# PIX/ASA 7.x:內部和外部介面上的SSH/Telnet配 置示例

# 目錄

簡介 必要條件 需求 採用元件 相關產品 慣例 設定 網路圖表 SSH配置 使用ASDM 5.x進行配置 <u>使用ASDM 6.x</u>進行配置 Telnet配置 ACS 4.x中的SSH/Telnet支援 驗證 調試SSH 檢視活動SSH會話 檢視公共RSA金鑰 疑難排解 如何從PIX中刪除RSA金鑰 SSH連線失敗 無法使用SSH訪問ASA 無法使用SSH訪問輔助ASA 相關資訊

# <u> 簡介</u>

本檔案將提供思科系列安全裝置7.x版及更新版本的內部和外部介面上的安全殼層(SSH)組態範例。 使用命令列遠端配置系列安全裝置涉及使用Telnet或SSH。由於Telnet通訊以明文形式傳送(包括 密碼),因此強烈建議使用SSH。SSH流量在通道中加密,因此有助於防止密碼和其他配置命令被 攔截。

出於管理目的,安全裝置允許與安全裝置建立SSH連線。如果可用,安全裝置允許每個安全情景最 多同時建立5個SSH連線,並且所有合併的情景最多允許100個連線。

在此配置示例中,PIX安全裝置被認為是SSH伺服器。從SSH客戶端(10.1.1.2/24和172.16.1.1/16)到 SSH伺服器的流量會進行加密。安全裝置支援SSH版本1和2中提供的SSH遠端外殼功能,並支援資 料加密標準(DES)和3DES密碼。SSH版本1和2不同,無法互操作。



# <u>需求</u>

本文件沒有特定需求。

### <u>採用元件</u>

本文檔中的資訊基於Cisco PIX防火牆軟體版本7.1和8.0。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

注意: PIX/ASA 7.x版及更高版本支援SSHv2,而7.x之前的版本不支援SSHv2。

### <u>相關產品</u>

此配置還可以與軟體版本7.x及更高版本的Cisco ASA 5500系列安全裝置配合使用。

### <u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

# <u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

注意:每個配置步驟都提供了使用命令列或自適應安全裝置管理器(ASDM)所需的資訊。

註:使用<u>Command Lookup Tool</u>(僅限<u>註冊</u>客戶)可獲取本節中使用的命令的詳細資訊。

### <u>網路圖表</u>

本檔案會使用以下網路設定:



# <u>SSH配置</u>

本檔案會使用以下設定:

- <u>對安全裝置的SSH訪問</u>
- 如何使用SSH客戶端
- <u>PIX配置</u>

對安全裝置的SSH訪問

完成以下步驟,配置對安全裝置的SSH訪問:

 SSH會話始終需要使用者名稱和密碼進行身份驗證。有兩種方法可以滿足此要求。配置使用者 名稱和密碼並使用AAA:語法:

pix(config)#username username password password pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server\_group [LOCAL]}

**注意:**如果使用TACACS+或RADIUS伺服器組進行身份驗證,則可以配置安全裝置,在 AAA伺服器不可用時將本地資料庫用作回退方法。指定伺服器組名稱,然後指定 LOCAL(LOCAL區分大小寫)。 我們建議您在本地資料庫中使用與AAA伺服器相同的使用者 名稱和密碼,因為安全裝置提示符不會指示使用的是哪種方法。**注意:**示例: pix(config)#aaa authentication ssh console TACACS+ LOCAL

**注意:**也可以使用本地資料庫作為無回退的主要身份驗證方法。若要執行此操作,請單獨輸入 LOCAL。範例:

pix(config)#aaa authentication ssh console LOCAL

**或**使用預設使用者名稱**pix**和預設Telnet密碼**cisco**。您可以使用以下命令更改Telnet密碼: pix(config)#**passwd** password

**注意:**在這種情況下,也可以使用**password**命令。兩個命令執行相同的操作。 2. 為PIX防火牆生成RSA金鑰對,這是SSH所必需的: pix(config)#**crypto key generate rsa modulus** *modulus\_size* 

**註**:modulus\_size(以位為單位)可以是512、768、1024或2048。指定的金鑰係數大小越大 ,生成RSA金鑰對所需的時間就越長。建議使用值1024。**注意:**用於生成RSA密<u>鑰對的命令</u> <u>對於</u>低於7.x的PIX軟體版本是不同的。在早期版本中,必須先設定域名,然後才能建立金鑰。 **注意:**在多情景模式下,必須為每個情景生成RSA金鑰。此外,系統情景模式中不支援加密命 令。

 指定允許連線到安全裝置的主機。此命令指定允許使用SSH連線的主機的源地址、網路掩碼和 介面。可以多次輸入多個主機、網路或介面。在此範例中,允許一台主機位於內部且一台主機 位於外部。

pix(config)#ssh 172.16.1.1 255.255.255.255 inside pix(config)#ssh 10.1.1.2 255.255.255.255 outside

4. 可選:預設情況下,安全裝置允許SSH版本1和版本2。輸入以下命令可將連線限製為特定版本
 :
 pix(config)# ssh version

**注意**:version\_number可以是1或2。

5. **可選:**預設情況下,SSH會話在五分鐘不活動後關閉。此超時可配置為持續1到60分鐘。 pix(config)#**ssh timeout** *minutes*  開啟SSH會話時提供PIX 500系列安全裝置的使用者名稱和登入密碼。啟動SSH會話時,在安全裝 置控制檯上顯示dot(.),然後顯示SSH使用者身份驗證提示:

hostname(config)# .

點的顯示不會影響SSH的功能。當生成伺服器金鑰或在SSH金鑰交換期間使用私鑰解密消息時,該 點出現在控制檯上,然後進行使用者身份驗證。這些任務可能需要兩分鐘或更長時間。圓點是進度 指示符,用於驗證安全裝置是否處於忙碌狀態且未掛起。

SSH版本1.x和2是完全不同的協定,並且不相容。下載相容的客戶端。有關詳細資訊,請參閱<u>高級</u> <u>配置的獲取SSH客戶端</u>部分。

#### <u>PIX配置</u>

本檔案會使用以下設定:

#### PIX配置

```
PIX Version 7.1(1)
1
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
Ţ
interface Ethernet0
nameif outside
security-level 0
ip address 192.168.200.1 255.255.255.0
1
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, !-
-- before the security appliance disconnects the
session. ssh timeout 60
console timeout 0
1
class-map inspection_default
match default-inspection-traffic
!
policy-map global_policy
class inspection_default
 inspect dns maximum-length 512
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
ļ
service-policy global_policy global
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7
: end
```

**註:要使用SSH訪問ASA/PIX的管理介面,請發出以下命令**:ssh 172.16.16.160 255.255.255.255

# 使用ASDM 5.x進行配置

完成以下步驟,以便使用ASDM為SSH配置裝置:

 選擇Configuration > Properties > Device Administration > User Accounts,以便使用ASDM新 增使用者。

ổ Home	Configuration Monitoring	Back Forward	Q Q Search Refresh	調 🦓 Save Help		CISCO SYSTEMS
Interfaces Security Policy NAT	Configuration > Properties > Device Administratio	Ce Administration > Use Ce & Counts User Accounts Create entries in the user account privileg User Name enable_15	er Accounts PIX local user databa es to be enforced. To Privilege (Level) NA (15)	se. Command author enable command au VPN Group Policy NG	ization must be enable horization, go to <u>Autho</u> VPN Group Lock	d in order for the lization.
VPN Routing Global Objects Properties	Boart Image/Con     Short Image/Con     Clock     Console     Pevice     Short P Mode     Management Ac     NTP     Password     Secure Copy     SMTP     SSMP	ciscouser	NA (2)	DiftGrpPolicy	Inherit Group Po	Edit Delete
	HETP Server     Jer Accounts     DHCP Services     JEDNS Client     Fallover		Apply	NA (2)	t	08 6:16:28 PM UTC

2. 選擇**Configuration > Properties > Device Access > AAA Access > Authentication**,以便使用 ASDM為SSH設定AAA身份驗證。

💰 Home 🛛	Configuration Monitoring	Back Forward Search Refresh Save Help
Interfaces Security Policy NAT	Configuration > Properties >	Device Access > AAA Access > Authentication         Image: Image
VPN	PHTTPS/ASDM     PAGE     PAGE	Require authentication for the following types of connections         HTTP/ASDM Server Group:       LOCAL         Serial       Server Group:         LOCAL       Use LOCAL when server group fails         SSH       Server Group:         LOCAL       Use LOCAL when server group fails
Properties	Copying     Priority Queue     SSL     SUNRPC Server     STCP Options     Timeouts     WRL Filtering	Teinet Server Oroup: LOCAL To Use LOCAL when server proup fails Apply Reset

3. 選擇Configuration > Properties > Device Administration > Password,以便使用ASDM更改

Telnet密碼。

C Home	Configuration Montering	Sack Forward Search Refresh Save Help	CO SYSTEMS
Hertaces Security Policy NAT Security Policy NAT Security NAT Security Routing Clobal Objects Properties	Configuration > Properties > D		
Device configur	ation loaded successfully.	ciscouser NA (2) 🙀 6/23/06 6:3	0:38 PM UTC

4. 選擇Configuration > Properties > Certificate > Key Pair,按一下Add並使用顯示的預設選項生 成與ASDM相同的RSA金鑰。

C Home	Configuration Monitoring	Back Forward Sea	rch Refresh	🗐 🢡 Save Halp	CISCO SYSTEMS
Herfaces Security Policy NAT Security Policy NAT Security NAT Security Properties	Configuration > Properties > Or Configuration > Properties > Or Configuration > Properties > Or Configuration > Configuration Configuration > Configuration > Configuration Configuration > Configuration >	rtificate = Key Pair Key Pair Configure the key pairs to Note: Operations on this Key Pair Name <default-rsa-k.< td=""><td>o be used in certifical s screen are applied i Type U RSA Genera</td><td>ites. Immediately upon completio Jsage Modulus Size al Purpose 102</td><td>Add Add Show Details Delete Refresh</td></default-rsa-k.<>	o be used in certifical s screen are applied i Type U RSA Genera	ites. Immediately upon completio Jsage Modulus Size al Purpose 102	Add Add Show Details Delete Refresh
Device configur	ation loaded successfully.		ciscouser N	A (2) 🛛 🛃 🙆	🔂 5/23/08 6:34:58 PM UTC

5. 選擇**Configuration > Properties > Device Access > Secure Shell**,以便使用ASDM指定允許使 用SSH連線的主機,並指定版本和超時選項。

Iome	Configuration Monitoring	Back Forward Sea	rch Refresh Save	<b>?</b> Нар	CISCO SYSTEMS
Hierfaces Hierfaces Security Policy NAT NAT VPN Security NAT Clobel Objects Properties	Configuration > Properties > Startup Wizard AAA Setup AAA AA Setur AAA AAC Setup AAA AAA Setup AAA AAA Setup AAA AAA AAC Setup AAA AAA AAA AAC Setup AAA AAA AAA AAC Setup AAA AAA AAA AAC Setup AAA AAA AAA AAA AAA AAC Setup AAA AAA AAAAA AAA AAA AAA AAA AAAA AAA AAA	Device Access - Secure Shell     Secure Shell     Allowed SSH Version(s):     Specify the addresses of a using Secure Shell (SSH)     Interface     inside     outside	IP Address 172.16.1.1 10.1.1.2	eout 60 minute e allowed to access the PIX Mask 255 255 255 255 255 255 255 255	Add Edit Delete
	OTimeouts 생 URL Filtering		Apply	Reset	
, Device configur	ation loaded successfully.		ciscouser NA (2)	i 🎯 🚱 🖯	5/23/06 6:37:58 PM UTC

6. 按一下「File > Save Running Configuration to Flash」以儲存組態。

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 I	Packet Tracer	Q Refre	
Save Running Configuration to Flash				
Save Running Configuration to TFTP Server       Infiguration         Save Running Configuration to Standby Unit       Infiguration         Save Internal Log Buffer to Flash       Infigure boot images from an end the boot system. Only one The first image in the list.			n externa TFTP bo	
Clear Internal Log Buffer	loot Order			
Exit Exit VPN Exit CLI Prompt Clock	1	disk0:/pix722	l.bin	

# 使用ASDM 6.x進行配置

請完成以下步驟:

1. 選擇**Configuration > Device Management > Users/AAA > User Accounts**以新增使用ASDM的 使用者。

Home 🖧 Configuration 🔯 Monitori	ng 🔚 Save 📿 Re	efresh 🕜 Back 🕥 Forwa	rd 🙄 Help			cisco
Device Management 🗗 🕂 🛪	Configuration > De	vice Management > Users/	AAA > User Accounts			C
Anagement Access     System Image/Configuration     Anagement Access     System Image/Configuration     Anagement Access     High Availability     Configuration     System Image/Configuration     System Image/Configuration     System Image/Configuration     System Image/Configuration	Create entries in th Command authoriz AAA authentication	he ASA local user database. ation must be enabled in order f n console commands must be en	or the user account privileges abled in order for certain acce	to be enforced. To enable (	command authorization, go to ed. To enable AAA authentica	Authorization.
Authentication Prompt	go to <u>eta interna</u>			,		
- Do Dynamic Access Policies	Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add
User Accounts	enable_15	15	Ful	- Inherit Group Policy	Inherit Group Policy N/A	Edit
Gertificate Management     E-IM DHCP						Delete
E E DNS						
E-B Advanced						
💑 Device Setup						
Freed						
CR Dometer Lorenze 1041						
Tellora Access Aut						
Ste-to-Site VPN						
Device Management						
				1		
			App'y	Reset		

2. 選擇Configuration > Device Management > Users/AAA > AAA Access > Authentication,以

便為使用ASDM的SSH設定AAA身份驗證。



3. 選擇**Configuration > Device Setup > Device Name/Password**,以便使用ASDM更改Telnet密 碼。

3	) Home 🗞 Configuration 🔯 Monitorin	g 🔚 Save 🔇 Refres	h 🔇 Back: 🜔 Forward	🖓 Help			
	Device Setup _ 0 ×	Configuration > Device	Setup > Device Name/Pas	sword			
elle		Hostname and Domain Na	ne				
Devk	E-+++ Routing	Hostname:	ciscoasa				
	Device Name/Password     System Time	Domain Name:	default.domain.invalid				
		Enable Password					
		Change the privileg	ed mode password.				
		Old Password:					
		New Pessword:					
		Confirm New Password:					
		Teinet Password					
		Change the passwo	rd to access the console of the s	ecurity appliance.			
		Old Password:					
		New Password:					
		Confirm New Password:					
	Pevice Setup						
	Frewal						
	Remote Access VPN						
	Sibe-to-Site VPN						
	Device Management						
	*			Apply	Reset		
				<admin< th=""><th>&gt; 15</th><th>😡 🎰</th><th>6</th></admin<>	> 15	😡 🎰	6

4. 選擇Configuration > Device Management > Certificate Management > Identity Certificates,按一下Add,然後使用顯示的預設選項生成與ASDM相同的RSA金鑰。

- 🕄 SMP 🕺 🗌	Issued To	Issued By	Expiry	Date	Usace	Add
- Management Access Ruk						Show Date
- 🚱 Activation Key					al	3104050
- 🛃 Auto Update 🔛	Add Identity Certificate			×	1	Dicide
High Availability	Import the identity certified	icate from a file:				Export
Logging	Decryption Passphrase:		_			Instal
gi Users/AAA Pa Castificate Management	Eiste Insect From	, 				
- 2 CA Certificates	His to Import From:		STRAGE			
- Realidentity Certificates	Add a new identity certif	sate:				
P DHCP	Key Pair:	<pre>@efault-RSA-Key&gt;</pre>	<ul> <li>Show</li> </ul>	New		
P DHCP Server	Certificate Subject DV:	CN-riscoasa	Select			
DNS		In the second				
Advanced	Generate self-signed	certificate				
- 🐺 ARP Static Table	🔲 Act as local certif	kate authority and issue dynam	c certificates to TLS-	Рлаху		
HTTP Redirect					given interface. You can go	to <u>SSL Settings</u>
- An SSL Certificates				Advanced		
Davies Esh a	Add Certifi	rate Cancel	Help			
Device serely						
Firewall					_	
Remote Access VPN						
Site-to-Site VPN						
Paulas Management						

5. 在Add a new Identity certificate下,按一下New,以便新增預設金鑰對(如果不存在)。然後 ,按一下Generate Now。

Home 🗞 Configuration 🛜 Monitor	ng 🔚 Save 🔇 Refresh 🔇 I	Bade 🔘 Forward 🦻 Help			CISCO
Device Management and X	Configuration > Device Manage	ement > Certificate Manageme	nt > Identity Certificates		
B B System Image/Configuration	Issued To	Issued By	Expiry Date	Usage	Add
E Logging					Show Details
- AAA Server Groups	Add Identity Certificate		x	1	Delete
- Authentication Prompt - L AAA Access	C Import the identity certifi	icate from a file:			Exact
<ul> <li>Dynamic Access Policies</li> <li>Dynamic Access Policies</li> </ul>	Derrontion Passobrase:				Testal
E- E Certificate Management	Fie to Import From:		Browse		412001
- 2 CA Certificates	G Add a new identity codd	li Irohai			
E CHCP	Kan Brite	- Default DEA Kings	One Nor		
E- Advanced	Ney Pair:	cosanceoseraito	5108 Nex		
	Cent 🕵 Add Key Pair		×		
	Name: 🛈 🗓 🤉	e default key pair name			
	C 51	ter new key pair name:			
	Size: 1024	*	L.	given interrace, rou can g	jo to <u>SSL Settings</u> to
	Usage: 🖝 Ge	neral purpose 🛛 🔿 Specia	s 🗌		
Service Setup					
Frewal	Generat	e Now Cancel	Help	]	
Remote Access VPN					
Ste-to-Site VPN					
Device Management					
*		Ap	ply Reset		

6. 選擇Configuration > Device Management > Management Access > Command Line(CLI)> Secure Shell(SSH),以便使用ASDM指定允許使用SSH連線的主機,並指定版本和超時選項

Home 🗞 Configure	stion 🛐 Monitoring 🔓	🚽 Save 🔇 Refresh 🔇 Back (	🕽 Farward 🦻 Help		CISCO
Device Manageme	nt an a × Con	figuration > Device Management	> Management Access > Command Lin	ne (CLI) > Secure Shell (SSH)	
Management / ASDM/HTT B S Command Command	Access A IPS A Une (CLI) r S	llowed 55H Version(s): 1 & 2	Timeout: 5 minutes	g Secure Shell (SSH).	
- 📴 CLI Pr	ompt	Interface	IP Address	Mask	Add
- 🍓 Conso	le Timeout	inside	10.77.241.142	255.255.255.255	
- The second	shel (SSH)	outside	192.168.200.1	255.255.255.255	Edit
Ele Acces					Delete
- CMP					
- 🛞 Nanageme	ant Interface				
- SNMP					
El OR Surten Image	Int Access Rule				
FF W High Availabilit	y				
E- 🖸 Logging					
E- 🐼 Users/AAA					
- AAA Serve	er Groups				
- Authentics	stion Prompt				
- De Dynamic A	ccess Policies				
- 🚮 User Acco	unts				
H- 🖬 Certricate Ma	nagement 😜				
1					
Device Setup					
Frewall					
Remote Access	VPN				
Ste-to-Site VPN					
Device Manager	ment				
	2		Apply Re	set	

7. 按一下視窗頂部的Save以儲存組態。

File View Tools Wizards Window H	lelp
Home 🎇 Configuration 🔯 Monitor	ing Save 🐼 Refresh 🔇 Back 🕥 Forward 🤗 Help
Device Management ⊡ ₽ ×	Config Save Running Configuration to Flash Management Access >
ASDM/HTTPS	Allowed SSH Version(s): 1 & 2 Timeout: 5

8. 當系統提示將組態儲存到快閃記憶體時,選擇Apply以儲存組態。

# <u>Telnet配置</u>

若要向控制檯新增Telnet訪問並設定空閒超時,請在全域性配置模式下發出**telnet**命令。預設情況下 ,安全裝置會關閉閒置5分鐘的Telnet會話。若要從先前設定的IP位址中移除Telnet存取許可權,請 使用此命令的*no*形式。

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}}

telnet命令用於指定哪些主機可以通過Telnet訪問安全裝置控制檯。

**註:您**可以在所有介面上啟用Telnet到安全裝置。但是,安全裝置強制所有到外部介面的Telnet流量 都受IPsec保護。要啟用到外部介面的Telnet會話,請在外部介面上配置IPsec以包括安全裝置生成 的IP流量,並在外部介面上啟用Telnet。

**注意:**一般來說,如果任何介面的安全級別為0或低於任何其他介面,則PIX/ASA不允許Telnet到該 介面。

**注意**:建議不要通過Telnet會話訪問安全裝置。身份驗證憑證資訊(如密碼)以明文傳送。Telnet伺 服器和客戶端通訊僅以明文進行。Cisco建議使用SSH實現更安全的資料通訊。

如果輸入IP地址,還必須輸入網路掩碼。沒有預設網路掩碼。請勿使用內部網路的子網掩碼。網路 掩碼只是IP地址的位掩碼。為了限制對單個IP地址的訪問,請在每個八位元中使用255;例如 255.255.255.255。

如果IPsec運行,則可以指定不安全的介面名稱,通常為外部介面。您至少可以配置crypto map命令 ,以便使用telnet命令指定介面名稱。

發出**password**命令以設定對主控台的Telnet存取密碼。預設值為cisco。發出**who**命令以檢視當前訪 問安全裝置控制檯的IP地址。發出**kill**命令以終止活動的Telnet控制檯會話。

要啟用到內部介面的Telnet會話,請檢視以下示例:

#### 範例 1

此範例僅允許主機10.1.1.1透過Telnet存取安全裝置主控台:

#### 範例 2

此範例僅允許網路10.0.0.0/8透過Telnet存取安全裝置主控台:

pix(config)#telnet 10.0.0.0 255.0.0.0 inside

#### 範例 3

此範例允許所有網路透過Telnet存取安全裝置主控台:

pix(config)#telnet 0.0.0.0 0.0.0.0 inside

如果使用帶有console關鍵字的**aaa**命令,則必須使用身份驗證伺服器對Telnet控制檯訪問進行身份 驗證。

**注意:**如果您已配置aaa**命令以要求安全裝置Telnet控制檯訪問進行身份驗證,並且控制檯登入請求** 超時,則可以從串列控制檯獲得對安全裝置的訪問許可權。為此,請輸入安全裝置使用者名稱和使 用enable password命令設定的密碼。

發出**telnet timeout**命令,以設定控制檯Telnet會話在被安全裝置註銷之前可以空閒的最長時間。不 能將no telnet 命令與telnet timeout 命令一起使用。

此示例說明如何更改最大會話空閒持續時間:

hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes

# <u>ACS 4.x中的SSH/Telnet支援</u>

如果您檢視RADIUS功能,則可以將RADIUS用於SSH功能。

當嘗試通過Telnet、SSH、HTTP或串列控制檯連線訪問安全裝置且流量與身份驗證語句匹配時,安 全裝置會請求使用者名稱和密碼。然後向RADIUS(ACS)伺服器傳送這些憑證,並根據伺服器的響應 授予或拒絕CLI訪問。

有關詳細資訊,請參閱配置AAA伺服器和本地資料庫的AAA伺服器和本地資料庫支援部分。

例如,ASA安全裝置7.0需要一個IP地址,安全裝置可從該地址接受連線,例如:

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

有關詳細資訊,請參閱<u>配置AAA伺服器和本地資料庫</u>的<u>允許SSH訪問</u>部分。

請參閱<u>PIX/ASA:使用TACACS+和RADIUS伺服器進行網路訪問的直通代理配置示例</u>,瞭解有關如何 使用ACS身份驗證配置PIX的SSH/Telnet訪問的詳細資訊。 使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**指令輸出的分析 。

# <u>調試SSH</u>

發出debug ssh命令以開啟SSH調試。

pix(config)#**debug ssh** SSH debugging on 此輸出顯示,從主機10.1.1.2(外部到PIX)到「pix」的身份驗證請求成功:

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

如果使用者提供的使用者名稱錯誤,例如,「pix1」而不是「pix」,則PIX防火牆將拒絕身份驗證 。此調試輸出顯示失敗的身份驗證:

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.
同樣,如果使用者提供錯誤的密碼,則此偵錯輸出會顯示失敗的驗證。
```

```
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 = 0
SSH2 0: authentication failed for pix
!--- Authentication for PIX was not successful due to the wrong password.
檢視活動SSH會話
```

發出此命令,檢查已連線的SSH會話數以及到PIX的連線狀態:

pix#show ssh session

SID	Client I	P V	Version	Mode	Encryption	Hmac	State	Username
0	10.1.1.2	1	1.99	IN	aes128-cbc	md5	SessionStarted	pix
				OUT	aes128-cbc	md5	SessionStarted	pix

選擇Monitoring > Properties > Device Access > Secure Shell Sessions以檢視具有ASDM的會話。

# <u>檢視公共RSA金鑰</u>

發出此命令,以檢視安全裝置上RSA金鑰的公共部分:

#### pix#show crypto key mypubkey rsa

Key pair was generated at: 19:36:28 UTC May 19 2006
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f300d06092a864886f70d010101050003818d0030818902818100c172f495f66c342c2ced37aa3442d812158c93131480dd967985ab1d7b92d95290f6958e9b5b0dd88c04396169184cd8fb951c19023347d6b3f93999ac2814950f442269b67328f64916b182e1534107590da2390fbefd387588887319196cde61aef1165c4bab03d081d5ddaf15ccc9ddb204c2b451e0f19ce0f3485b1d698b0203010001

選擇**Configuration > Properties > Certificate > Key Pair**,然後按一下**Show Details**以檢視RSA金鑰 與ASDM。

# 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

# 如何從PIX中刪除RSA金鑰

某些情況下,例如升級PIX軟體或更改PIX中的SSH版本時,可能需要刪除並重新建立RSA金鑰。發 出此命令,以便從PIX中刪除RSA金鑰對:

pix(config)#crypto key zeroize rsa

選擇**Configuration > Properties > Certificate > Key Pair**,然後按一下**Delete**以刪除RSA金鑰和 ASDM。

### <u>SSH連線失敗</u>

PIX/ASA上的錯誤消息:

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

SSH客戶端電腦上的相應錯誤消息:

為了解決此問題,請刪除並重新建立RSA金鑰。發出此命令,以便從ASA中刪除RSA金鑰對:

ASA(config)#crypto key zeroize rsa

核發此命令,以便產生新金鑰:

ASA(config)# crypto key generate rsa modulus 1024

# <u>無法使用SSH訪問ASA</u>

錯誤消息:

ssh\_exchange\_identification: read: Connection reset by peer 為了解決此問題,請完成以下步驟:

- 1. 重新載入ASA或刪除所有與SSH相關的配置和RSA金鑰。
- 2. 重新配置SSH命令並重新生成RSA金鑰。

# <u>無法使用SSH訪問輔助ASA</u>

當ASA處於故障切換模式時,無法通過VPN隧道通過SSH連線到備用ASA。這是因為SSH的應答流 量會佔用備用ASA的外部介面。

# 相關資訊

- <u>Cisco PIX 500系列安全裝置</u>
- Cisco ASA 5500系列調適型安全裝置
- <u>Cisco PIX防火牆軟體</u>
- Cisco Secure PIX防火牆命令參考
- <u>配置SSH連線 思科路由器和思科集中器</u>
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems