration in ASDM.

File Rules Search Options Tools Wizards Help						
Refresh ASDM with the Running Configuration on the Device Reset Device to the Factory Default Configuration						
Show Running Configuration in New Window						
Save Running Configuration to Flash Save Running Configuration to TFTP Server Save Running Configuration to Standby Unit Save Internal Log Buffer to Flash						
Print						
Clear ASDM Cache Clear Internal Log Buffer						
Exit						

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Troubleshooting Commands

The <u>Output Interpreter Tool</u> (<u>registered</u> customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use debug commands.

- **debug icmp trace**—Shows whether ICMP requests from the hosts reach the PIX. In order to run this debug, you need to add the **access-list** command to permit ICMP in your configuration.
- logging buffer debugging—Shows connections that are established and denied to hosts that

go through the PIX. The information is stored in the PIX log buffer and you can see the output with the **show log** command.

Troubleshooting Procedure

ASDM can be used to enable logging, and also to view the logs:

1. Choose Configuration > Properties > Logging > Logging Setup, check Enable Logging, and click

Apply.						
Cisco ASDM 5.1 for PIX - File Rules Bearch Opti	10.1.1.1 ions Tools Wizards	Help				
Home Configurati	ion Montorry	Back Forward	Q Refres	h Save	? Help	Cisco Systems
Image: Security Policy Image: Security Policy Security Policy Image: Security Policy NAT Image: Security Policy VPN Image: Security Policy Routing Image: Security Policy Image: Security Policy Image: Security Policy I	ation × Froperties × Log artup Wizard VA Setup 10- Spoofing RP 10- Update ertificate evice Access evice Administrati HCP Services NS Client ailover ragment istory Metrics Audit bgging - ogging Setup E-Mail Setup E-Mail Setup Event Lists - Logging Filters Rate Limit - Syslog Servers - Syslog Setup riority Queue SL UNRPC Server CP Options	ping > Logging Setup ■ ● ● ● ● ● Logging Setup ■ Enable loggin ■ Send debug n ■ Logging to Intern Specify the size of be overwritten. Buffer Size: 41 You can choose to Save Buffer To: ASDM Logging Specify the size of Queue Size: 1	gi nessages as syslog al Buffer f the internal buffer f D96 bytes o save the buffer co IF FIP Server IF Flash (the queue for syslog) 00 Ap	ps o which syslog ntents before t Configure F Configure F gs Intended fo	Enable logging of Send syslogs in gs will be saved. V the buffer is overw FTP Settings Tash Usage ar viewing in ASDIV Reset	on the failover standby unit EMBLEM format Yhen the buffer fills up, it will ritten.

 Choose Monitoring > Logging > Log Buffer > Logging Level and choose Logging Buffer from the drop-down list. Click View.



3. Here is an example of the Log Buffer:

Log Buf	fer	- 🖸 Color Settinge 🏠 Create Pule 🖼 Shrw Pule Lind:
- Reine		
This table	shows syslog messages	s in ASDM logging buffer as of now.
Severity	Time	Message ID: Description
<u>î</u> 6	Jul 12 2006 13:08:11	605005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user "enable_15"
<u>1</u> 6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
<u>i</u> 6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
<u>1</u> 6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
<u>i</u> 6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1138) to NP Identity Ifc:10.
<u>1</u> 6	Jul 12 2006 13:08:10	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>1</u> 6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
<u>i</u> 6	Jul 12 2006 13:08:09	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:08	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<mark>1</mark> 6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:07	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>1</u> 6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:06	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<mark>€</mark> 6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>t</u> 6	Jul 12 2006 13:08:05	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<mark>1</mark> 6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>t</u> 6	Jul 12 2006 13:08:04	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>1</u> 6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>t</u> 6	Jul 12 2006 13:08:03	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>t</u> 6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:02	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>1</u> 6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<u>i</u> 6	Jul 12 2006 13:08:01	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
<mark>1</mark> 6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
0 Er	nemencies 0 Alerte	Critical & Errore & Warninge & Notificatione & Informational & Dahugaing

Unable to Access Websites by Name

In certain scenarios, the internal networks cannot access the internet websites by using name (works with IP address) in the web browser. This issue is common and usually occurs if the DNS server is not defined, especially in cases where PIX/ASA is the DHCP server. Also, this can occur in cases if the PIX/ASA is unable to push the DNS server or if the DNS server is not reachable.

Related Information

- <u>Cisco PIX 500 Series Security Appliances</u>
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco Secure PIX Firewall Command References</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco Adaptive Security Device Manager (ASDM) Troubleshoot and Alerts</u>
- Requests for Comments (RFCs)
- <u>Technical Support & Documentation Cisco Systems</u>