PIX/ASA 7.x: SSH/Telnet no exemplo de configuração da interface interna e externa

Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados **Produtos Relacionados** Convenções Configurar Diagrama de Rede Configurações SSH Configuração com ASDM 5.x Configuração com ASDM 6.x Configuração do telnet Apoio SSH/Telnet no ACS 4.x Verificar Debugar o SSH Veja sessões SSH ativa Veja a chave pública RSA Troubleshooting Como remover as chaves RSA do PIX Conexão de SSH falhada Incapaz de alcançar o ASA com SSH Incapaz de alcançar o ASA secundário usando o SSH Informações Relacionadas

Introdução

Este documento fornece uma configuração de exemplo do Secure Shell (SSH) nas interfaces internas e externas da versão 7.x, e mais recente, do Cisco Series Security Appliance. A configuração da ferramenta de segurança da série remotamente com a linha de comando envolve o uso do telnet ou do SSH. Porque as comunicações de Telnet são enviadas no texto claro, que inclui senhas, o SSH é altamente recomendado. O tráfego SSH é cifrado em um túnel e desse modo as ajudas protegem senhas e outros comandos configuration da intercepção.

A ferramenta de segurança permite conexões de SSH à ferramenta de segurança para propósitos do gerenciamento. A ferramenta de segurança permite um máximo de cinco conexões de SSH simultâneas para cada <u>contexto de segurança</u>, se disponível, e um máximo global de 100 conexões para todos os contextos combinados.

Neste exemplo de configuração, a ferramenta de segurança PIX é considerada ser o servidor de SSH. O tráfego dos clientes SSH (10.1.1.2/24 e 172.16.1.1/16) ao servidor de SSH é cifrado. A ferramenta de segurança apoia a funcionalidade do shell remoto SSH fornecida nas versões de SSH 1 e 2 e apoia o Data Encryption Standard (DES) e as cifras 3DES. As versões de SSH 1 e 2 são diferentes e não são interoperáveis.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 7.1 e 8.0 do Software do firewall Cisco PIX.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Nota: SSHv2 é apoiado na versão 7.x e mais recente PIX/ASA e não apoiado nas versões mais cedo a 7.x.

Produtos Relacionados

Esta configuração pode igualmente ser usada com a ferramenta de segurança do 5500 Series de Cisco ASA com versões de software 7.x e mais tarde.

Convenções

Consulte as <u>Convenções de Dicas Técnicas da Cisco</u> para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Cada etapa de configuração é presentado com a informação necessária para usar a linha de comando ou o Security Device Manager adaptável (ASDM).

Nota: Use a <u>Command Lookup Tool</u> (<u>somente clientes registrados</u>) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações SSH

Este documento utiliza as seguintes configurações:

- <u>Acesso SSH à ferramenta de segurança</u>
- Como usar um cliente SSH
- <u>Configuração de PIX</u>

Acesso SSH à ferramenta de segurança

Termine estas etapas a fim configurar o acesso SSH à ferramenta de segurança:

- 1. As sessões SSH exigem sempre um nome de usuário e senha para a autenticação. Há duas maneiras de cumprir esta exigência. Configurar um nome de usuário e senha e use o AAA:Sintaxe:pix(config)#username username password password pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]} Nota: Se VOCê USA um TACACS+ ou um grupo de servidor Radius para a autenticação, você pode configurar a ferramenta de segurança para usar o base de dados local como um método da reserva se o servidor AAA é não disponível. Especifique o nome de grupo de servidor e então o LOCAL (o LOCAL é diferenciando maiúsculas e minúsculas). Nós recomendamos que você usa o mesmo nome de usuário e a senha no base de dados local como o servidor AAA, porque a alerta da ferramenta de segurança não dá nenhuma indicação que o método for USado.Nota: Exemplo:pix(config) #aaa authentication ssh console TACACS+ LOCAL Nota: VOCê pode alternativamente usar o base de dados local como seu método principal da autenticação sem a reserva. A fim fazer isto, entre em sozinho LOCAL.Exemplo:pix(config)#aaa authentication ssh console LOCAL OUUse o nome de usuário padrão do pix e a senha telnet do padrão de Cisco. Você pode mudar a senha telnet com este comando:pix(config)#passwd password Nota: O comando password pode igualmente ser usado nesta situação. Os comandos both fazem a mesma coisa.
- 2. Gerencia um par de chaves RSA para o PIX Firewall, que seja exigido para o SSH:pix(config)#crypto key generate rsa modulus modulus_size Nota: o modulus_size (nos bit) pode ser 512, 768, 1024, ou 2048. Maior o tamanho que chave do módulo você especificam, mais por muito tempo toma para gerar o par de chaves RSA. O valor de 1024 é recomendado.Nota: O comando usado para gerar um par de chaves RSA é diferente para versões de software de PIX mais cedo do que 7.x. Nas versões anterior, um Domain Name deve ser ajustado antes que você possa criar chaves.Nota: No modo de contexto múltiplo, você deve gerar as chaves RSA para o cada contextos. Além, os comandos crypto não são apoiados no modo do contexto do sistema.

- 3. Especifique os anfitriões permitidos conectar à ferramenta de segurança. Este comando especifica o endereço de origem, o netmask e a relação dos host permitidos conectar com o SSH. Pode ser entrado épocas múltiplas para host múltiplos, redes, ou relações. Neste exemplo, um host no interno e um host na parte externa são permitidos.pix(config)#ssh 172.16.1.1 255.255.255.255 inside pix(config)#ssh 10.1.1.2 255.255.255.0tside
- 4. Opcional: À revelia, a ferramenta de segurança permite a versão de SSH 1 e a versão 2. incorpora este comando a fim restringir conexões a uma versão específica:pix(config)# ssh version <version_number> Nota: o version_number pode ser 1 ou 2.
- 5. **Opcional:** À revelia, as sessões SSH são fechadas após cinco minutos da inatividade. Este intervalo pode ser configurado dura por entre 1 e 60 minutos.pix(config)#ssh timeout minutes

Como usar um cliente SSH

Forneça o username e a senha de login da ferramenta de segurança da série PIX 500 quando você abrir a sessão SSH. Quando você começar uma sessão SSH, indicadores de um ponto (.) no console da ferramenta de segurança antes que a alerta da autenticação de usuário SSH aparecer:

hostname(config)# .

O indicador do ponto não afeta a funcionalidade do SSH. O ponto aparece no console quando uma chave de servidor está gerada ou uma mensagem está decifrada com chaves privadas durante trocas de chave SSH antes que a autenticação de usuário ocorra. Estas tarefas podem tomar até dois minutos ou mais por muito tempo. O ponto é um Progress Indicator que verifica que a ferramenta de segurança é ocupada e não o pendurou.

As versões de SSH 1.x e 2 são protocolos totalmente diferentes e não são compatíveis. Transfira um cliente compatível. Refira a <u>obtenção a uma</u> seção do <u>cliente SSH das</u> <u>configurações</u> <u>avançadas</u> para mais informação.

Configuração de PIX

Este documento utiliza esta configuração:

```
Configuração de PIX
PIX Version 7.1(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
!
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:a6b05fd04f9fbd0a39f1ca7328de91f7 : end
```

Nota: A fim alcançar a interface de gerenciamento do ASA/PIX usando o SSH, emita este comando: Gerenciamento de 172.16.16.160 255.255.255.255 do ssh

Configuração com ASDM 5.x

Termine estas etapas a fim configurar o dispositivo para o SSH usando o ASDM:

 Escolha a configuração > as propriedades > a administração > as contas de usuário do dispositivo a fim adicionar um usuário com ASDM.

Image: Security Falcy Image: Security Falcy Image: Security Falcy Image: Security Falcy <th>G Hame</th> <th>Configuration Monitoring</th> <th>Back Forward</th> <th>Q Q Search Refresh</th> <th>調 🤶 Save Halp</th> <th></th> <th>Cisco Systems</th>	G Hame	Configuration Monitoring	Back Forward	Q Q Search Refresh	調 🤶 Save Halp		Cisco Systems
FTTP Server Jerr Accounts DHCP Services Jons Client Failover Apply Reset	Herfaces Herfaces Security Policy NAT Security Policy NAT VPN Security Policy NAT Security Policy Security Policy Security Policy Security Policy Prove Security Policy Security Policy Securit	Configuration > Properties > Devi Startup Wizard AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup Configuration AAP Auto Update Certificate Device Access Device Access Device Administration Console	ice Administration > U Create entries in the user account privileg User Name enable_15 ciscouser	Ser Accounts PIX local user databa les to be enforced. To Privilege (Level) NA (15) NA (2)	ise. Command author enable command aut VPN Group Policy NA DiftGrpPolicy	Ization must be enable horization, go to <u>Author</u> VPN Group Lock N/A Inherit Group Po	d in order for the Ization. Add Edit Delete
		Fillover		Apply	Rese	t	

2. Escolha a **configuração > as propriedades > o acesso de dispositivo > o acesso > a autenticação AAA** a fim estabelecer a autenticação de AAA para o SSH com ASDM.

G Home	Configuration Monitoring	Back Forward	Q C Search Refre	sh Save	? Неір	CISCO SYSTEMS
Home Interfaces Security Policy NAT Security Policy	Configuration Montoring Configuration > Properties = Configuration = Properties = Configuration = Properties = Configuration = Properties = Configuration = Configuration = Configu	Back Forward	Search Refr coss > Authenticat prization/Accounting Authorization ation for administrat ation for administrat attocation for administrat attocation for the foll M Server Group: Server Group: Server Group: Server Group: Server Group:	Accounting Accounting or access to the se of privileged LOCAL LOCAL	Help Help PIX. mode commandu Connections	DCAL when server group fails DCAL when server group fails DCAL when server group fails DCAL when server group fails DCAL when server group fails
Device configura	tion Inaded successfully	J	riscouse			A 5/22/08 8-24-28 PM LITC

 Escolha a configuração > as propriedades > a administração > a senha do dispositivo a fim mudar a senha telnet com ASDM.

G Home	Configuration Monitoring	Cisco Sys Back Forward Search Refresh Save Halp	TENS
Herfaces Security Policy NAT Security Policy NAT Security NAT Security Routing Clobal Objects Properties	Configuration > Properties > D	Plassword Change the privileged mode and Telnet passwords. Enable Password Change the privileged mode password. This is also the password to log into ASDM. Of d Password: New Password: Confirm New Password: Old Password: Output Apply Reset	
Device configura	ation loaded successfully.	ciscouser 🛛 NA (2) 🛛 🙀 👘 5/23/06 6:30:38 PI	M UTC

4. Escolha a **configuração > as propriedades > o certificado > o par de chaves**, o clique **adiciona** e usa as opções padrão apresentadas a fim gerar as mesmas chaves RSA com ASDM.



5. Escolha a configuração > as propriedades > o acesso de dispositivo > o Secure Shell a fim usar o ASDM para especificar os anfitriões permitidos conectar com o SSH e especificar a versão e as opções de timeout.

Home C	Sonfiguration Monitoring	Sack Forward Search Refresh Save Help	Cisco Systems
Interfaces Security Policy NAT Security Policy NAT Security Routing Clobal Objects Clobal Objects	Configuration > Properties > D Startup Wizard AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Setup AAA Coss Certificate Device Access AAA Access AAA Access AAA Access Certificate Device Access AAA Access Certificate Device Access Certificate Device Access Certificate Device Access Certificate Device Access Certificate Certificate Device Access Certificate	Access - Secure Shell Secure Bhell Allowed SSH Version(s): Image: Secure Shell (0) Specify the addresses of all hosts/networks which are allowed to access the PIX using Secure Shell (SSH). Interface IP Address Mask inside 172.10.1.1 255.255.255.255 outside 10.1.1.2	Add Edit Delete
	URL Filtering	Apply Reset	

6. Clique o **arquivo > salvar que executa a configuração para piscar** a fim salvar a configuração.

🚰 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	istration > Boot Image/Configur /Configuration onfiguration nfigure boot images from an externa the boot system. Only one TFTP bo		
Save Running Configuration to TFTP Server Save Running Configuration to Standby Unit Save Internal Log Buffer to Flash			
Clear ASDM Cache Clear Internal Log Buffer	first image in the list. loot Order		
Exit	1 disk0:/pix722.bin		

Configuração com ASDM 6.x

Conclua estes passos:

1. Escolha a configuração > o Gerenciamento de dispositivos > o Users/AAA > as contas de usuário a fim adicionar um usuário com

A	SDIVI.					_	
S	Home 🖧 Configuration 🔯 Monitori	ng 🔚 Save 🔇 Ra	fresh 🔇 Back 🔘 Forwa	d 🦹 🖓 Help			CISCO
Device Ust	Device Management C P × Management Access D System Image/Configuration D High Availability D Logong D Jess/AAA MAA Server Groups Authentication Prompt	Configuration > Device Management > Users/AAA > User Accounts 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 A AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication go to Authentication.					
		Username stluser1 enable_13	Privlege Level (Role) 2 15	Access Restrictions Full	VPN Group Policy - Inherit Group Policy N(A	VPN Group Lod: Snherit Group Pelicy N/A	Add tak Delote
	*			Αρρίγ	Reset		
				<admin></admin>	15 😡	🐨 🗌 🔂 3/21	./08 10:10:29 PM 15T

 Escolha a configuração > o Gerenciamento de dispositivos > o Users/AAA > o acesso > a autenticação AAA a fim estabelecer a autenticação de AAA para o SSH com ASDM.

Device Management D. V A	Configuration > Device Management > Users/AMA > AAA Access > Authentication
⊞-∰ Management Access ⊞-∰ System Image/Configuration	Authentication Authorization Accounting
S ⊕-@ High Availability ⊕-B Logging	Enable authentication for administrator access to the ASA.
E-SMI Users/AAA	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 🚮 Certificate Management	HTTP/ASDM Server Group: LOCAL * Use LOCAL when server group fails
B-P DHCP	Serial Server Group: LOCAL 💌 🗖 Use LOCAL when server group fails
E-B Advanced	Server Group: LOCAL V III Use LOCAL when server group fails
	Teinet Server Group: LOCAL V 🗖 Use LOCAL when server group fails
Bevice Setup	
Freval	
Remote Access VPN	
Remote Access VPN Ste-to-Site VPN	
Sterios Permote Access VPN Sterios Sterios Device Management	Ante I Dent

 Escolha a configuração > a instalação > o nome de dispositivo/senha de dispositivo a fim mudar a senha telnet com ASDM.

S) Home 🦓 Configuration 🔯 Monitorin	ng 🕞 Save 💽 Refres	sh 🔇 Back: 🔘 Forward	2 Help	
	Device Setup Q_ ×	Configuration > Device	e Setup > Device Name/Pas	sword	
eList		Hostname and Domain Na	me		
Devk	E-+++ Routing	Hostname:	ciscoasa		
	Device Name/Password System Time	Domain Name:	default.domain.invalid		
		Enable Password			
		Change the privileg	ed mode password.		
		Old Pass word:			
		New Password:			
		Confirm New Password:			
		Teinet Password			
		Change the passwo	and to access the console of the se	ecurity appliance.	
		Old Password:			
		New Password:			
		Confirm New Password	:		
	A Device Setup				
	Firewal				
	Remote Access VPN				
	Ste-to-Site VPN				
	Device Management				
	*			Apply Reset	
				<admin> 15</admin>	🗔 🍻 🔒

4. Escolha a configuração > o > gerenciamento de certificado > os certificados de identidade do Gerenciamento de dispositivos, o clique adiciona e usa as opções padrão apresentadas a fim gerar as mesmas chaves RSA com

vice Management (7 P × C	Configuration > Device Manage	ement > Certificate Manage	ment > Identity Certificates		
- T SNMP	Issued To	Issued By	Expiry Date	Usage	Add
- PM Management Access Ruk System Image/Configuration					Show Del
- 🍓 Activation Key	🚰 Add Identiby Contificate			×1	0.00
- 🛃 Auto Update - 😘 Boot Image/Configuratio	And Identity Certificate				District
🖗 High Availability	C Import the identity certif	ficate from a file:			Expor
Cogging	Decryption Passphrase:		_		Insta
Certificate Management	File to Import From:		Browse		
- A Certificates	C Well a new identity card	- 			
P DHOP	·· ///////////////////////////////////	585:			
- 💕 DHCP Relay	Key Pair:	<default-rsa-key></default-rsa-key>	Show New		
- fp" DHCP Server	Certificate Subject DN:	CN-ciscoasa	Select		
Advanced	Generate self-signed	i certificate			
E- B ARP	E Act as local contri	icate a thority and issue dynami	is costificates to TLS-Porov		
HTTP Redirect				sinon interface. Very same	a to SEL Solling
SS. Certificates			Advanced	given ricerrace. Too carry	0 (0 <u>301 380 11</u>
- M History Metrics				-	
	Allowed	and soul 1			
Device Setup	Add Certin	cate Cancel	nep		
Frewal					
Remote Access VDM					
Contract Material Contraction					
Ske-to-Ske VPN					
Davika Managament					

5. Sob adicionar um clique novo do certificado de identidade novo a fim adicionar um par de

chave padrão se um não faz existe. Então, o clique **gerencie** agora.



6. Escolha a configuração > o Gerenciamento de dispositivos > o acesso de gerenciamento > a linha de comando (CLI) > Shell Seguro (ssh) a fim usar o ASDM para especificar os anfitriões permitidos conectar com o SSH e especificar a versão e as opções de timeout.



7. Clique a **salvaguarda** sobre o indicador a fim salvar a configuração.

File	e View Tools Wizards Window H	elp
C	Home 🔏 Configuration 🔯 Monitor	ing 🔚 Save 🐼 Refresh 🔇 Back 🕥 Forward 🤗 Help 📄
	Device Management 🗗 🕂 🗙	Config Save Running Configuration to Flash Management Access >
/ice List	Management Access	Allowed SSH Version(s): 1 & 2 Timeout: 5

8. Quando alertado para salvar a configuração no flash, escolha **aplicam-se** a fim salvar a configuração.

Configuração do telnet

A fim adicionar o acesso do telnet ao console e ajustar o idle timeout, emita o **comando telnet no** modo de configuração global. À revelia, as sessões de Telnet que são deixadas inativas por cinco minutos são fechadas pela ferramenta de segurança. A fim remover o acesso do telnet de um endereço IP de Um ou Mais Servidores Cisco ICM NT previamente ajustado, não use *nenhum* formulário deste 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}}

O comando telnet deixa-o especificar que anfitriões podem alcançar o console da ferramenta de segurança com telnet.

Nota: Você pode permitir o telnet à ferramenta de segurança em todas as relações. Contudo, a ferramenta de segurança reforça que todo o tráfego do telnet à interface externa esteja protegido pelo IPsec. A fim permitir uma sessão de Telnet à interface externa, configurar o IPsec na interface externa para incluir o tráfego IP que é gerado pela ferramenta de segurança e para permitir o telnet na interface externa.

Nota: Geralmente, se nenhuma relação que tiver um nível de segurança de 0 ou o abaixar do que toda a outra relação, a seguir PIX/ASA não permite o telnet a essa relação.

Nota: Não se recomenda alcançar a ferramenta de segurança através de uma sessão de Telnet. A informação das credenciais de autenticação, tal como a senha, é enviada como o texto claro. O servidor Telnet e a comunicação cliente acontecem somente com o texto claro. Cisco recomenda usar o SSH para uma comunicação de dados mais fixada.

Se você incorpora um endereço IP de Um ou Mais Servidores Cisco ICM NT, você deve igualmente incorporar um netmask. Não há nenhum netmask do padrão. Não use a máscara da sub-rede da rede interna. O netmask é somente uma máscara de bit para o endereço IP de Um ou Mais Servidores Cisco ICM NT. A fim limitar o acesso a um único endereço IP de Um ou Mais Servidores Cisco ICM NT, use 255 em cada octeto; por exemplo, 255.255.255.255.

Se o IPsec se opera, você pode especificar um nome inseguro da relação, que seja tipicamente a interface externa. Pelo menos, você pode configurar o **comando crypto map** a fim especificar um nome da relação com o **comando telnet**.

Emita o **comando password** a fim ajustar uma senha para o acesso do telnet ao console. O padrão é Cisco. Emita o **comando who** a fim ver que os endereços IP de Um ou Mais Servidores Cisco ICM NT alcançam atualmente o console da ferramenta de segurança. Emita o **comando kill** a fim terminar uma sessão de console ativa do telnet.

A fim permitir uma sessão de Telnet à interface interna, reveja estes exemplos:

Exemplo 1

Este exemplo permite somente o host 10.1.1.1 aceder ao console da ferramenta de segurança com o telnet:

pix(config)#telnet 10.1.1.1 255.255.255.255 inside Exemplo 2

Este exemplo permite somente a rede 10.0.0.0/8 aceder ao console da ferramenta de segurança com o telnet:

pix(config)#telnet 10.0.0.0 255.0.0.0 inside Exemplo 3

Este exemplo permite que todas as redes acedam ao console da ferramenta de segurança com o telnet:

pix(config)#telnet 0.0.0.0 0.0.0.0 inside

Se você usa o **comando aaa** com a palavra-chave do console, o acesso de console do telnet deve ser autenticado com um Authentication Server.

Nota: Se você configurou o **comando aaa** a fim exigir a autenticação para o acesso de console do telnet da ferramenta de segurança e o console de login pede épocas para fora, você pode aceder à ferramenta de segurança do console serial. A fim fazer isto, incorpore o username da ferramenta de segurança e a senha que é ajustada com o **comando enable password**.

Emita o comando do **Timeout da Telnet** a fim ajustar o tempo máximo que uma sessão de Telnet do console pode ser inativa antes que esteja terminado pela ferramenta de segurança. Você não pode não usar **nenhum comando telnet** com o comando do **Timeout da Telnet**.

Este exemplo mostra como mudar a duração da quietude da sessão máxima:

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

Apoio SSH/Telnet no ACS 4.x

Se você olha as funções do RAIO, você pode usar o RAIO para a funcionalidade SSH.

Quando uma tentativa é feita para alcançar a ferramenta de segurança com telnet, SSH, HTTP, ou uma conexão do console serial e o tráfego combinam uma instrução de autenticação, a ferramenta de segurança pede um nome de usuário e senha. Envia então estas credenciais ao server do RAIO (ACS), e concede ou nega o acesso CLI baseado na resposta do server.

Refira a <u>seção de suporte do servidor AAA e do base de dados local de</u> <u>configurar servidores</u> <u>AAA e o base de dados local</u> para mais informação.

Por exemplo, sua ferramenta de segurança 7.0 ASA precisa um endereço IP de Um ou Mais Servidores Cisco ICM NT de que a ferramenta de segurança aceita conexões, como:

Refira a seção <u>reservando do acesso SSH de</u> <u>configurar servidores AAA e o base de dados local</u> para mais informação.

Refira o <u>PIX/ASA: Corte-através do proxy para o acesso de rede usando o TACACS+ e o</u> <u>exemplo da configuração de servidor RADIUS</u> para obter mais informações sobre de como configurar SSH/Telnet alcance ao PIX com autenticação de ACS.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

Debugar o SSH

Emita o comando debug ssh a fim girar sobre a eliminação de erros SSH.

pix(config)#debug ssh SSH debugging on

Esta saída mostra que o pedido de autenticação do host 10.1.1.2 (fora ao PIX) ao "pix" é bem sucedido:

```
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 um usuário dá um nome de usuário errado, por exemplo, "pix1" em vez do "pix", o PIX Firewall rejeita a autenticação. Este resultado do debug mostra a autenticação falha:

```
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.
```

Similarmente, se o usuário fornece a senha errada, este resultado do debug mostra-lhe a autenticação falha.

```
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.
```

Sessões SSH ativa da vista

Emita este comando a fim verificar o número de sessões SSH que são conectadas e do estado de conexão ao PIX:

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
Escolha a monitoração > as propriedades > as sessões do acesso de dispositivo > do Secure
Shell a fim ver as sessões com o ASDM.

Veja a chave pública RSA

Emita este comando a fim ver a parcela pública das chaves RSA na ferramenta de segurança:

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 Escolba a configuração > as propriedades > o certificado > o par de chaves o clique detalbas de

Escolha a **configuração > as propriedades > o certificado > o par de chaves**, e clique **detalhes da mostra** a fim ver chaves RSA com o ASDM.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Como remover as chaves RSA do PIX

Determinadas situações, como quando você promove o software de PIX ou muda a versão de SSH no PIX, podem exigi-lo remover e recrear chaves RSA. Emita este comando a fim remover o par de chaves RSA do PIX:

pix(config)#crypto key zeroize rsa

Escolha a **configuração > as propriedades > o certificado > o par de chaves**, e clique a **supressão** a fim remover as chaves RSA com o ASDM.

Conexão de SSH falhada

Mensagem de Erro no PIX/ASA:

%PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed. O Mensagem de Erro correspondente na máquina de cliente SSH:

Selected cipher type <unknown> not supported by server. A fim resolver esta edição, remova e recreie as chaves RSA. Emita este comando a fim remover o par de chaves RSA do ASA:

ASA(config)#crypto key zeroize rsa Emita este comando a fim gerar a chave nova:

ASA(config)# crypto key generate rsa modulus 1024

Incapaz de alcançar o ASA com SSH

Mensagem de Erro:

<u>ssh exchange identification: read: Connection reset by peer</u> Para resolver esse problema, siga estas etapas:

- 1. Recarregue o ASA ou remova toda a configuração relativa SSH e as chaves RSA.
- 2. Reconfigure os comands SSH e regenere as chaves RSA.

Incapaz de alcançar o ASA secundário usando o SSH

Quando o ASA reage do modo de failover, não é possível ao SSH ao ASA à espera através do túnel VPN. Isto é porque o tráfego da resposta para o SSH toma a interface externa do ASA à espera.

Informações Relacionadas

- <u>Cisco PIX 500 Series Security Appliances</u>
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco PIX Firewall Software</u>
- <u>Referências do comando Cisco Secure PIX Firewall</u>
- <u>Configurando conexões de SSH Roteadores Cisco & concentradores Cisco</u>
- Solicitações de Comentários (RFCs)
- <u>Suporte Técnico e Documentação Cisco Systems</u>