PIX/ASA 7.x: SSH/telnet op het configuratievoorbeeld van de binnen- en buitenkant

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten **Conventies** Configureren Netwerkdiagram SSH-configuraties Configuratie met ASDM 5.x Configuratie met ASDM 6.x **Telnet-configuratie** Ondersteuning van SSH/telnet in ACS 4.x Verifiëren **Debug SSH** Actieve SSH-sessies bekijken Bekijk de openbare RSA-toets Problemen oplossen Hoe de RSA-toetsen uit de PIX te verwijderen SSH-verbinding is mislukt Kan geen toegang krijgen tot ASA met SSH Kan geen toegang tot secundaire ASA met SSH Gerelateerde informatie

Inleiding

Dit document biedt een voorbeeldconfiguratie van Secure Shell (SSH) op de binnen- en externe interfaces van Cisco Series security applicatie versie 7.x en hoger. De configuratie van de Series security applicatie extern met de opdrachtregel betreft het gebruik van telnet of SSH. Omdat de mededelingen van het telnet in heldere tekst worden verzonden, die wachtwoorden omvat, wordt SSH zeer aanbevolen. Het SSH-verkeer is versleuteld in een tunnel en beschermt dus wachtwoorden en andere configuratieopdrachten tegen interceptie.

Met de security applicatie kunt u SSH-verbindingen naar het security apparaat maken voor beheerdoeleinden. Het security apparaat maakt maximaal vijf gelijktijdige SSH-verbindingen

mogelijk voor elke <u>beveiligingscontext</u>, indien beschikbaar, en maximaal 100 verbindingen voor alle contexten samen.

In dit configuratievoorbeeld wordt de PIX security applicatie beschouwd als de SSH-server. Het verkeer van SSH-clients (10.1.1.2/24 en 172.16.1.1/16) naar de SSH-server is versleuteld. Het beveiligingsapparaat ondersteunt de SSH-functionaliteit op afstand die wordt geboden door SSH-versies 1 en 2 en ondersteunt Data Encryption Standard (DES) en 3DES-telefoons. SSH versies 1 en 2 verschillen en zijn niet interoperabel.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco PIX Firewall versie 7.1 en 8.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Opmerking: SSHv2 wordt ondersteund in PIX/ASA versie 7.x en later en niet ondersteund in versies eerder tot 7.x.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco ASA 5500 Series security applicatie met softwareversies 7.x en hoger.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Elke configuratiestap is voorzien van de benodigde informatie om de opdrachtregel of de adaptieve security apparaatbeheer (ASDM) te gebruiken.

Opmerking: Gebruik het <u>Opdrachtupgereedschap</u> (alleen<u>geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

PIX Inside 172.16.5.10/16 SSH Server Cloud SSH Client 10.1.1.2/24 Router 10.1.1.1/24 Router 10.1.1.1/24 Router 10.1.1.1/24 SSH Client 172.168.200.1/24 SSH Client 172.168.201.1/24

SSH-configuraties

Dit document gebruikt deze configuraties:

- <u>SSH-toegang tot de security applicatie</u>
- Hoe een SSH-client wordt gebruikt
- PIX-configuratie

SSH-toegang tot de security applicatie

Volg deze stappen om de SSH-toegang tot het beveiligingsapparaat te configureren:

1. SSH-sessies vereisen altijd een gebruikersnaam en wachtwoord voor verificatie. Er zijn twee manieren om aan deze eis te voldoen.Configureer een gebruikersnaam en wachtwoord en gebruik AAA:Syntaxis:

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

Opmerking: Als u een TACACS+ of RADIUS-servergroep voor verificatie gebruikt, kunt u het security apparaat configureren om de lokale database als back-upmethode te gebruiken als de AAA-server niet beschikbaar is. Specificeer de naam van de servergroep en PLAATSELIJK (PLAATSELIJK is hoofdlettergevoelig). Wij raden u aan in de lokale database dezelfde gebruikersnaam en wachtwoord te gebruiken als de AAA-server, omdat de melding van het beveiligingsapparaat geen indicatie geeft van de gebruikte methode.**Opmerking:** Voorbeeld:

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

Opmerking: U kunt de lokale database ook gebruiken als hoofdmethode voor authenticatie zonder back-up. Voer daartoe alleen LOCAL in.Voorbeeld: pix(config)#aaa authentication ssh console LOCAL

OFGebruik de standaardgebruikersnaam voor **PIX** en het defaultwachtwoord van telnet van **Cisco**. U kunt het Telnet-wachtwoord met deze opdracht wijzigen: pix(config)#passwd password

Opmerking: de opdracht **wachtwoord** kan ook in deze situatie worden gebruikt. Beide opdrachten doen hetzelfde.

Het netwerk in dit document is als volgt opgebouwd:

2. Genereert een RSA-sleutelpaar voor de PIX-firewall, die nodig is voor SSH: pix(config)#crypto key generate rsa modulus modulus_size

Opmerking: modulus_size (in bits) kan 512, 768, 1024 of 2048 zijn. Hoe groter de standaardgrootte die je specificeert, hoe langer het duurt om het RSA-sleutelpaar te genereren. De waarde van 1024 wordt aanbevolen.**Opmerking:** de opdracht die wordt gebruikt om <u>een RSA key pair te genereren</u> is anders voor PIX-softwareversies eerder dan 7.x. In eerdere versies moet een domeinnaam worden ingesteld voordat u sleutels kunt maken.**Opmerking:** In de multi-context-modus moet u de RSA-toetsen voor elke context genereren. Bovendien worden crypto opdrachten niet ondersteund in de systeemcontextmodus.

3. Specificeer de hosts verbinding met het beveiligingsapparaat te maken.Deze opdracht specificeert het bronadres, netmask en interface van de host(s) die mogen worden aangesloten bij SSH. Het kan meerdere keren zijn ingevoerd voor meerdere hosts, netwerken of interfaces. In dit voorbeeld, wordt één gastheer binnen en één gastheer op de buitenkant toegestaan.

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. **Optioneel:** Standaard staat het security apparaat zowel versie 1 als versie 2 toe. Voer deze opdracht in om de verbindingen tot een bepaalde versie te beperken: pix(config)# ssh version

Opmerking: version_number kan 1 of 2 zijn.

5. **Optioneel:** De standaardinstelling is dat SSH-sessies worden gesloten na vijf minuten van inactiviteit. Deze tijdelijke versie kan worden ingesteld op een duur van tussen de 1 en 60 minuten.

pix(config)#ssh timeout minutes

Hoe een SSH-client wordt gebruikt

Geef de gebruikersnaam en het inlogwachtwoord op van de PIX 500 Series security applicatie terwijl u de SSH-sessie opent. Wanneer u een SSH-sessie start, wordt er een punt (..) weergegeven op de beveiligingswasmachineconnector voordat de SSH-gebruikersverificatiemelding wordt weergegeven:

hostname(config)# .

De weergave van de punt heeft geen invloed op de functionaliteit van SSH. De stip verschijnt op de console wanneer een server key gegenereerd wordt of wanneer een bericht gedecrypteerd wordt met privé toetsen tijdens SSH-sleuteluitwisseling voordat er gebruikersverificatie plaatsvindt. Deze taken kunnen tot twee minuten of langer duren. Het punt is een voortgangsindicator die aangeeft dat het beveiligingsapparaat bezig is en niet heeft gehaakt.

SSH-versies 1.x en 2 zijn volledig verschillende protocollen en zijn niet compatibel. Download een compatibele client. Raadpleeg het gedeelte <u>Verkrijg een SSH-client</u> van <u>Advanced Configuration</u> voor meer informatie.

PIX-configuratie

Dit document gebruikt deze configuratie:

PIX-configuratie PIX Version 7.1(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, !-



Opmerking: Om toegang te krijgen tot de beheerinterface van de ASA/PIX met behulp van SSH, geeft u deze opdracht uit: SH 172.16.16.160 255.255.255 Beheer

Configuratie met ASDM 5.x

Voltooi deze stappen om het apparaat voor SSH te configureren met behulp van ASDM:

 Kies Configuratie > Eigenschappen > Apparaatbeheer > Gebruikersrekeningen om een gebruiker met ASDM toe te voegen.

C Home	Configuration Monitoring	Back Forward	Q Q Search Refresh	調 🢡 Save Halp		Cisco Systems
Hertaces Hertaces Securty Policy NAT Securty Policy Securty Policy NAT Securty Policy Securty Policy Secur	Configuration > Properties > Devi * * * * * * * * * * * * * * * * * * *	ice Administration > U Create entries in the user account privileg User Name enable_15 ciscouser	Ser Accounts PIX local user databa es 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
	PhCP Services PhCP Services PhCP Services PhCP Services PhCP Services PhCP Services		Apply	Rese	t	
			ciscouser	NA (2)	🖟 🔘 🔂 5/23/0	6 6:16:28 PM UTC

2. Kies Configuratie > Eigenschappen > Toegang tot apparaat > AAA Toegang > Verificatie om AAA-verificatie voor SSH met ASDM in te stellen.

den Home	Configuration Montoring	Back Forward	Q Q Search Refre	sh Save	? Неір	Cisco Systems
Home Interfaces Security Policy NAT Security Policy	Configuration Montoring	Back Forward Device Access > AAA Ac Require authentication Enable authentication Enable authentication Require authentication Require authentication Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable Require authentication Enable	Search Refre cose = Authenticatio inization/Accounting Authorization don for administration intication to allow us Server Group: Server Group: Server Group: Server Group: Server Group:	sh Save	Help PIX. mode command T I Use L annections T I Use L I I Use L I I I Use L I I I I I I I I I I I I I I I I I I I	CAL when server group fails OCAL when server group fails OCAL when server group fails OCAL when server group fails OCAL when server group fails
Device configura	ation loaded successfully		ciscouse	r NA (2)	- -	

 Kies Configuratie > Eigenschappen > Apparaatbeheer > Wachtwoord om het Telnetwachtwoord met ASDM te wijzigen.

Home C	Sonfiguration Monitoring	Sack Forward Search Refresh Save Help	CISCO SYSTEMS
Interfaces Security Policy NAT Security Policy NAT Security Routing Clobel Objects Properties	Configuration > Properties > D Startup Wizard AAA Setup AAA	Password Change the prolifeged mode and Tellnet passwords. Enable Password Change the prolifeged mode password. This is also the password to log into Cid Pessword: New Password: Confirm New Password: Old Password: Old Password: New Password: Confirm New Password: Confirm New Password:	D ASDM.
Device configurati	ion loaded successfully.	ciscouser 🛛 NA (2) 🛛 🛃 🗧 🖯	i/23/06 6:30:38 PM UTC

4. Kies **Configuratie > Eigenschappen > Certificaat > Belangrijkste paneel**, klik op **Toevoegen** en gebruik de standaardopties die worden weergegeven om dezelfde RSA-toetsen met ASDM te

genereren.



5. Kies Configuratie > Eigenschappen > Toegang tot apparaat > Secure Shell om ASDM te gebruiken om hosts te specificeren die zijn toegestaan om verbinding te maken met SSH en om de versie- en uitwijkopties te specificeren.

Same a	Configuration Monitoring	Back Forward Searc	h Refresh Save	? Helip	CISCO SYSTEMS
Herfaces Security Policy NAT Security Policy NAT Security NAT Security Routing Clobal Objects Clobal Objects	Configuration > Properties > D Configuration > Properties > Properties > D Configuration > Properties > Properties > Properties > D Configuration > Properties > Prop	evice Access - Secure Shell Secure Shell Allowed SSH Version(s): Specify the addresses of al using Secure Shell (SSH). Interface inside outside	I hosts/networks which are I hosts/networks which are IP Address 172.18.1.1 10.1.1.2	eout 60 minute allowed to access the PIX Mask 255 255 255 255 255 255 255 255	s Add Edit Delete
	URL Filtering		Apply	Reset	
Device configurat	lion loaded successfully.		ciscouser NA (2)	🚽 🔕 🔒	5/23/08 6:37:58 PM UTC

6. Klik op **Bestand > Configuratie opslaan in van flitser** om de configuratie op te slaan.

🚰 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 Pa	ब्दू acket Tracer	(C Refre
Save Running Configuration to Flash	istration > E /Configuratio	300t Image/C n	onfigur:
Save Running Configuration to TFTP Server Save Running Configuration to Standby Unit Save Internal Log Buffer to Flash Print	onfiguration hfigure boot i the boot sys first image ir	images from ar stem. Only one n the list.) externa TFTP bo
Clear Internal Log Buffer	loot Order		
Exit	1	disk0:/pix722	l.bin
VPN	-		

Configuratie met ASDM 6.x

Voer de volgende stappen uit:

1. Kies Configuratie > Apparaatbeheer > Gebruikers/AAA > Gebruikersrekeningen om een gebruiker met ASDM toe te

VC	egen.						
Ċ	Home 🖧 Configuration 🔯 Monitori	ing 🔒 Save 🔇 Re	efresh 🕜 Back 🕥 Form	ed 🦹 Help			cisco
	Device Management 🗗 🗭 🛪	Configuration > De	vice Management > Users/	AAA > User Accounts			
evice Ust	8-12 Management Access 8-23 System Image/Configuration	Create entries in t	he ASA local user database.				
Ô,	E High Availability	Command authoriz	ation must be enabled in order	for the user account privileges	to be enforced. To enable	command authorization, go to	Authorization.
	AAA Server Groups	go to <u>Authenticatio</u>	n console commands must be en <u>m</u>	abled in order for certain acce	ess restrictions to be enrorce	d, To enable AAA authenticat	ion command
	- AAA Access	Username	Privlege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add
	- Dynamic Access Policies	ssluser1	2	Ful	Inherit Group Policy	Inherit Group Policy	
	E Cartificata Management	enable_15	15	rul	N/A	N/A	Edit
	E-1 DHCP						Delete
	申_課 DNS						
	🖲 - 🐻 Advanced						
	A Device Setup						
	Frend						
	Remote Access VPN						
	Sterto-Site VPN						
	Device Management						
				Αρρίχ	Reset		
				<admin></admin>	15 😡	🍻 🔂 3/21	/08 10:10:29 PM 15T

 Kies Configuratie > Apparaatbeheer > Gebruikers/AAA > Toegang > Verificatie om AAAverificatie voor SSH met ASDM in te stellen.

G) Home 🦓 Configuration 🔯 Monitorin	ng 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🢡 Help
	Device Management 🗗 🖗 🗙	Configuration > Device Management > Users/AAA > AAA Access > Authentication
evice List	E - P Management Access E - System Image/Configuration	Authentication Authorization Accounting
Ď	E- Wigh Availability	Enable authentication for administrator access to the ASA.
	AAA Server Groups	Require authentication to allow use of privileged mode commands
	Authentication Prompt	Enable Server Group: LOCAL 💌 🗖 Use LOCAL when server group fails
	- 🏰 Dynamic Access Policies	Require authentication for the following types of connections
	- 🚮 User Accounts	HTTP/ASDM Server Group: LOCAL V Lise LOCAL when server group fails
	B-1 DHCP	Serial Server Group: LOCAL 💌 🗖 Use LOCAL when server group fails
	E-B Advanced	Server Group: LOCAL T Lise LOCAL when server group fails
		Teinet Server Group: LOCAL 💌 🗖 Use LOCAL when server group fails
	Device Setup	
	Frewal	
	Remote Access VPN	
	Ske-to-Ske VPN	
	Device Management	Apply Reset
	,	<admin> 15 🔯 🚔 🔒</admin>

3. Kies **Configuratie > Instellen apparaat > Naam/wachtwoord van het apparaat** om het Telnetwachtwoord met ASDM te wijzigen.

S) Home 🗞 Configuration 🔯 Monitorin	ng 🔄 Save 🔇 Refres	h 🔇 Back 🔘 Forward	🥐 Неір			
	Device Setup _ 0 ×	Configuration > Device	Setup > Device Name/Pa	ssword			
eLis	3 Startup Wizard	Hostname and Domain Nar	ne				
Devk	E-++++ Routing	Hostname:	ciscoasa				
	Device Name/Password System Time	Domain Name:	default.domain.invalid				
		Enable Password					
		Change the privilege	ed mode password.				
		Old Password:					
		New Pessword:					
		Confirm New Password:					
		Telnet Password					
		Change the passwo	rd to access the console of the	security appliance.			
		Old Password:					
		New Password:					
		Confirm New Password:					
	A Device Setup						
	Firewal						
	Remote Access VPN						
	Ste-to-Site VPN						
	Device Management						
	*			Apply	Reset		
				<admin.< th=""><th>> 15</th><th>😡 🍻</th><th>6</th></admin.<>	> 15	😡 🍻	6

4. Kies **Configuratie > Apparaatbeheer > Certificaatbeheer > Identity Certificaten**, klik op **Toevoegen** en gebruik de standaardopties die worden weergegeven om dezelfde RSAtoetsen met ASDM te

Device Management @ Q × (Configuration > Device Manag	ement > Certificate Manage	ement > Identity Co	ertificates		
- A SNMP	Issued To	Issued By	Expiry	Date	Usage	Add
Management Access Ruk System Image/Configuration						Show Dete
- 👰 Activation Key	ili Add Identity Certificate			x		Delate
- State Unage/Configuratio						
+)- 🤗 High Availability	Import the identity certified	ficate from a file:				Export
E- Cogong	Decryption Passphrase:					Instal
🕀 🔂 Certificate Management	File to Import From:		Browse			
- An CA Certificates	Add a new identity certil	ficate:				
⊒- 💕 ОНСР	Fare Daire	-Defe & PSI-Ver/2	T Show	New		
- 🎁 DHCP Relay	Noy For I	<pre>sberauk+cover.ey></pre>	· Snow	New		
	Certificate Subject DN:	CN=ciscoasa	Select			
E- 🐻 Advanced	Generate self-signed	d certificate				
- ARP Static Table	🖂 Act es local certi	ficate authority and issue dynas	ric certificates to TLS-	Proxy		
HTTP Redirect					given interface. You can gr	a to <u>SSL Settings</u>
- Westerv Metrics				Advanced		
A Device Setup	Add Certif	icate Cancel	Help			
Frewal					I	
Remote Access VPN						
Ske-to-Ske VPN						

5. Klik onder Een nieuw identiteitsbewijs toevoegen op Nieuw om een standaardtoetsenbord

toe te voegen als dit niet bestaat. Klik vervolgens op **Generate Now**.

Device Management 🗗 🤉 😕 Co	nfiguration > Device Manager	nent > Certificate Managemen	t > Identity Certificates		
E- 💕 Management Access					
System Image/Configuration High Availability	Essued To	Issued By	Expiry Date	Usage	Add
E- 🔄 Logging					Show Octai
AAA Server Groups	🚺 Add Identity Certificate			×	Delete
- Autonencication Prompt	C Import the identity certification	ate from a file:			Export
- Dynamic Access Policies - Dr. User Accounts	Decryption Passphrase:				Instal
Certificate Management	File to Import From:		Browse		
- 2 CA Certificates	Add a new identity certification	ate:			
B DHCP	Key Pair:	Chefault-RSA-Keyo	Show News		
Advanced	Card Education				
	Add Key Pair		×		
	Name: 🛈 Use o	default key pair name			
	C Ente	r new key pair name:			to TTL Collinson
	Size: 1024	*	t	given incerrace, rou can g	0 00 <u>201 5900 05</u>
	Usage: 💽 Gene	ral purpose 🕜 Special			
Device Setup					
Frewal	Generate	Now Cancel	Help		
Site-to-Site VPN					
Device Management					

6. Kies Configuratie > Apparaatbeheer > Toegang > Opdrachtlijn (CLI) > Secure Shell (SSH) om ASDM te gebruiken om hosts te specificeren die toegang hebben tot SSH en om de versie- en tijdelijke opties te

specificeren.



7. Klik op **Opslaan** boven in het venster om de configuratie op te slaan.

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 >
/ice List	Management Access ASDM/HTTPS	Allowed SSH Version(s): 1 & 2 💌 Timeout: 5

8. Wanneer gevraagd wordt de configuratie op flitser op te slaan, kies **Toepassen** om de configuratie op te slaan.

Telnet-configuratie

Om de toegang van het telnet aan de console toe te voegen en de ongebruikte tijd in te stellen, geeft u het **telnet** bevel in globale configuratiewijze uit. Telnet-sessies die gedurende vijf minuten stilstaand zijn, worden standaard door het security apparaat gesloten. Om de toegang van het telnet uit een eerder vastgesteld IP adres te verwijderen, gebruik de *geen* vorm van deze opdracht.

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}}

Met de opdracht **telnet** kunt u specificeren welke hosts toegang hebben tot de veiligheidswasconsole met telnet.

N.B.: U kunt telnet op alle interfaces naar het beveiligingsapparaat inschakelen. Het security apparaat dwingt echter wel om al het Telnet-verkeer naar de externe interface te beveiligen door IPsec. Om een Telnet-sessie naar de externe interface mogelijk te maken, moet u IPsec op de externe interface configureren om IP-verkeer op te nemen dat door het security apparaat gegenereerd wordt en telnet op de externe interface mogelijk te maken.

Opmerking: In het algemeen, als een interface met een beveiligingsniveau van 0 of lager dan een andere interface, dan staat PIX/ASA telnet aan die interface niet toe.

N.B.: Het wordt niet aanbevolen om via een Telnet-sessie toegang te krijgen tot het security apparaat. De authenticatie crediteureninformatie, zoals wachtwoord, wordt als duidelijke tekst verzonden. De Telnet server en de client communicatie gebeurt alleen met de duidelijke tekst. Cisco raadt aan SSH te gebruiken voor een meer beveiligde datacommunicatie.

Als u een IP-adres invoert, moet u ook een netmask invoeren. Er is geen standaardnetmask. Gebruik het subnetwerk masker van het interne netwerk niet. Het netwerkmasker is slechts een beetje masker voor het IP-adres. Om de toegang tot één IP-adres te beperken, gebruik 255 in elke octet; bijvoorbeeld 255 255 255 255 255 .

Als IPsec actief is, kunt u een onveilige interfacenaam opgeven, die normaal de externe interface is. U kunt ten minste de opdracht **crypto map** configureren om een interfacenaam te specificeren met de opdracht **telnet**.

Geef het wachtwoord uit opdracht om een wachtwoord in te stellen voor de toegang tot de console

van het telnet. De standaardinstelling is cisco. Geef de opdracht **who** uit om te zien welke IPadressen momenteel toegang hebben tot de beveiligingswasmachineconcern. Geef de opdracht **doden** uit om een actieve sessie van de Telnet-console te beëindigen.

Om een Telnet-sessie naar de interne interface mogelijk te maken, bekijkt u deze voorbeelden:

Voorbeeld 1

Dit voorbeeld maakt het alleen mogelijk dat de host 10.1.1.1 via telnet toegang krijgt tot de beveiligingswasmachineconnector:

pix(config)#telnet 10.1.1.1 255.255.255.255 inside
Voorbeeld 2

Dit voorbeeld geeft alleen toegang tot de netwerkconsole van 10.0.0.0/8 door telnet:

pix(config)#telnet 10.0.0.0 255.0.0.0 inside
Voorbeeld 3

In dit voorbeeld kunnen alle netwerken via telnet toegang krijgen tot de beveiligingswasmachineconcern:

pix(config)#**telnet** 0.0.0.0 0.0.0.0 inside

Als u de opdracht AAA met het sleutelwoord gebruikt, moet de toegang tot de Telnet-console met een authenticatieserver geauthentiseerd zijn.

N.B.: Als u de **AAA**-opdracht hebt ingesteld om verificatie van de toegang tot de Telnet-console van het security apparaat en de ingelogde inlogwachttijden van de console nodig te hebben, kunt u vanuit de seriële console toegang tot het security apparaat krijgen. Voer daartoe de gebruikersnaam voor het beveiligingsapparaat in en het wachtwoord dat is ingesteld met de opdracht **Wachtwoord** inschakelen.

Geef de opdracht voor **tijdelijke** installatie van telnet uit om de maximale tijd in te stellen die een sessie van telnet onklaar kan zijn voordat deze door het beveiligingsapparaat is uitgelogd. U kunt de **geen telnet** opdracht gebruiken met de opdracht **telnet timeout**.

Dit voorbeeld toont hoe om de maximum ongebruikte de zitting te veranderen:

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

Ondersteuning van SSH/telnet in ACS 4.x

Als u de RADIUS-functies bekijkt, kunt u de RADIUS voor de SSH-functie gebruiken.

Wanneer een poging wordt gedaan om toegang te krijgen tot het security apparaat met telnet, SSH, HTTP of een seriële console-verbinding en de verkeersovereenkomsten overeenkomen met een verificatieverklaring, vraagt het security apparaat om een gebruikersnaam en wachtwoord. Het stuurt deze aanmeldingsgegevens naar de RADIUS (ACS) server en verleent of ontkent CLItoegang op basis van de reactie van de server.

Raadpleeg het gedeelte <u>AAA-server en lokale database ondersteuning</u> van <u>AAA-servers en de</u> <u>lokale database</u> voor meer informatie.

Uw ASA security apparaat 7.0 heeft bijvoorbeeld een IP-adres nodig waarvan het security apparaat verbindingen accepteert, zoals:

hostname(config)#ssh source_IP_address mask source_interface

Raadpleeg het gedeelte <u>Toegang</u> van <u>SSH</u> tot <u>AAA-servers configureren en de lokale database</u> voor meer informatie.

Raadpleeg <u>PIX/ASA : Cut-through Proxy voor Network Access met behulp van TACACS+ en</u> <u>RADIUS Server Configuration Voorbeeld</u> voor meer informatie over het configureren van SSH/telnet-toegang tot PIX met ACS-verificatie.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

Debug SSH

Geef de opdracht debug ssh uit om de debugging van SSH aan te zetten.

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

Deze output laat zien dat de authenticatieaanvraag van host 10.1.1.2 (buiten tot PIX) naar "pix" succesvol is:

```
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
```

Als een gebruiker een verkeerde gebruikersnaam geeft, bijvoorbeeld, "pix1" in plaats van "pix", wijst de PIX Firewall de authenticatie af. Dit debug uitvoer toont de mislukte authenticatie:

```
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.
```

Op dezelfde manier, als de gebruiker het verkeerde wachtwoord verstrekt, deze debug uitvoer toont u de mislukte authenticatie.

pix# Device ssh opened successfully. SSH0: SSH client: IP = '10.1.1.2' interface # = 1SSH: 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.

Actieve SSH-sessies bekijken

Geef deze opdracht uit om het aantal SSH-sessies dat aangesloten is en de verbindingsstaat met PIX te controleren:

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

Kies **Bewaking > Eigenschappen > Apparaattoegang > Secure Shell sessies** om de sessies met ASDM te bekijken.

Bekijk de openbare RSA-toets

Geef deze opdracht uit om het openbare gedeelte van de RSA-toetsen op het security apparaat te bekijken:

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

Kies Configuratie > Eigenschappen > Certificaat > Belangrijkste paneel en klik op Details tonen om de toetsen RSA met ASDM te bekijken.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Hoe de RSA-toetsen uit de PIX te verwijderen

In bepaalde situaties, zoals wanneer u een upgrade van PIX-software uitvoert of de SSH-versie in de PIX wijzigt, moet u de RSA-toetsen verwijderen en opnieuw maken. Geef deze opdracht uit om de RSA-toets van de PIX te verwijderen:

pix(config)#crypto key zeroize rsa

Kies **Configuratie > Eigenschappen > Certificaat > Belangrijkste paneel** en klik op **Verwijderen** om RSA-toetsen met ASDM te verwijderen.

SSH-verbinding is mislukt

Foutbericht op PIX/ASA:

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

Het corresponderende foutbericht op de SSH-clientmachine:

Selected cipher type

Om dit probleem op te lossen, verwijdert en maakt u de RSA-toetsen opnieuw aan. Geef deze opdracht uit om het RSA-sleutelpaar van ASA te verwijderen:

ASA(config) #crypto key zeroize rsa

Geef deze opdracht uit om de nieuwe toets te genereren:

ASA(config) # crypto key generate rsa modulus 1024

Kan geen toegang krijgen tot ASA met SSH

Foutbericht:

Voltooi de volgende stappen om dit probleem op te lossen:

- 1. Of herladen de ASA of verwijderen alle SSH gerelateerde configuratie en de RSA toetsen.
- 2. Herstel de SSH-opdrachten en regenereer de RSA-toetsen.

Kan geen toegang tot secundaire ASA met SSH

Wanneer ASA in de failover-modus staat, is SSH niet mogelijk voor de stand-by ASA door de VPN-tunnel. Dit komt doordat het antwoordverkeer voor SSH de externe interface van de stand-by ASA neemt.

Gerelateerde informatie

- <u>Cisco PIX 500 Series security applicaties</u>
- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- <u>Cisco PIX-firewallsoftware</u>
- Opdrachtreferenties van Cisco Secure PIX-firewall
- <u>SSH-verbindingen configureren Cisco-routers en Cisco-connectors</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>