# PIX/ASA 7.x: Esempio di configurazione di SSH/Telnet sull'interfaccia interna ed esterna

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione Esempio di rete Configurazioni SSH Configurazione con ASDM 5.x Configurazione con ASDM 6.x **Configurazione Telnet** Supporto SSH/Telnet in ACS 4.x Verifica Debug SSH Visualizzazione delle sessioni SSH attive Visualizza chiave RSA pubblica Risoluzione dei problemi Come rimuovere le chiavi RSA dal PIX Connessione SSH non riuscita Impossibile accedere ad ASA con SSH Impossibile accedere all'appliance ASA secondaria con SSH Informazioni correlate

# **Introduzione**

In questo documento viene fornito un esempio di configurazione di Secure Shell (SSH) sulle interfacce interna ed esterna di Cisco Series Security Appliance versione 7.x e successive. La configurazione dell'appliance di sicurezza serie in remoto con la riga di comando implica l'uso di Telnet o SSH. Poiché le comunicazioni Telnet vengono inviate in formato testo non crittografato, incluse le password, si consiglia di utilizzare il protocollo SSH. Il traffico SSH è crittografato in un tunnel e contribuisce a proteggere le password e altri comandi di configurazione dall'intercettazione.

L'appliance di sicurezza consente le connessioni SSH all'appliance di sicurezza a scopo di gestione. L'appliance di sicurezza consente un massimo di cinque connessioni SSH simultanee per ciascun <u>contesto di sicurezza</u>, se disponibili, e un massimo globale di 100 connessioni per tutti

i contesti combinati.

Nell'esempio di configurazione, l'appliance di sicurezza PIX è considerata il server SSH. Il traffico tra i client SSH (10.1.1.2/24 e 172.16.1.1/16) e il server SSH è crittografato. L'appliance di sicurezza supporta la funzionalità SSH della shell remota fornita nelle versioni 1 e 2 e le cifrature Data Encryption Standard (DES) e 3DES. Le versioni 1 e 2 del protocollo SSH sono diverse e non sono interoperabili.

# **Prerequisiti**

## **Requisiti**

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco PIX Firewall versione 7.1 e 8.0.

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.

**Nota:** SSHv2 è supportato in PIX/ASA versione 7.x e successive e non nelle versioni precedenti alla 7.x.

## Prodotti correlati

Questa configurazione può essere utilizzata anche con l'appliance di sicurezza Cisco ASA serie 5500 con software 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:** a ogni passo della configurazione vengono presentate le informazioni necessarie per utilizzare la riga di comando o Adaptive Security Device Manager (ASDM).

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

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



## **Configurazioni SSH**

Nel documento vengono usate queste configurazioni:

- <u>Accesso SSH alle appliance di sicurezza</u>
- <u>Come utilizzare un client SSH</u>
- <u>Configurazione PIX</u>

### Accesso SSH alle appliance di sicurezza

Per configurare l'accesso SSH all'appliance di sicurezza, attenersi alla seguente procedura:

1. Le sessioni SSH richiedono sempre un nome utente e una password per l'autenticazione. Esistono due modi per soddisfare questo requisito.Configurare un nome utente e una password e utilizzare il server AAA:Sintassi: pix(config)#username username password password pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server\_group [LOCAL]}

**Nota:** se si utilizza un gruppo di server TACACS+ o RADIUS per l'autenticazione, è possibile configurare l'appliance di sicurezza in modo che utilizzi il database locale come metodo di fallback se il server AAA non è disponibile. Specificare il nome del gruppo di server, quindi LOCAL (LOCAL rileva la distinzione tra maiuscole e minuscole). È consigliabile utilizzare lo stesso nome utente e la stessa password nel database locale del server AAA, in quanto il prompt dell'appliance di sicurezza non indica in alcun modo il metodo utilizzato.**Nota:** esempio:

pix(config)#aaa authentication ssh console TACACS+ LOCAL

**Nota: in** alternativa è possibile utilizzare il database locale come metodo di autenticazione principale senza fallback. A tale scopo, immettere LOCAL da solo.Esempio: pix(config)#aaa authentication ssh console LOCAL

OUsare il nome utente predefinito **pix** e la password Telnet predefinita di **cisco**. È possibile modificare la password Telnet con questo comando: pix(config)#passwd password

**Nota:** il comando **password** può essere utilizzato anche in questa situazione. Entrambi i comandi eseguono la stessa operazione.

2. Generare una coppia di chiavi RSA per PIX Firewall, necessaria per SSH: pix(config)#crypto key generate rsa modulus modulus\_size

**Nota:** il valore di modulus\_size (in bit) può essere 512, 768, 1024 o 2048. Maggiore è la dimensione del modulo chiave specificata, maggiore sarà il tempo necessario per generare la coppia di chiavi RSA. Si consiglia un valore di 1024.**Nota:** il comando utilizzato per generare una coppia di chiavi RSA è diverso nelle versioni software PIX precedenti alla 7.x. Nelle versioni precedenti è necessario impostare un nome di dominio prima di poter creare le chiavi.**Nota:** in modalità contesto multiplo, è necessario generare le chiavi RSA per ogni contesto. Inoltre, i comandi crypto non sono supportati in modalità contesto di sistema.

- 3. Specificare gli host autorizzati alla connessione all'appliance di sicurezza.Questo comando specifica l'indirizzo di origine, la netmask e l'interfaccia degli host a cui è consentito connettersi con SSH. Può essere immesso più volte per più host, reti o interfacce. Nell'esempio, sono consentiti un host all'interno e un host all'esterno. pix(config)#ssh 172.16.1.1 255.255.255 inside pix(config)#ssh 10.1.1.2 255.255.255 outside
- 4. Facoltativo: Per impostazione predefinita, l'appliance di sicurezza supporta sia la versione 1 che la versione 2 del protocollo SSH. Immettere questo comando per limitare le connessioni a una versione specifica: pix(config)# ssh version

Nota: il numero\_versione può essere 1 o 2.

5. **Facoltativo:** Per impostazione predefinita, le sessioni SSH vengono chiuse dopo cinque minuti di inattività. Questo timeout può essere configurato in modo da durare da 1 a 60 minuti.

pix(config)#ssh timeout minutes

#### Come utilizzare un client SSH

Fornire il nome utente e la password di accesso dell'appliance di sicurezza PIX serie 500 quando si apre la sessione SSH. Quando si avvia una sessione SSH, sulla console dell'appliance di sicurezza viene visualizzato un punto (.) prima della visualizzazione del prompt di autenticazione dell'utente SSH:

#### hostname(config)# .

La visualizzazione del punto non influisce sulla funzionalità SSH. Il punto viene visualizzato sulla console quando viene generata una chiave del server o quando un messaggio viene decrittografato con chiavi private durante lo scambio di chiavi SSH prima dell'autenticazione dell'utente. Queste attività possono richiedere fino a due minuti o più. Il punto è un indicatore di stato che verifica se l'appliance di sicurezza è occupata e non è bloccata.

SSH versioni 1.x e 2 sono protocolli completamente diversi e non sono compatibili. Scaricare un client compatibile. Per ulteriori informazioni, consultare la sezione <u>Ottenere un client SSH</u> in <u>Configurazioni avanzate</u>.

**Configurazione PIX** 

Nel documento viene usata questa configurazione:

**Configurazione PIX** 

```
PIX Version 7.1(1)
1
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface Ethernet0
nameif outside
security-level 0
ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
nameif inside
 security-level 100
ip address 172.16.5.10 255.255.0.0
1
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp permit any outside
no asdm history enable
arp timeout 14400
route outside 10.1.1.0 255.255.255.0 192.168.200.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!--- AAA for the SSH configuration username ciscouser
password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL
http server enable
http 172.16.0.0 255.255.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstar
telnet timeout 5
!--- Enter this command for each address or subnet !---
to identify the IP addresses from which !--- the
security appliance accepts connections. !--- The
security appliance accepts SSH connections from all
interfaces. ssh 10.1.1.2 255.255.255.255 outside
!--- Allows the users on the host 172.161.1.1 !--- to
access the security appliance !--- on the inside
interface. ssh 172.16.1.1 255.255.255.255 inside
```

!--- Sets the duration from 1 to 60 minutes !--(default 5 minutes) that the SSH session can be idle, !-



**Nota:** per accedere all'interfaccia di gestione dell'ASA/PIX con SSH, usare questo comando: SSH 172.16.160.255.255.255.255 Gestione

## Configurazione con ASDM 5.x

Per configurare il dispositivo SSH utilizzando ASDM, attenersi alla seguente procedura:

 Per aggiungere un utente con ASDM, scegliere Configurazione > Proprietà > Amministrazione dispositivi > Account utente.

di Home	Configuration Monitoring	Gack Forward	Q Q Search Refresh	📑 🦓 Save Help		Cisco Systems
Hterfaces	Configuration > Properties > Devi	Ce Administration > User Accounts Create entries in the User account privileg	er Accounts PIX local user databa es to be enforced. To Privilege (Level)	se. Command author enable command aut VPN Group Policy	ization must be enable horization, go to <u>Autho</u> VPN Group Lock	d in order for the fization.
VPN Routing Global Objects Properties	Console Clock Clock Clock Console Clock Console Clock Console Cons	enable_15 ciscouser	(NA (15)  NA (2)	DiftGrpPolicy	Inherit Group Po	Edit Delete
	Server		Apply	Rese		18 8-18-29 DHI I ITA

2. Per impostare l'autenticazione AAA per SSH con ASDM, scegliere **Configurazione > Proprietà > Accesso dispositivo > Accesso AAA >** 

G Home	Configuration Monitoring	Back Forward	Q C Search Refr	sh Save	<b>?</b> Нар	Cisco Systems
Interfaces Security Policy NAT	Configuration - Properties - Configuration - Properties - Startup Wizard AAA Setup - BAAI-Spoofing - AAA Setup - BAAI-Spoofing - AAA Setup - BAAI-Spoofing - AAA Setup - BAAI-Spoofing - BAAI-Spoofin	Device Access > AAA Acc Authentication/Authon Enable authenticat Require authenticat Enable	rizationAccounting Authorization for administra ntication to allow u Server Group:	Accounting tor access to the use of privileged in LOCAL	PIX. mode comman	ds
VPN	PHTTPS/ASDM     Source Shell     Source Shell     Source Administration     Source Administratin     Source Administration     Source Administr	Require auther F HTTP/ASDM F Serial F SSH	ntication for the fol 1 Server Group: Server Group: Server Group:	lowing types of c [LOCAL ] [LOCAL ] [LOCAL ]	onnections	LOCAL when server group fails LOCAL when server group fails LOCAL when server group fails
Properties	P Audit     Cogging     Priority Queue     SSL     SUNRPC Server     STCP Options     OTimeouts     WRL Filtering	☐ Teinet	Server Group:		TUse Reset	LOCAL when server group fails
Device configura	tion loaded successfully.		ciscous	er NA (2)		🔂 5/23/06 6:24:28 PM UTC

3. Per modificare la password Telnet con ASDM, scegliere Configurazione > Proprietà > Amministrazione dispositivi > Password.

Home C	Sonfiguration Monitoring	C C C C C C C C C C C C C C C C C C C	у Сіясо Ятятемя Нар
Home C	Configuration       Montorng         Configuration       Properties > I         P       P         Startup Wizard       Image: Startup Wizard         P       AAA Setup         Banti-Spoofing         Device Access         Device Access         Device Administration         Banner         Boot Image/Con         Clock         Device         PTP Mode         Device         PTP Mode         Management Acc         NITP         Secure Copy         SMTP         SMMP         TFTP Server         OUSer Accounts         DHCP Services         DNS Client         Failover	Back       Forward       Search       Refresh       Save         Mice Administration > Presevord       Image: Search       Refresh       Save         Password       Change the privileged mode and Telnet passwords.       Image: Search       Enable Password         Change the privileged mode and Telnet password       Image: Search       Image: Search       Telnet password         Confirm New Password:       Image: Search       Image: Search       Image: Search       Image: Search         Telnet Password       Image: Search       Image: Search       Image: Search       Image: Search         Old Password:       Image: Search       Image: Search       Image: Search       Image: Search         Old Password:       Image: Search       Image: Search       Image: Search       Image: Search         Old Password:       Image: Search       Image: Search       Image: Search       Image: Search         Old Password:       Image: Search       Image: Search       Image: Search       Image: Search       Image: Search         New Password:       Image: Search       Image: Search       Image: Search       Image: Search       Image: Search         Output       Image: Search       Image: Search       Image: Search       Image: Search       Image: Search       Image: Search       I	Hap also the password to log into ASDM.
Device configurat	ion loaded successfully.	ciscouser NA (2)	📓 🛛 🔒 5/23/06 6:30:38 PM UTC

 Scegliere Configurazione > Proprietà > Certificato > Coppia di chiavi, fare clic su Aggiungi e usare le opzioni predefinite presentate per generare le stesse chiavi RSA con ASDM.



5. Scegliere Configurazione > Proprietà > Accesso dispositivo > Secure Shell per utilizzare ASDM per specificare gli host a cui è consentito connettersi con SSH e le opzioni di versione e

timeout.

ổ Home 🕻	Configuration Monitoring	Sack Forward Search Refresh Save Help	CISCO SYSTEMS
Hieritaces Security Policy NAT Security Policy NAT Security Routing Global Objects Sichal Objects	Configuration > Properties > D  Configuration > Properties > D  Configuration > Properties > D  Configuration Wizard  Configuration  AAA Setup  AAA Setup  AAA Setup  ARP  AAA Cocess  AAA Access  AAAA Access  AAA Access  AAA Access  AA	Mice Access = Secure Shell         Secure Shell         Allowed SSH Version(s):       Timeout         Specify the addresses of all hosts/networks which are allowed to accusing Secure Shell (SSH).         Interface       IP Address         Interface       172.18.1.1         255.255.255.255.         outside       10.1.1.2	minutes cess the PIX sk Add 255 Edit Delete
	Timeouts	Apply Reset	
Device configurat	ion loaded successfully.	ciscouser NA (2)	🚱 🗄 5/23/06 6:37:58 PM UTC

6. Per salvare la configurazione, fare clic su **File > Salva configurazione corrente** in **Flash**.

🚰 Cisco ASDM 5.2 for ASA - 172.16.33.1				
File 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	ward Packet Tracer Refre			
Save Running Configuration to Flash	Configuration			
Save Running Configuration to TFTP Server Save Running Configuration to Standby Unit Save Internal Log Buffer to Flash Print	nfiguration hfigure boot images from an externa the boot system. Only one TFTP bo first image in the list.			
Clear ASDM Cache Clear Internal Log Buffer	ioot Order			
Exit	1 disk0:/pix722.bin			
VPN	2			

## Configurazione con ASDM 6.x

Attenersi alla seguente procedura:

1. Per aggiungere un utente con ASDM, scegliere **Configurazione > Gestione dispositivi > Utenti/AAA >** Account

ut	ente.								
C	) Home 🚳 Configuration 🔯 Monitori	ing 🔚 Save 💽 Re	efresh 🕜 Back 🔘 Form	rd े Help			cisco		
	Device Management 3 P ×	Configuration > De	vice Management > Users/	AAA > User Accounts					
Device Ust	Point Access     System Image/Configuration     Point Access     Point Access	Create entries in the ASA local user database. Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to <u>A</u> AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication go to <u>Authontication</u> .							
	-IDo AAA Access	Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add		
	- Dynamic Access Policies	ssluser1	2	Ful	Inherit Group Policy	Inherit Group Policy			
	Set User Accounts	enable_15	15	rul	N(A	N/A	Edit		
	E-M DHCP						Delete		
	E BLDNS								
	🖲 📆 Advanced								
	A Device Setup								
	Frexal								
	Remote Access VPN								
	Sterto-Site VPN								
	Device Management								
				Αρτίγ	Reset				
	p)			<admin></admin>	15 😡	😹 🛛 🖻 3/2	/00 10:10:29 PM 15T		

2. Per impostare l'autenticazione AAA per SSH con ASDM, scegliere **Configurazione > Gestione dispositivi > Utenti/AAA > Accesso AAA >** Autenticazione.

Device Management & A	Configuration > Device Management > Users/AAA > AAA Access > Authentication
· · · · · · · · · · · · · · · · · · ·	Authentication Authorization Accounting
≧     ⊕     ₩igh Availability       □     ≅     •       □     E     Logging	Enable authentication for administrator access to the ASA.
E- State AAA Server Groups	Require authentication to allow use of privileged mode commands
Authentication Prompt	Enable Server Group: LOCAL V Use LOCAL when server group fails
- 🏰 Dynamic Access Policies	Require authentication for the following types of connections
👷 User Accounts 	HTTP/ASDM Server Group: LOCAL 💌 🔲 Use LOCAL when server group fails
B-f DHCP	Serial Server Group: LOCAL T Use LOCAL when server group fails
E-B Advanced	Server Group: LOCAL View DCAL when server group fails
	Teinet Server Group: LOCAL 💌 🔲 Use LOCAL when server group fails
S. During Setur.	
Frewal	
Remote Access VPN	
Ske-to-Ske VPN	
Device Management	
*	Appry Reset
	<admin> 15 😡 🛱 🔒</admin>

 Per modificare la password Telnet con ASDM, scegliere Configurazione > Configurazione dispositivo > Nome/password.

đ	) Home 🦓 Configuration 🔯 Monitorin	ng 🔚 Save 🔇 Refre	sh 🔇 Back 🔘 Forward	💡 Help			
	Device Setup _ 0 ×	Configuration > Devic	e Setup > Device Name/P	assword			
eLis		Hostname and Domain Na	ame				
Devk	H-++++ Routing	Hostname:	ciscoasa				
	Device Name/Password     System Time	Domain Name:	default.domain.invalid				
		Enable Password					
		Change the priviles	ged mode password.				
		Old Password:					
		New Password:					
		Confirm New Password	i:				
		Telnet Password					
		🔽 Change the passw	ord to access the console of the	security appliance.			
		Old Password:					
		New Password:					
		Confirm New Password	d:				
	A Device Setup						
	Frewal						
	Remote Access VPN						
	Ste-to-Site VPN						
	Device Management						
	*			Apply	Reset		
				<admin< th=""><th>&gt; 15</th><th>😡 🍰</th><th>6</th></admin<>	> 15	😡 🍰	6

4. Scegliere Configurazione > Gestione dispositivi > Gestione certificati > Certificati di identità, fare clic su Aggiungi e usare le opzioni predefinite presentate per generare le stesse chiavi RSA per

A	S	D	M
	-	_	

wice Management @ ₽ × Coni	iguration > Device Manage	ement > Certificate Managen	ent > Identity Certificate	5	
SMMP	Issued To	Issued By	Expiry Date	Usage	Add
System Image/Configuration					Show Deteri
- 🚵 Activation Key	Add Identity Certificate			X	DeGelder
- Sect Image/Configuratio	C. C. Martin and Martin and				French
🔐 High Availability	<ul> <li>Import the identity certified</li> </ul>	icate from a file:	_		Export
G Users/AAA	Decryption Passphrase:				Instal
Certificate Management	File to Import From:		Втомар		
- Res Identity Certificates	Add a new identity certif	salet			
P OHOP	Key Pair:	<default-rsa-key></default-rsa-key>	Show New.		
- Mr DHCP Relay	Test Preter To breat The				
DNS DNS	Certificate Subject Diva	ICN-discoasa	Select		
Advanced	Generate self-signed	certificate			
- 🚟 ARP Static Table	🔲 Act as local certif	kate authority and issue dynamic	certificates to TLS-Proxy		
- HITP Redirect				given interface. You can g	o to <u>SSL Settings</u>
- 🔄 History Metrics			Advanced	L	
Device Setup	Add Certifi	cate Cancel	Help		
-					
Eemote Access VPN					
Ste to Ske VPN					

5. In Aggiungi nuovo certificato di identità fare clic su Nuovo per aggiungere una coppia di

chiavi predefinita, se non ne esiste una. Fare quindi clic su **Genera**.

G	Home 🖓 Configuration 📴 Monitorin	ng 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help	CISCO					
*	Device Management at a x Configuration > Device Management > Certificate Management > Identity Certificates							
Se Le	Management Access     Sustem Image/Configuration							
Den	E W High Availability	Issued To Issued By Expiry Date Usage	Add					
	E- 🔂 Logging		Show Details					
	AAA Server Groups	🔂 Add Identity Certificate	Delete					
	- Se Authentication Prompt	C. Tenands the Identify conditions from a file.	Friend					
	- Dynamic Access Policies	C Import the identity certificate man a ris:	Export					
	- 5 User Accounts	Decryption Passphrase:	Instal					
	- 2 CA Certificates	File to Import From: Erowac						
	Provident Report Frances	Add a new identity certificate:						
	EF 👼 DNS	Key Pair: <default-rsa-key> Y Show New</default-rsa-key>						
	E- C Advanced	Cett Cit Add Key Pair						
		Name: 🕥 Use default kuy pair name						
		C Enternewikey pair name:	to TTL Column to					
		Size: 1024	00 201 200 105 00					
		Usage: 🕫 General purpose 🔿 Special						
	Q During Solution							
	Device setup	Generate Now Cancel Help						
	Firewall							
	Remote Access VPN							
	Ste-to-Site VPN							
	Device management							
	*	Appty Reset						

 Per utilizzare ASDM e specificare gli host a cui è consentito connettersi con SSH e le opzioni di versione e timeout, scegliere Configurazione > Gestione dispositivi > Accesso alla gestione > Riga di comando (CLI) > Secure Shell (SSH).

C	Home 🦓 Configuration 🔯 Monitorin	g 🔚 Save 🔇 Refresh 🤇	Back 🔘 Forward 🧳 Help		CISCO
	Device Management 🗗 🤉 🛛	Configuration > Device Mana	agement > Management Access > Command L	Line (CLI) > Secure Shell (SSH)	
Dentce List	Management Access     ASDM(HTTPS     Some of the second seco	Allowed SSH Version(s): 1 & 2  Timeout: 5 minutes Specify the addresses of all hosts/networks which are allowed to access the ASA using Secure Shell (SSH).			
	- Del CLI Prompt	Interface	IP Address	Mask	Add
	🗧 🍓 Console Timeout	inside	10.77.241.142	255.255.255.255	(hereas)
	- 🍓 Secure Shell (SSH) - 🚌 Teinet	outside	192.168.200.1	255.255.255.255	Edit
	E- B File Access				Delete
	Management Interface				
	E System Image/Configuration				
	H 🔐 High Availability				
	E-C Logang				
	AAA Server Groups				
	- Se Authentication Prompt				
	- 🔂 AAA Access				
	User Accounts				
	H- Certricate Management				
	4 D				
	A Device Setup				
	Frewall				
	Remote Access VPN				
	Ste-to-Site VPN				
	Device Management				
	*		Apply	Reset	

7. Per salvare la configurazione, fare clic su **Save** (Salva) nella parte superiore della finestra.

File	View Tools Wizards	Window	Help	
	Home Configuration	Monit	oring 🔚 Save 🐼 Refresh 🔇 Back 🕥 Forward 🤗 H	elp
	Device Management	а т ×	Config Save Running Configuration to Flash Management Acc	cess >
/ice List	Management Access		Allowed SSH Version(s): 1 & 2 💌 Timeout: 5	

8. Quando viene chiesto di salvare la configurazione sulla memoria flash, scegliere **Apply** (Applica) per salvarla.

## **Configurazione Telnet**

Per aggiungere l'accesso Telnet alla console e impostare il timeout di inattività, usare il comando **telnet** in modalità di configurazione globale. Per impostazione predefinita, le sessioni Telnet rimaste inattive per cinque minuti vengono chiuse dall'appliance di sicurezza. Per rimuovere l'accesso Telnet da un indirizzo IP impostato in precedenza, utilizzare la forma *no* di questo comando.

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout
number}}
no telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} |
{timeout number}}
```

Il comando **telnet** consente di specificare quali host possono accedere alla console dell'appliance di sicurezza tramite Telnet.

**Nota:** è possibile abilitare Telnet su tutte le interfacce dell'accessorio di sicurezza. Tuttavia, l'appliance di sicurezza applica la protezione IPsec a tutto il traffico Telnet diretto all'interfaccia esterna. Per abilitare una sessione Telnet con l'interfaccia esterna, configurare IPsec sull'interfaccia esterna in modo da includere il traffico IP generato dall'appliance di sicurezza e abilitare Telnet sull'interfaccia esterna.

**Nota:** in generale, se un'interfaccia ha un livello di sicurezza pari a 0 o inferiore a quello di un'altra interfaccia, il protocollo PIX/ASA non consente il collegamento Telnet a quell'interfaccia.

**Nota:** si consiglia di non accedere all'accessorio di protezione tramite una sessione Telnet. Le informazioni sulle credenziali di autenticazione, ad esempio la password, vengono inviate come testo non crittografato. La comunicazione tra server e client Telnet avviene solo con testo non crittografato. Cisco consiglia di utilizzare il protocollo SSH per una comunicazione dei dati più sicura.

Se si immette un indirizzo IP, è necessario immettere anche una netmask. Non esiste una maschera di rete predefinita. Non utilizzare la subnetwork mask della rete interna. La netmask è solo una maschera di bit per l'indirizzo IP. Per limitare l'accesso a un singolo indirizzo IP, utilizzare 255 in ciascun ottetto; ad esempio, 255.255.255.255.

Se IPSec funziona, è possibile specificare un nome di interfaccia non sicuro, in genere l'interfaccia esterna. È possibile configurare almeno il comando **crypto map** per specificare un nome di interfaccia con il comando **telnet**.

Usare il comando **password** per impostare una password per l'accesso Telnet alla console. Il valore predefinito è cisco. Per visualizzare gli indirizzi IP che accedono attualmente alla console dell'appliance di sicurezza, usare il comando **who**. Utilizzare il comando **kill** per terminare una sessione console Telnet attiva.

Per abilitare una sessione Telnet per l'interfaccia interna, esaminare gli esempi seguenti:

Esempio 1

Nell'esempio seguente viene consentito solo all'host 10.1.1.1 di accedere alla console dell'appliance di sicurezza tramite Telnet:

pix(config)#telnet 10.1.1.1 255.255.255.255 inside Esempio 2

Nell'esempio seguente viene consentito l'accesso alla console dell'appliance di sicurezza solo alla rete 10.0.0.0/8 tramite Telnet:

pix(config)#telnet 10.0.0.0 255.0.0.0 inside
Esempio 3

Nell'esempio seguente tutte le reti possono accedere alla console dell'accessorio di protezione tramite Telnet:

pix(config)#telnet 0.0.0.0 0.0.0.0 inside

Se si utilizza il comando **aaa** con la parola chiave console, l'accesso alla console Telnet deve essere autenticato con un server di autenticazione.

**Nota:** se il comando **aaa** è stato configurato in modo da richiedere l'autenticazione per l'accesso alla console Telnet dell'accessorio di sicurezza e la richiesta di accesso alla console scade, è possibile accedere all'accessorio di sicurezza dalla console seriale. A tale scopo, immettere il nome utente e la password dell'accessorio di protezione impostati con il comando **enable password**.

Utilizzare il comando **telnet timeout** per impostare il tempo massimo di inattività di una sessione Telnet della console prima che l'accessorio di sicurezza la disconnetta. non è possibile usare il comando **no telnet** con il comando **telnet timeout**.

Nell'esempio viene mostrato come modificare la durata massima di inattività della sessione:

hostname(config)#telnet timeout 10
hostname(config)#show running-config telnet timeout
telnet timeout 10 minutes

Supporto SSH/Telnet in ACS 4.x

Se si esaminano le funzioni RADIUS, è possibile utilizzare RADIUS per la funzionalità SSH.

Quando si tenta di accedere all'accessorio di protezione tramite una connessione Telnet, SSH, HTTP o una console seriale e il traffico corrisponde a un'istruzione di autenticazione, l'accessorio di protezione richiede un nome utente e una password. Invia quindi queste credenziali al server RADIUS (ACS) e concede o nega l'accesso CLI in base alla risposta del server.

Per ulteriori informazioni, consultare la sezione <u>Server AAA e supporto del database locale</u> in <u>Configurazione dei server AAA e del database locale</u>.

Ad esempio, l'appliance di sicurezza ASA 7.0 richiede un indirizzo IP da cui l'appliance accetta le connessioni, come:

hostname(config)#ssh source\_IP\_address mask source\_interface

Per ulteriori informazioni, consultare la sezione <u>Autorizzazione dell'accesso SSH</u> in <u>Configurazione dei server AAA e del database locale</u>.

Per ulteriori informazioni, fare riferimento al documento <u>PIX/ASA: Proxy Cut-through per l'accesso</u> <u>alla rete con TACACS+ e esempio di configurazione del server RADIUS</u> per ulteriori informazioni su come configurare l'accesso SSH/Telnet ai PIX con autenticazione ACS.

# **Verifica**

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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**.

## **Debug SSH**

Usare il comando debug ssh per attivare il debug SSH.

pix(config)#**debug ssh** SSH debugging on

Questo output mostra che la richiesta di autenticazione dall'host 10.1.1.2 (esterno a PIX) a "pix" ha esito positivo:

```
pix#
Device ssh opened successfully.
   SSH0: SSH client: IP = '10.1.1.2' interface # = 1
   SSH: host key initialised
   SSH0: starting SSH control process
   SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
   SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
client version string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0:
begin ser ver key generation
   SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
```

```
SSH2 0: SSH2_MSG_KEXINIT received
   SSH2: kex: client->server aes128-cbc hmac-md5 none
   SSH2: kex: server->client aes128-cbc hmac-md5 none
   SSH2 0: expecting SSH2_MSG_KEXDH_INIT
   SSH2 0: SSH2_MSG_KEXDH_INIT received
   SSH2 0: signature length 143
   SSH2: kex_derive_keys complete
   SSH2 0: newkeys: mode 1
   SSH2 0: SSH2_MSG_NEWKEYS sent
   SSH2 0: waiting for SSH2_MSG_NEWKEYS
   SSH2 0: newkeys: mode 0
  SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method is
'no AAA', aaa server group ID = 0
  SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication successful for pix
!--- Authentication for the PIX was successful. SSH2 0: channel open request SSH2 0: pty-req
request SSH2 0: requested tty: vt100, height 25, width 80 SSH2 0: shell request SSH2 0: shell
message received
```

Se un utente assegna un nome utente errato, ad esempio "pix1" anziché "pix", il firewall PIX rifiuta l'autenticazione. Questo output di debug visualizza l'autenticazione non riuscita:

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
   string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix1): user authen method is
'no AAA', aaa server group ID = 0
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix1
!--- Authentication for pix1 was not successful due to the wrong username.
```

Analogamente, se l'utente specifica una password errata, questo output di debug mostrerà l'autenticazione non riuscita.

pix# Device ssh opened successfully. SSH0: SSH client: IP = '10.1.1.2' interface # = 1 SSH: host key initialised SSH0: starting SSH control process SSH0: Exchanging versions - SSH-1.99-Cisco-1.25 SSH0: send SSH message: outdata is NULL server version string: SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83) SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation SSH0: complete server key generation, elapsed time = 1920 ms SSH2 0: SSH2\_MSG\_KEXINIT sent SSH2 0: SSH2\_MSG\_KEXINIT received SSH2: kex: client->server aes128-cbc hmac-md5 none SSH2: kex: server->client aes128-cbc hmac-md5 none SSH2 0: expecting SSH2\_MSG\_KEXDH\_INIT SSH2 0: SSH2\_MSG\_KEXDH\_INIT received SSH2 0: signature length 143 SSH2: kex\_derive\_keys complete SSH2 0: newkeys: mode 1 SSH2 0: SSH2\_MSG\_NEWKEYS sent SSH2 0: waiting for SSH2\_MSG\_NEWKEYS SSH2 0: newkeys: mode 0 SSH2 0: SSH2\_MSG\_NEWKEYS receivedSSH(pix): user authen method is 'no AAA', aaa server group ID = 0 SSH(pix): user authen method is 'no AAA', aaa server group ID = 0 SSH2 0: authentication failed for pixSSH(pix): user authen method is 'no AAA', aaa server group ID = 0SSH2 0: authentication failed for pix !--- Authentication for PIX was not successful due to the wrong password.

#### Visualizzazione delle sessioni SSH attive

Per controllare il numero di sessioni SSH connesse e lo stato della connessione al PIX, usare questo comando:

pix#show ssh session

SID	Client	IP	Version	Mode	Encryption	Hmac	State	Username
0	10.1.1.	2	1.99	IN	aes128-cbc	md5	SessionStarted	pix
				OUT	aes128-cbc	md5	SessionStarted	pix

Per visualizzare le sessioni con ASDM, scegliere **Monitoraggio > Proprietà > Accesso dispositivo >** Sessioni Secure Shell.

#### Visualizza chiave RSA pubblica

Per visualizzare la parte pubblica delle chiavi RSA sull'appliance di sicurezza, eseguire questo comando:

```
pix#show crypto key mypubkey rsa
```

Scegliere **Configurazione > Proprietà > Certificato > Coppia di chiavi**, quindi fare clic su **Mostra dettagli** per visualizzare le chiavi RSA con ASDM.

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

## Come rimuovere le chiavi RSA dal PIX

In alcune situazioni, ad esempio quando si aggiorna il software PIX o si modifica la versione SSH nel PIX, può essere necessario rimuovere e ricreare le chiavi RSA. Per rimuovere la coppia di chiavi RSA dal PIX, usare questo comando:

pix(config)#crypto key zeroize rsa

Scegliere **Configurazione > Proprietà > Certificato > Coppia di chiavi**, quindi fare clic su **Elimina** per rimuovere le chiavi RSA da ASDM.

Connessione SSH non riuscita

Messaggio di errore su PIX/ASA:

%PIX ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.

Il messaggio di errore corrispondente sul computer client SSH:

Selected cipher type

Per risolvere il problema, rimuovere e ricreare le chiavi RSA. Per rimuovere la coppia di chiavi RSA dall'appliance ASA, eseguire questo comando:

ASA(config)#crypto key zeroize rsa

Per generare la nuova chiave, usare questo comando:

ASA(config)# crypto key generate rsa modulus 1024

Impossibile accedere ad ASA con SSH

Messaggio di errore:

ssh\_exchange\_identification: read: Connection reset by peer
Per risolvere il problema procedere come segue:

- 1. Ricaricare l'ASA o rimuovere tutta la configurazione SSH e le chiavi RSA.
- 2. Riconfigurare i comandi SSH e rigenerare le chiavi RSA.

Impossibile accedere all'appliance ASA secondaria con SSH

Quando l'ASA è in modalità failover, non è possibile eseguire il protocollo SSH sull'ASA in standby tramite il tunnel VPN. Infatti il traffico di risposta per SSH prende l'interfaccia esterna dell'ASA di standby.

# Informazioni correlate

- <u>Cisco PIX serie 500 Security Appliance</u>
- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- <u>Configurazione delle connessioni SSH Router Cisco e concentratori Cisco</u>
- RFC (Requests for Comments)
- Documentazione e supporto tecnico Cisco Systems