PIX/ASA 7.x e versioni successive: Esempio di connessione di più reti interne con la configurazione di Internet

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione Premesse Esempio di rete Configurazioni Configurazione PIX con ASDM Configurazione PIX con CLI Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi Procedura di risoluzione dei problemi Impossibile accedere ai siti Web per nome Informazioni correlate

Introduzione

In questo documento viene fornita una configurazione di esempio per PIX/ASA Security Appliance versione 7.x e successive con più reti interne che si connettono a Internet (o a una rete esterna) tramite l'interfaccia della riga di comando (CLI) o Adaptive Security Device Manager (ASDM) versione 5.x e successive.

Per informazioni su come stabilire e risolvere i problemi di connettività tramite PIX/ASA, consultare il documento sulla <u>definizione e risoluzione dei problemi di connettività tramite Cisco Security</u> <u>Appliance</u>.

Per informazioni sui comandi PIX comuni, fare riferimento a <u>Uso dei comandi nat, global, static,</u> <u>conduit e access-list e a Reindirizzamento porte (inoltro) su PIX</u>.

Nota: alcune opzioni di altre versioni di ASDM possono essere diverse da quelle di ASDM 5.1. Per ulteriori informazioni, consultare la <u>documentazione di ASDM</u>.

Prerequisiti

Requisiti

Quando si aggiungono più reti interne dietro un firewall PIX, tenere presente quanto segue:

- Il PIX non supporta l'indirizzamento secondario.
- Ènecessario usare un router dietro il PIX per ottenere il routing tra la rete esistente e la rete appena aggiunta.
- Il gateway predefinito di tutti gli host deve puntare al router interno.
- Aggiungere un percorso predefinito sul router interno che punti al PIX.
- Cancellare la cache ARP (Address Resolution Protocol) sul router interno.

Per consentire la configurazione del dispositivo da parte di ASDM, consultare il documento sulla concessione dell'accesso HTTPS per ASDM.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PIX Security Appliance 515E con versione software 7.1
- ASDM 5.1
- Router Cisco con software Cisco IOS® versione 12.3(7)T

Nota: questo documento è stato ricertificato con il software PIX/ASA versione 8.x e con il software Cisco IOS versione 12.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA Security Appliance versione 7.x e successive.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Premesse

In questo scenario, sono disponibili tre reti interne (10.1.1.0/24, 10.2.1.0/24 e 10.3.1.0/24) da connettere a Internet (o a una rete esterna) tramite PIX. Le reti interne sono collegate all'interfaccia interna di PIX. La connettività Internet avviene tramite un router collegato all'interfaccia esterna del PIX. Il PIX ha l'indirizzo IP 172.16.1.1/24.

Le route statiche vengono utilizzate per indirizzare i pacchetti dalle reti interne a Internet e viceversa. Anziché utilizzare le route statiche, è inoltre possibile utilizzare un protocollo di routing dinamico, ad esempio RIP (Routing Information Protocol) o OSPF (Open Shortest Path First).

Gli host interni comunicano con Internet convertendo le reti interne in PIX utilizzando NAT dinamico (pool di indirizzi IP - da 172.16.1.5 a 172.16.1.10). Se il pool di indirizzi IP è esaurito, il PIX invierà (utilizzando l'indirizzo IP 172.16.1.4) gli host interni per raggiungere Internet.

Per ulteriori informazioni su NAT/PAT, fare riferimento alle istruzioni PIX/ASA 7.x NAT e PAT.

Nota: se il NAT statico utilizza l'indirizzo IP esterno (global_IP) per la conversione, potrebbe verificarsi una conversione. Pertanto, nella traduzione statica utilizzare la parola chiave interface anziché l'indirizzo IP.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Il gateway predefinito degli host sulla rete 10.1.1.0 punta al router A. Viene aggiunto un percorso predefinito sul router B che punta al router A. Il router A ha una route predefinita che punta al PIX all'interno dell'interfaccia.

Configurazioni

Nel documento vengono usate queste configurazioni:

- <u>Configurazione routerA</u>
- <u>Configurazione routerB</u>
- <u>Configurazione di PIX Security Appliance 7.1Configurazione PIX con ASDMConfigurazione</u>
 <u>CLI di PIX Security Appliance</u>

Configurazione routerA
RouterA# show running-config
Building configuration
Current configuration : 1151 bytes
!
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname RouterA
!
interface Ethernet2/0
ip address 10.2.1.1 255.255.255.0
half-duplex
!
interface Ethernet2/1
ip address 10.1.1.2 255.255.255.0
half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route 10.3.1.0 255.255.255.0 10.1.1.3 !
!
line con O
line aux O
line vty 0 4
!
end Deuteral#
RouterB# show running-config
Current configuration : 1132 bytes
I
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
interface FastEthernet0/0

```
ip address 10.1.1.3 255.255.255.0
 speed auto
!
interface Ethernet1/0
ip address 10.3.1.1 255.255.255.0
half-duplex
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
control-plane
!
1
line con 0
line aux 0
line vty 0 4
!
end
RouterB#
```

Se si desidera utilizzare ASDM per la configurazione dell'appliance di sicurezza PIX, ma il dispositivo non è stato avviato, attenersi alla seguente procedura:

1. Collegare la console al PIX.

Configurazione di PIX Security Appliance 7.1

2. Da una configurazione cancellata, usare i prompt interattivi per abilitare ASDM per la gestione del PIX dalla workstation 10.1.1.5.

```
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 maximumlength 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>

Configurazione PIX con ASDM

Per eseguire la configurazione tramite l'interfaccia utente grafica ASDM, completare i seguenti passaggi:

- 1. Dalla workstation 10.1.1.5, aprire un browser Web per utilizzare ADSM (in questo esempio, https://10.1.1.1).
- 2. Fare clic su sì nelle richieste di certificato.
- 3. Accedere con la password enable, come configurato in precedenza.
- 4. Se è la prima volta che ASDM viene eseguito sul PC, viene richiesto di utilizzare ASDM Launcher o ASDM come app Java. Nell'esempio, l'utilità di avvio ASDM è selezionata e installata.
- 5. Andare alla finestra Home ASDM e fare clic su **Configuration** (Configurazione).

			Interface Stat	lus			
General License			Interface	IP Address/W	lask Line	Link	Current Kb
Host Name: pixfire	vall.default.domain.invalid	I Contraction of the second	linside	10.1.1.1/24	💽 up	🔮 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 inter	face to view inpu	t and output Kby	ps	
VPN Status			Traffic Status	-			
IKE Tunnels: 0	IPSec Tunnels:	0	Connections	Per Second Usage			
CPU CPU Usag	: (persent)		0.5 17:56:19 UDP: 0	TCP:	0 <u>1</u>	Fotal: D	d en tr
Memory - Memory U	age (MB)			ees (name onage (on had		
35%0 35%0 17,555,10			0.5 17:58:19	• • •	Output Kbo:	5 1	
Latest ASDM Stelles Me	00000					onfigure 45	DM Sydon Filt
	aanBra						and a second second

6. Per configurare l'interfaccia esterna, scegliere **Interfaccia > Modifica**.

Cisco ASDM	5.1 for PIX - 10.1.1.1				e Barra	<u>_ ×</u>
File Rules 8	Bearch Options Tools Wizards	Help				
G Home	Configuration Monitoring	Back Forward	Q Q Search Refresh	Save Help		CISCO SYSTEMS
	Configuration > Interfaces					
Interfaces	● 盘 筆 ■	- R. S. E. S				
Security Policy	Interface	Name Enabled	Security Level IP Address	Subnet Mask	Management MTU Only	Add
2 de	Ethernet0	No		Ī	No	Edit
NAT	Ethernet1	Inside Yes	10010.1.1.1	255.255.255.0	No 1500	Delete
93						
VPN						
Routing						
Rinhal Objects						
Properties						
	•				×	
	F Enable traffic between two	o or more interfaces w	hich are configured with	same security levels		
			Apply 1	Reset		
	,		<admin> </admin>	NA (15)	7/11/08	5:59:49 PM UTC

7. Immettere i dettagli dell'interfaccia e al termine fare clic su OK.

Edit Interface		
Hardware Port:	EthernetO	Configure Hardware Properties
🔽 Enable Interface	Dedicate this interface to mana	gement only
Interface Name:	outside	
Security Level:	0	
- IP Address		
Ose Static IP	C Obtain Address via DHCP	
IP Address:	172.16.1.1	
Subnet Mask:	255.255.255.0	
MTH		
MIO.	1500	
Description:		
	OK Cancel	Help

8. Fare clic su **OK** nella finestra di dialogo Modifica del livello di protezione.



9. Fare clic su **Apply** (Applica) per accettare la configurazione dell'interfaccia. La configurazione viene inoltre inserita nel

PIX.

Eile Dules	5.1 for PIX - 10.1.1.1	Holm	_					
Home	Configuration Montoring	Back F	orward	Q Search	Q Refresh	Save Help		Cisco Systems
Interfaces	Configuration ≻ Interfaces 	• • •	8 9					
Security Policy	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU Add
2 de	Ethernet0	outside	Yes	0	172.16.1.1	255.255.255.0	No 15	500 Edit
NAT	Ethernet1	inside	Yes	100	10.1.1.1	255.255.255.0	No: 15	500 Delete:
VPN 420 Routing Global Objects Properties	■ Enable traffic between to	vo ar more in	terfaces w	hich are c	onfigured with sa	ame secunty levels		-
				Apply	Re	eset	0	

10. Per esaminare la regola del criterio di protezione utilizzata, scegliere **Criterio di protezione** nella scheda Funzionalità. Nell'esempio viene utilizzata la regola interna predefinita.

Cisco ASDM 5.1	I for PIX - 10.1.1.1	tarta Hele					
Home C	onfiguration Monitoring	Back Forward	Q Q Search Refresh	Save Help		Cisi	CO SYSTEMS
Home C	Configuration Montoring Configuration - Security P Configuration - Security P Configuration - Security P Configuration - Security - Configuration Configuration Configuratio Configuration Configuration Configuration Configurati	Source HostNetwork	s C Service Policy Ru Show All Destination Host/Network	Save Hep les Rule Applied To Traffic	Interface inside (outbound)	Service	Add Edit Delete
		Apply	Reset	Advan	ced	0.1704.000.000	
			<admin></admin>	NA (15)	😹 🔂	7/11/06 6:01	:49 PM UTC

11. Nell'esempio viene utilizzato NAT. Deselezionare la casella di controllo **Abilita traffico attraverso il firewall senza conversione indirizzi** e fare clic su **Aggiungi** per configurare la regola

NAT.

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>	

 Configurare la rete di origine. Nell'esempio, viene usato 10.0.0.0 per l'indirizzo IP e 255.0.0.0 per la maschera.Per definire gli indirizzi del pool NAT, fare clic su Manage Pools (Gestisci pool).

0001411	00	Se Policy NAT				
Source Host	t/Network					
		Interface: IP Address: Mask:	inside 10.0.00 265.0.00		-	
			Browse			
						NAT Options
anslate Addi	ress on Inte	rface: outsi	de 🗾			
anslate Addi Translate Ad C 1 : s C	ress on Inte ddress To — Static T Redirect p	rface: outsi IP Address; iort	ide 🗾]	
anslate Addı Translate Ad C 1 : 8 F	ress on Inte ddress To — Static T Redirect p © TCP © UDP	rface: outsi IP Address; ort Original port	ide 🗾	▼ Translated p	ort:	
anslate Addi Translate Ad C 1 2 8 F C 1 2 8 F C 1 2 6	ress on Inte ddress To — Static Redirect p © TCP © UDP Dynamic	rface: outsi IP Address; fort Original port Address Pool:	de 💌	Translated p	ort: Manage P	ools
anslate Addi Translate Ad C 1 2 C C 1 2 C	ress on Inte ddress To — Static Redirect p © TCP © UDP Dynamic Pool ID	rface: outsi IP Address: fort Original port Address Pool:	de 📕	Translated p	ort: Manage P	ools
anslate Addi Translate Ad C 1 2 8	ress on Inte ddress To — Static Redirect p © TCP © UDP Dynamic Pool ID N/A	rface: outsi IP Address; fort Original port Address Pool: No address po	ide	Translated p ss 💽 ress	ort: Manage P	ools

13. Selezionare l'interfaccia esterna e fare clic su Add (Aggiungi).

Interface nside	Pool ID	IP Address(es)	Add
outside			Edit
			Delete

 In questo esempio vengono configurati un pool di indirizzi Range e PAT. Configurare l'intervallo dell'indirizzo del pool NAT e fare clic su OK.

2					
Range	1				
C Port A	idress Transla	ation (PAT)			
C Port A	ddress Transla	ation (PAT) usin	g the IP addre	ss of the interfa	ce
-					
IP A	ddress: 172	2.16.1.5	-	172.16.1.10	
	10				
Netv	vork Mask (opt	tional): 25	5.255.255.0		
100000					

15. Per configurare l'indirizzo PAT, selezionare l'interfaccia esterna al passaggio 13. Fare clic su

nterface:	outside	•	Pool ID:	1	
C Range					
Port Add	dress Translation	(PAT)			
C Port Ad	dress Translation	(PAT) using	the IP addres	s of the interface	9
IP Ad	dress: 172.16.	1.4	— – r		
Netw	ork Mask (optiona	il): 255.	255.255.0		

Per continuare, fare clic su **OK**.

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

 Nella finestra Modifica regola di conversione indirizzi selezionare l'ID pool che deve essere utilizzato dalla rete di origine configurata. Fare clic su OK.

• Use NAI	r cu	Ise Policy NAT					
Source Ho	st/Network						
		Interface: IP Address: Mask:	inside 10.0.0.0 255.0.0.0		- -		
			Browse				
				7			NAT Options
anslate Ad	dress on Inte	rface: outsi	de 💌 💌	1			
		,	_	-			
Translate /	Address To –						
Translate /	Address To – Static	IP Address:			-		
Translate /	Address To – Static Redirect p	IP Address: port			-		
Translate /	Address To – Static Redirect p © TCP © UDP	IP Address: port Original port		Translated	z port		
Translate / C · I·	Address To – Static Redirect (TCP C UDP Dynamic	IP Address: bort Original port Address Pool:	1	Translated	port Mana	ge Pools	
Translate /	Address To – Static Redirect (TCP C UDP Dynamic Pool ID	IP Address: bort Original port Address Pool:	[1 A	Translated	port Mana	ge Pools	
Translate /	Address To – Static Redirect (TCP CUDP Dynamic Pool ID	IP Address: oort Original port Address Pool: 172.16.1.4 172.16.1.5-172	1 1 1 1 1 1 1 1	Translated	port. Manaj	ge Pools	
Translate /	Address To – Static Redirect (TCP C UDP Dynamic Pool ID	IP Address: oort Original port Address Pool: 172.16.1.4 172.16.1.5-173	1 1 16110	Translated Idress	port. Manaj	ge Pools	

17. Fare clic su **Apply** (Applica) per eseguire il push della regola NAT configurata nel PIX.

tome Co	nfiguration	Monitoring	Back Forward	Search Refresh	Save Help		authran
erfaces	 A P Enable Transl Show Ru 	I > NAT > Trans Control I and Control I and	Internation Rules	is franslation nption Rules I Show All			
NAT	Rule		Original			Translated	Ad
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Ed
a <u>2</u> g	46	inside	⊑ [□] 10.0.0.0/8	🦘 any:	outside	172.16.1.4 172.16.1.5-172.16.1.10	Dele
Nobjects							
	Stati	NAT 🕀	Dynamic NAT 🖾 St	atic Policy NAT 🔬 D	Mamic Policy N	IAT Nanana Pools	<u>-</u>
	1.16			1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 - 1977 -		inaliage r colo	··· .

 Nell'esempio vengono utilizzate route statiche. Fare clic su Routing, selezionare Static Route, quindi fare clic su Add.

Elsco ASDM 5.1	1 for PIX - 10.1.1.1		<u>_ ×</u>
Home C	Configuration Montoring	Is Help	Cisco Systems
Hierfaces Security Policy NAT WPN Construction Constr	Configuration - Routing - Ro	Uting > Static Route Static Route Specify static routes. Interface IP Address Netmask Gateway IP Metric Tunneled	Add Edit Delete
		Asphy Reset	
	,	sadmin> NA (15) 🖓 🔂 🛛 🗛 7/1	1/06 7:45:00 PM UTC

19.	Configurare il	gateway	predefinito	e fare o	clic su
	- A 11 C				

<u></u>	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 ro	ute)
	ок	Cancel	Help

20. Fare clic su Add (Aggiungi) e aggiungere le route alle reti

	🚰 Add Static Rout	e			×
	Interface Na	me:	inside	•	
	IP Address:		10.2.1.0		
	Mask:		255.255.255.0	•	
	Gateway IP:		10.1.1.2		
	Metric		1		
	C Tunneled	(Used o	nly for default rou	ute)	
interne.	ОК		Cancel	Help	
🔂 Ado	l Static Route			×	
i Ado	<mark>i Static Route</mark> Interface Name:	inside		×	
Add	i Static Route Interface Name: IP Address:	inside 10.3.1	.0	X	
Add	d Static Route Interface Name: IP Address: Mask:	inside 10.3.1	. 0 55.255.0 ▼	X	
Add	i Static Route Interface Name: IP Address: Mask: Gateway IP:	inside 10.3.1 255.2 10.1.1	.0 55.255.0	X	
Add	Interface Name: IP Address: Mask: Gateway IP: Metric	inside 10.3.1 255.2 10.1.1	.0 55.255.0	X	
Add	Interface Name: IP Address: Mask: Gateway IP: Metric Tunneled (Used o	10.3.1 255.2 10.1.1 1 0nly for d	1.0 55.255.0		

21. Verificare che siano configurate le route corrette e fare clic su **Applica**.

File Rules 6	5.1 for PIX - 10.1.1.1 earch Options Tools Wizar	ts Help	×
S Home	Configuration Monitoring	O O Q O Refresh Save Help	Cisco Systems
Interfaces Interfaces Security Policy NAT Security Policy NAT Security Poly Routing Global Objects Properties	Configuration - Routing - Ro Multicast MRoute MRoute B B PIM B COSPF - Proxy ARPs - RIP - Static Route	Interface IP Address Netmask Gateway IP Metric Tuni outside Interface IP Address Netmask Gateway IP Metric Tuni outside Inside 10.0.0 0.0.0.0 172.18.1.2 1 P Inside 10.2.1.0 255.255.255.0 10.1.1.3 1 P Inside 10.3.1.0 265.255.255.0 10.1.1.3 1 P	neler Add IG IA Delete
	<u> </u>	<admin> NA (15) → → →</admin>	₱ 7/11/06 7:48:40 PM UTC

Configurazione PIX con CLI

La configurazione tramite l'interfaccia grafica ASDM è ora completata.

Èpossibile visualizzare questa configurazione dalla CLI:

PIX Security Appliance CLI

```
pixfirewall(config)#write terminal
PIX Version 7.0(0)102
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-
```



Per visualizzare la configurazione CLI in ASDM, scegliere **File > Mostra configurazione corrente** in **una nuova finestra**.

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

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

- **debug icmp trace**: visualizza se le richieste ICMP dagli host raggiungono il PIX. Per eseguire il debug, aggiungere il comando **access-list** per autorizzare l'uso di ICMP nella configurazione.
- **logging buffer debugging**: visualizza le connessioni stabilite e negate agli host che passano attraverso il PIX. Le informazioni vengono memorizzate nel buffer di registro PIX e l'output può essere visualizzato con il comando **show log**.

Procedura di risoluzione dei problemi

ASDM può essere utilizzato per abilitare il logging e anche per visualizzare i log:

1. Scegliete Configurazione > Proprietà > Registrazione > Impostazione registrazione, selezionate Abilita registrazione e fate clic su

Applica.	5.1 for PIX - 10.1.1.1		-		-0>
File Rules B	earch Options Tools Wizard	is Help	_		
S Home	Configuration Montoring	Back Forward Search	Retresh	🗐 🧖 Save Help	Cisco Systems
Herrisces Security Policy NAT VPN Routing Global Objects Properties	Configuration > Properties > I	Logging > Logging Setup Logging Setup File A Set File (Constraint) File Send debug message Logging to Internal Buffer Specify the size of the inter be overwritten. Buffer Size: 4096 You can choose to save the Save Buffer To: File ASDM Logging Specify the size of the que Gueue Size: 100	es as syslogs email buffer to w bytes he buffer contei rP Server ash ue for syslogs	Enable logging Send syslogs i which syslogs will be saved nts before the buffer is over Configure FTP Settings Configure Flash Usage Intended for viewing in ASE Reset	g on the failover standby unit in EMBLEM format When the buffer fills up, it will written.

2. Scegliere **Monitoraggio > Log buffer > Livello di log** e scegliere **Log buffer** dall'elenco a discesa. Fare clic su

Visualizza	l.								
Elsco ASDM 3	5.1 for PIX - 10.	1.1.1 Tools Wizen	is Heln		199	122			
Home	Configuration	Monitoring	Back	Forward	Q Search	Refresh	Бале	? Help	CISCO SYSTEMS
	Monitoring >	Logging > Log B	utter						
Interfaces	C E Log B	time Log Viewer Juffer	-Log 9u	lffør					
VFN VFN Routing				Click the ASDM as or higher.	view button k of now. Sele	oelow to disp ct the desire	ilay syslog r d logging le poing	messages in the wel to see mess	a logging buffer for sages at that severity
Properties ELogging								-	
							lew		
	1								

3. Di seguito è riportato un esempio di buffer del log:

💁 Log Buf	fer Electron	
C Rema	esh 🔄 Save 🖙 Clea	r 🛄 Color Settings 📲 Create Rule 🔤 Brithw Rule Find:
This table	shows syslog messages	s in ASDM logging buffer as of now.
Severity	Time	Message ID: Description
<u>ê</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>4</u> 6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
<u>ê</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>ê</u> 6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) 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>4</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>4</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
<u>1</u> 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>*</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>4</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
<u>4</u> 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>i</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
<u>*</u> 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>i</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>4</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>i</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>4</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>4</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>4</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
<u>∔</u> 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	nergencies 🗿 Alerts	Critical e Errors A Warnings A Notifications A Informational O Debugging

Impossibile accedere ai siti Web per nome

In alcuni casi, le reti interne non possono accedere ai siti Web utilizzando il nome (funziona con l'indirizzo IP) nel browser. Questo problema è comune e si verifica in genere se il server DNS non è definito, in particolare nei casi in cui PIX/ASA è il server DHCP. Inoltre, ciò può verificarsi se il PIX/ASA non è in grado di eseguire il push del server DNS o se il server DNS non è raggiungibile.

Informazioni correlate

- <u>Cisco PIX serie 500 Security Appliance</u>
- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- <u>Riferimenti per i comandi di Cisco Secure PIX Firewall</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Risoluzione dei problemi e avvisi di Cisco Adaptive Security Device Manager (ASDM)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico Cisco Systems