PIX/ASA 7.x:在内部和外部接口的SSH/Telnet配 置示例

目录

简介 先决条件 要求 使用的组件 相关产品 规则 配置 网络图 SSH 配置 用 ASDM 5.x 进行配置 用 ASDM 6.x 进行配置 Telnet 配置 ACS 4.x 中的 SSH/Telnet 支持 验证 调试 SSH 查看活动的 SSH 会话 查看 RSA 公钥 故障排除 如何从 PIX 删除 RSA 密钥 SSH 连接失败 无法通过 SSH 访问 ASA 使用SSH,无法访问第二ASA 相关信息

<u>简介</u>

本文档对于在 Cisco 系列安全设备 7.x 版及更高版本的内部和外部接口上配置 Secure Shell (SSH) 提供了一个示例。用命令行远程配置系列安全设备的过程中使用 Telnet 或 SSH。由于 Telnet 通信 是以明文发送的(其中包括口令),因此强烈建议使用 SSH。SSH 流量在某个隧道中进行加密 ,并因此帮助保护口令和其他配置命令免遭拦截。

安全设备允许通过 SSH 连接到安全设备进行管理。安全设备对于每个<u>安全上下文</u>最多允许五个并 发的 SSH 连接(如果有),而对于所有上下文合在一起全局最多支持 100 个连接。

在本配置示例中,将 PIX 安全设备视为 SSH 服务器。从 SSH 客户端(10.1.1.2/24 和 172.16.1.1/16)到 SSH 服务器的流量受到加密。安全设备支持 SSH 版本 1 和 2 中提供的 SSH 远 程 shell 功能,并支持数据加密标准 (DES) 和 3DES 加密。SSH 版本 1 和 2 存在差异,不可互操

作。

<u>先决条件</u>

<u>要求</u>

本文档没有任何特定的要求。

<u>使用的组件</u>

本文档中的信息基于 Cisco PIX 防火墙软件 7.1 版和 8.0 版。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

注意: PIX/ASA版本7.x和以上支持和版本不支持SSHv2前对7.x。

<u>相关产品</u>

此配置可能也与有软件版本的7.x Cisco ASA 5500系列安全工具一起使用和以后。

<u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则</u>。

<u>配置</u>

本部分提供有关如何配置本文档所述功能的信息。

注意: 对于每个配置步骤都提供使用命令行或自适应安全设备管理器 (ASDM) 所需的信息。

注意:使用<u>命令查找工具</u>(<u>仅限注册用户</u>)可获取有关本部分所使用命令的详细信息。

<u>网络图</u>





SSH 配置

本文档使用以下配置:

- 通过 SSH 访问安全设备
- <u>如何使用 SSH 客户端</u>
- <u>PIX 配置</u>

通过 SSH 访问安全设备

完成以下这些步骤,以便配置对安全设备的 SSH 访问:

- 1. SSH 会话始终要求输入用户名和口令进行身份验证。有二种方式可满足此要求。配置用户名和口令,并使用 AAA:语法:pix(config)#username username password password password pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]} 注意:如果使用 TACACS+或 RADIUS 服务器组进行身份验证,则可以将安全设备配置为在 AAA 服务器不可用时使用本地数据库作为备用方法。指定服务器组名称,然后指定LOCAL(LOCAL区分大小写)。建议在本地数据库中使用的用户名和口令与 AAA 服务器相同,因为安全设备提示符并不指明使用何种方法。注意:示例:pix(config)#aaa authentication ssh console TACACS+ LOCAL 注意:还可以使用本地数据库作为身份验证的主要方法,而不设置备用方法。为此,请仅输入LOCAL。示例:pix(config)#aaa authentication ssh console LOCAL 或者使用默认用户名 pix 和默认 Telnet 口令 cisco。可以用下面这个命令更改 Telnet 口令:pix(config)#passwd password 注意:这种情况下也可以使用 password 命令。这两个命令作用相同。
- 2.为 PIX 防火墙生成 RSA 密钥对,对于 SSH 而言这是必要步骤:pix(config)#crypto key generate rsa modulus modulus_size 注意: modulus_size(以位为单位)可以是 512、768、 1024 或 2048。指定的密钥模数大小越大,生成 RSA 密钥对所需的时间就越长。建议取 1024 作为此值。注意: 7.x 之前的 PIX 软件版本中用于生成 RSA 密钥对</u>的命令不同。在早期版本 中,必须先设置域名,然后才能创建密钥。注意: 在多上下文模式下,必须为每个上下文都 生成 RSA 密钥。此外,系统上下文模式下不支持 crypto 命令。
- 3. 指定允许连接到安全设备的主机。此命令指定允许以 SSH 进行连接的主机的源地址、网络掩码和接口。可以多次输入此命令,从而指定多个主机、网络或接口。在本示例中,允许内部一台主机和外部一台主机。pix(config)#ssh 172.16.1.1 255.255.255 inside pix(config)#ssh 10.1.1.2 255.255.255 outside
- 4. 可选:默认情况下,安全设备同时允许 SSH 版本 1 和版本 2。输入此命令,以便仅允许某个 特定版本的连接:pix(config)# ssh version <version_number> 注意: version_number 可以是 1 或 2。
- 5. **可选:**默认情况下,非活动状态持续五分钟后即关闭 SSH 会话。可以配置此超时,以使此过 程持续 1 至 60 分钟。pix(config)#ssh timeout minutes

如何使用 SSH 客户端

打开 SSH 会话时,请提供 PIX 500 系列安全设备的用户名和登录口令。启动 SSH 会话时,安全设 备控制台上显示一个点 (.),然后再显示 SSH 用户身份验证提示符:

hostname(config)# .

显示这个点不会影响 SSH 的功能。在 SSH 密钥交换过程中,当生成服务器密钥或用私钥将消息解 密时控制台即显示这个点,然后再进行用户身份验证。完成这些任务可能需要两分钟或更长时间。 此点是一种进度指示器,可确认安全设备繁忙且未挂起。

SSH 版本 1.x 和 2 是完全不同的协议,因此相互不兼容。请下载兼容的客户端。有关详细信息,请

<u>PIX 配置</u>

本文档使用以下配置:

PIX 配置

```
PIX Version 7.1(1)
1
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
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, !--- before the security
appliance disconnects the session. ssh timeout 60
console timeout 0 ! 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 ! service-policy global_policy global Cryptochecksum:a6b05fd04f9fbd0a39flca7328de91f7 : end

注意: 要使用 SSH 访问 ASA/PIX 的管理接口,请发出此命令: ssh 172.16.16.160 255.255.255.255 Management

<u>用 ASDM 5.x 进行配置</u>

完成以下这些步骤,以便使用 ASDM 配置设备以支持 SSH:

1. 选择 Configuration > Properties > Device Administration > User Accounts,以便用 ASDM 添 加用户。

Iome	Configuration Monitoring	Back Forward	Q Q Search Refresh	🗐 🦓 Save Help		Cisco Systems
Herfaces Security Policy	Configuration > Properties > De	vice Administration > U Control (Control (Contro) (Contro) (Contro) (Contro) (Contro) (Contr	Ser Accounts PIX local user databa jes to be enforced. To	se. Command author enable command aut	tzation must be enabled thortzation, go to <u>Authon</u> 2	In order for the
VFN VFN Routing Global Objects Properties	Clock Clock Clock Clock Cl	enable_15 ciscouser	NA (15) NA (2)	N/A DiftGrpPolicy	N/A Inherit Group Po	Edit Delete
	FTP Server Joer Accounts DHCP Services DNS Client Fallover		Apply	NA (2)	1 B (@) (#) 572300	8-16-28 PM UTC

2. 选择 Configuration > Properties > Device Access > AAA Access > Authentication,以便用 ASDM 为 SSH 设置 AAA 身份验证。

Canal Cana Cana	Configuration Montoring	Back Forward Search Refresh Save Help
Interfaces	Configuration - Properties - De	Avice Access > AAA Access > Authentication A Itel S III (S) Authentication/Authorization/Accounting Authentication Authorization Accounting
	Er MARP → Auto Update ⊕ E Certificale ⊖ Device Access → AAA Access → AAA Access	Enable authentication for administrator access to the PIX . Require authentication to allow use of privileged mode commands Example: Server Group: LOCAL C Use LOCAL when server group fails
VPN	Becure Shell Becure Shell Becure Shell Becure Administration BOPCE Administration DHCP Services BONS Client	Require authentication for the following types of connections
Global Objects	Failover Fragment History Metrics In Audit Logging	Seriel Server Group: LOCAL Use LOCAL when server group fails Server Group: LOCAL Use LOCAL when server group fails Server Group: LOCAL Use LOCAL when server group fails Server Group: LOCAL Server Group: LOCAL
	Priority Queue SSL SUNRPC Server TCP Options Timeouts WIRL Sitesian	
Device configura	tion loaded successfully.	Apply Reset

3. 选择 Configuration > Properties > Device Administration > Password,以便用 ASDM 更改 Telnet 口令。

Itome	Configuration Monitorin	g Back	Forward	Q Search	Q Refresh	П Save	орн Најр	Cisco Systems
Herfaces Herfaces Security Policy NAT Security Policy Properties	Configuration > Fropert Configuration > Fropert Configuration > Fropert Configuration > Fropert AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup Certificate Certificate Certificate Certificate Certificate Console	Con	dministration = word ange the privile Enable Passwo Change the On Ne Co Telnet Passwo Change the Oh Ne Co	Password eged mode ord prMleged 1 Passwor w Password d Password d Password w Password	and Telnet p mode password: c: rd: Password: d: rd: Password: 	asswords.	also the pass e. Reset	sword to log into ASDM.
Device configur	ration loaded successfully.				ciscouser	NA (2)		📙 🔂 5/23/06 6:30:38 PM UTC

4. 选择 Configuration > Properties > Certificate > Key Pair,单击 Add 并使用给出的默认选项

以便用 ASDM 生成相同的 RSA 密钥。



5. 选择 Configuration > Properties > Device Access > Secure Shell,以便用 ASDM 指定允许通 过 SSH 进行连接的主机,并指定版本和超时选项。

S Home	Configuration Montering	Sack Forward Search Refresh Save Help	CISCO SYSTEMS
Hierfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Properties	Configuration > Properties > D	Mode Access - Secure Shell Secure Shell Allowed SSH Version(s): Image: Timeout Specify the addresses of all hosts/networks which are allowed to access the PIX using Secure Shell (SSH). Interface IP Address Mask Inside 172.18.1.1 255.255.255.255 outside 10.1.1.2 255.255.255.255	Add Edit Delete
Device configura	ation loaded successfully.	ciscouser NA (2) 😹 🐼 🔂 5	23/06 6:37:58 PM UTC

6. 单击 File > Save Running Configuration to Flash,以便保存配置。

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	ward Packet Tracer Refre			
Show Running Configuration in New Window	istration > Doct Image/Configure			
Save Running Configuration to Flash	/Configuration /Configuration nfigure boot images from an externa the boot system. Only one TFTP bo first image in the list.			
Save Running Configuration to TFTP Server Save Running Configuration to Standby Unit Save Internal Log Buffer to Flash				
Print				
Clear ASDM Cache	loct Order			
Clear Internal Log Buffer	1 disk0:/pix722.bin			
Exit Sign Darmer Boot Image/Config VPN CLI Prompt Clock				

<u>用 ASDM 6.x 进行配置</u>

完成这些步骤:

1. 选择 Configuration > Device Management > Users/AAA > User Accounts,以便用 ASDM 添 加用户。

3	Home 🖧 Configuration 🛐 Monitor	ing 🔚 Save 🔇 Re	fresh 🕜 Back 🔘 Forwa	rd 🦻 Help			cisco
Device Ust	Device Management C + × Management Access System Image/Configuration High Availability Logoing Solution AAA Server Groups	Configuration > Dev Create entries in th Command authoriza AAA authentication go to <u>Authentication</u>	vice Management > Users/ re ASA local user database. ation must be enabled in order f r console commands must be en	AAA > User Accounts or the user account privileges abled in order for certain acce	to be enforced. To enable a	command authorization, go to d. To enable AAA authentica	Authorization.
	- 20 Authentication Prompt	University	Estudio en Louvel (Estalo)	Arrest Destations	1000 Course Dates	100 Control and	
	- Dynamic Access Policies	username ech sort	Privilege Level (Role)	Access Restrictions	- Tobert Group Policy	- Tohert Group Door	Aca
	User Accounts	enable_15	15	rul	N/A	NA	Edit
	한다고 Certificate Management 요구한 DHCP 관구한 DNS 관구한 Advanced						Delete
	Device Setup						
	Ste-to-Ske VPN						
	÷			Αρφίγ	Reset		
				<admin></admin>	15 🐠	🞲 🔛 🤃 🤃	L/08 10:10:29 PM 15

2. 选择 Configuration > Device Management > Users/AAA > AAA Access > Authentication,以 便用 ASDM 为 SSH 设置 AAA 身份验证。

G	Home 🗞 Configuration 🔯 Monitorin	ng 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help
	Device Management 🗗 🖗 🗙	Configuration > Device Management > Users/AAA > AAA Access > Authentication
wice Lie	B - P Management Access B - System Image/Configuration	Authentication Authorization Accounting
ã.	문-@ High Availability 문-월 Logging	Enable authentication for administrator access to the ASA.
_	E-M Users/AAA	Require authentication to allow use of privileged mode commands
	And Server Groups	Enable Server Group: LOCAL CAL CAL 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
	E-P DHCP	Serial Server Group: LOCAL 🔽 🗖 Use LOCAL when server group fails.
	⊕ DNS ⊞ Advanced	Server Group: LOCAL V Lise LOCAL when server group fails
		Teinet Server Group: LOCAL 💌 🗖 Use LOCAL when server group fails
	2012212	
	A Device Setup	
	Frewal	
	Remote Access VPN	
	Ske-to-Ske VPN	
	Device Management	
	» *	Apply Reset
		<admin> 15 🐻 🛱 🔒</admin>

3. 选择 Configuration > Device Setup > Device Name/Password,以便用 ASDM 更改 Telnet □ 令。

Device Setup 🗇 🗘 🗙	Configuration > Devi	ce Setup > Device Name/Password	
Startup Wizard	Hostname and Domain N	lame	
Enterraces Enterraces	Hostname:	ciscoasa	
B - Pevice Name/Password	Domain Name:	default.domain.invalid	
	Enable Password		
	Change the privile	ged mode password.	
	Old Password:		
	New Pessword:		
	Confirm New Passwor	d:	
	Telnet Password		
	Change the passy	vord to access the console of the security appliance.	
	Old Password:		
	New Password:		
	Confirm New Passwor	d:	
Device Setup			
Frewal			
Remote Access VPN			
Site-to-Site VPN			
Device Management			

4. 选择 Configuration > Device Management > Certificate Management > Identity Certificates,单击 Add 并使用给出的默认选项,以便用 ASDM 生成相同的 RSA 密钥。

e Management (7 Con Con	figuration > Device Manag	ement > Certificate Manager	ment > Identity Certi	ificates		
SMMP	Issued To	Issued By	Expiry Da	ste	Usage	Add
System Image/Configuration						ShowDetails
Activation Key	🖆 Add Identity Certificate			×	1	Defectes
Boot Image/Configuratio	C Import the identity certif	icate from a file:				Export
ging	Decryption Passphrase:		-			Instel
cate Management	File to Import From:		Browse			
ertificates by Certificates	 Add a new identity certif 	icate:				
7. Outra	Key Pair:	<default-rsa-key></default-rsa-key>	T Show	New		
P Server	Certificate Subject DN:	CN=ciscoasa	Select			
	The demonstrate service service of the service	i cerui kate				
ARP Static Table	Acties local certa	icate authority and issue dynam	c certanicaties to TLS-Pro	1XY		
ertificates			bA	vanced	given interface. You can go	to <u>551 Settings</u> t
ary Metrics						
	add Cettf	rate Cancel	tieln			
	100 0010					
s VPN						
/PN						
anagement						
2			Apply Peset	1		
•						

5. 在 Add a new Identity certificate 下单击 New,以便添加默认的密钥对(如果没有)。然后

,	单击 Generate Nov	/o	ade 🔿 Forward 🤌 Helo			cisco
	Device Management of 9 ×	Configuration > Device Manage	ment > Certificate Manager	rent > Identity Certificates		cisco
e je	E- Management Access					
Derbo	System Image/Configuration Bread High Availability	Essued To	Issued By	Expiry Date	Usage	Add
	E- 🔁 Logging					Show Details
	AAA Server Groups	🔂 Add Identity Certificate		2	<	Delete
	- Authentication Prompt - 🏰 AAA Access	C Import the identity certific	cate from a file:			Export
	Dynamic Access Policies User Accounts	Decryption Passphrase:		-		Instel
	E- 🔜 Certificate Management	File to Import From:		Browsc		
	dentity Certificates	Add a new identity certific	cate:			
	E B DHCP	Key Pair:	<default-rsa-key></default-rsa-key>	Show New		
	E- 📴 Advanced	Cert 📬 Add Key Pair				
		E I mar c the	delay? I have all sound			
		Name: O ga	serate vey partitione			
		com luce	er newrikey pair name:		given interface. You can go	to <u>SSL Settinos</u> to
		5000: [1024				
		usage: (* Gen	iera purpose Cospe			
	Device Setup	General	Nov Cancel	Heb		
	Firewall		Canca		-	
	Remote Access VPN					
	Ste-to-Site VPN					
	Device Management					
	*			Apply Reset		

6. 选择 Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH),以便用 ASDM 指定允许通过 SSH 进行连接的主机,并指定版本和超时选项。

C	Home 🖓 Configuration 🔯 Monitoring	a 🔚 Save 🔇 Refresh 🔇 I	Bade 🔘 Forward 🧳 Help		CISCO
	Device Management 🗗 🔍 🗡	Configuration > Device Manage	ement > Management Access > Command	Line (CLI) > Secure Shell (SSH)	
🔲 Device List	Asperant Access A	Allowed SSH Version(s): 1 & 2 Specify the addresses of all hosts	Timeout: 5 minutes	zing Seaure Shell (SSH).	
	Console Timeout	Interface	IP Address	Mask	L Add !
	- 🍓 Secure Shell (SSH)	outside	192,168,200,1	255,255,255,255	Edit
	Pienet Pienet				Delete
	:		Apply	Reset	

7. 单击窗口顶部的 Save 以保存配置。

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

8. 提示在闪存中保存配置时,选择 Apply 以保存配置。

<u>Telnet 配置</u>

要添加对控制台的 Telnet 访问和设置空闲超时,请在全局配置模式下发出 **telnet** 命令。默认情况下 ,Telnet 会话持续处于非活动状态五分钟,安全设备就会将其关闭。要从以前设置的 IP 地址中删除 Telnet 访问,请使用此命令的 *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}}

使用 telnet 命令可以指定哪些主机能通过 Telnet 访问安全设备控制台。

注意:可以在所有接口上对安全设备启用 Telnet。但是,安全设备强制所有通向外部接口的 Telnet 流量都受到 IPsec 保护。要启用通向外部接口的 Telnet 会话,请在外部接口上配置 IPsec,使其包 括由安全设备生成的 IP 流量,并在外部接口上启用 Telnet。

注意: 一般而言,如果任何接口的安全级别为 0 或低于任何其他接口,则 PIX/ASA 不允许对该接 口进行 Telnet。

注意: 建议不要通过 Telnet 会话访问安全设备。身份验证凭据信息(如口令)是以明文形式发送的。Telnet 服务器和客户端通信仅以明文形式进行。Cisco 建议使用 SSH 以使数据通信更安全。

如果输入 IP 地址,则还必须输入网络掩码。没有默认的网络掩码。请勿使用内部网络的子网掩码。 网络掩码只是 IP 地址的位掩码。要限制对单个 IP 地址的访问,请在每个八位组中都使用 255;例 如,255.255.255.255。

如果 IPsec 运行正常,则可以指定不安全的接口名称,这通常是外部接口。最低限度可以配置 crypto map 命令,以便用 telnet 命令指定一个接口名称。

发出 password 命令,以便为对于控制台的 Telnet 访问设置口令。默认值为 cisco。发出 who 命令 ,以便查看当前有哪些 IP 地址访问安全设备控制台。发出 kill 命令,以便终止活动的 Telnet 控制台 会话。

要启用通向内部接口的 Telnet 会话,请查看以下这些示例:

示例 1

本示例仅允许主机 10.1.1.1 通过 Telnet 访问安全设备控制台:

pix(config)#telnet 10.1.1.1 255.255.255.255 inside

本示例仅允许网络 10.0.0.0/8 通过 Telnet 访问安全设备控制台:

示例3

本示例允许所有网络通过 Telnet 访问安全设备控制台:

^{pix(config)#**telnet** 0.0.0.0 0.0.0.0 inside 如果使用带有 console 关键字的 **aaa** 命令,则必须用身份验证服务器对 Telnet 控制台访问进行身份 验证。}

注意:如果配置了 aaa 命令,要求对安全设备 Telnet 控制台访问进行身份验证,并且控制台登录 请求超时,则可以从串行控制台访问安全设备。为此,请输入用 enable password 命令设置的安全 设备用户名和口令。

发出 **telnet timeout** 命令,以便设置安全设备注销控制台 Telnet 会话之前该会话可处于空闲状态的 最长时间。不能将 **no telnet** 命令与 telnet timeout 命令配合使用。

本示例显示如何更改会话空闲最长持续时间:

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

ACS 4.x 中的 SSH/Telnet 支持

如果发现了 RADIUS 功能,则可以对 SSH 功能使用 RADIUS。

当尝试通过 Telnet、SSH、HTTP 或串行控制台连接访问安全设备,并且流量符合身份验证声明时 ,安全设备将请求用户名和口令。然后安全设备将这些凭据发送到 RADIUS (ACS) 服务器,并根据 服务器的响应准许或拒绝 CLI 访问。

有关详细信息,请参阅<u>配置 AAA 服务器和本地数据库</u>的 <u>AAA 服务器和本地数据库支持</u>部分。

例如,ASA 安全设备 7.0 需要一个 IP 地址,安全设备将从中接受连接,如:

hostname(config)#**ssh source_IP_address mask source_interface** 有关详细信息,请参阅<u>配置 AAA 服务器和本地数据库</u>的<u>允许 SSH 访问</u>部分。

请参阅 <u>PIX/ASA:使用 TACACS+ 和 RADIUS 服务器的网络访问直通代理配置示例</u>,详细了解有 关如何配置对 PIX 带有 ACS 身份验证的 SSH/Telnet 访问。

验证

使用本部分可确认配置能否正常运行。

<u>命令输出解释程序(仅限注册用户</u>)(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输 出的分析。

<u>调试 SSH</u>

发出 debug ssh 命令以打开 SSH 调试。

^{pix(config)#**debug ssh** SSH debugging on 下面的输出显示从主机 10.1.1.2(在 PIX 的外部)到"PIX"的身份验证请求成功:}

```
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
﹐如果用户提供的用户名有误(例如"pix1"而非"pix"),则 PIX 防火墙拒绝身份验证。下面的调试输
出显示身份验证失败:
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.
同样地,如果用户提供的口令有误,则下面的调试输出显示身份验证失败。
```

pix#

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.

<u>查看活动的 SSH 会话</u>

发出下面这个命令以便检查所连接的 SSH 会话的数量以及与 PIX 的连接状态:

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 选择 Monitoring > Properties > Device Access > Secure Shell Sessions,以便用 ASDM 查看会话

0

<u>查看 RSA 公钥</u>

发出下面这个命令,以便查看安全设备上 RSA 密钥的公共部分:

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: 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4 95f66c34 2c2ced37 aa3442d8 12158c93 131480dd 967985ab 1d7b92d9 5290f695 8e9b5b0d d88c0439 6169184c d8fb951c 19023347 d6b3f939 99ac2814 950f4422 69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c de61aef1 165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001 选择Configuration>属性>证书>密钥对,并且单击显示详细信息为了查看与ASDM的RSA密钥。

<u>故障排除</u>

本部分提供的信息可用于对配置进行故障排除。

如何从 PIX 删除 RSA 密钥

某些情况下(例如升级 PIX 软件或更改 PIX 中的 SSH 版本时),可能会要求删除并重新创建 RSA 密钥。发出下面这个命令,以便从 PIX 删除 RSA 密钥对:

pix(config)#crypto key zeroize rsa 选择Configuration>属性>证书>密钥对,并且点击删除为了去除与ASDM的RSA密钥。

<u>SSH 连接失败</u>

在PIX/ASA的错误消息:

%PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed. 在SSH客户端计算机的对应的错误消息:

Selected cipher type <unknown> not supported by server. 要解决此问题,请删除并重新创建 RSA 密钥。发出下面这个命令,以便从 ASA 删除 RSA 密钥对 :

ASA(config)#**crypto key zeroize rsa** 发出下面这个命令,以便生成新密钥:

ASA(config)# crypto key generate rsa modulus 1024

<u>无法通过 SSH 访问 ASA</u>

错误消息:

ssh_exchange_identification: read: Connection reset by peer 要解决此问题,请完成以下步骤:

- 1. 重新加载 ASA,或删除所有与 SSH 相关的配置和 RSA 密钥。
- 2. 重新配置 SSH 命令,并重新生成 RSA 密钥。

<u>使用SSH,无法访问第二ASA</u>

当ASA在故障切换模式时,不是可能的对SSH对待机ASA通过VPN通道。这是因为SSH的回复流量 取出待机ASA的外部接口。

相关信息

- <u>Cisco PIX 500 系列安全设备</u>
- <u>Cisco ASA 5500 系列自适应安全设备</u>
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 配置 SSH 连接 Cisco 路由器和 Cisco 集中器
- <u>请求注解 (RFC)</u>
- <u>技术支持和文档 Cisco Systems</u>