PIX/ASA 7.x: SSH/Telnet auf der internen und externen Schnittstelle - Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Konfigurieren Netzwerkdiagramm SSH-Konfigurationen Konfiguration mit ASDM 5.x Konfiguration mit ASDM 6.x **Telnet-Konfiguration** SSH/Telnet-Unterstützung in ACS 4.x Überprüfen **Debug-SSH** Aktive SSH-Sitzungen anzeigen Öffentlichen RSA-Schlüssel anzeigen Fehlerbehebung Entfernen der RSA-Schlüssel aus dem PIX SSH-Verbindung fehlgeschlagen Zugriff auf ASA mit SSH nicht möglich Zugriff auf sekundäre ASA mit SSH nicht möglich Zugehörige Informationen

Einführung

Dieses Dokument enthält eine Beispielkonfiguration von Secure Shell (SSH) auf den Innen- und Außenschnittstellen der Cisco Series Security Appliance Version 7.x und höher. Bei der Remote-Konfiguration der Security Appliance mit der Befehlszeile wird Telnet oder SSH verwendet. Da Telnet-Kommunikation in Klartext mit Kennwörtern versendet wird, wird SSH dringend empfohlen. SSH-Datenverkehr wird in einem Tunnel verschlüsselt und schützt so Kennwörter und andere Konfigurationsbefehle vor Abfangen.

Die Sicherheits-Appliance ermöglicht zu Verwaltungszwecken SSH-Verbindungen mit der Sicherheits-Appliance. Die Sicherheits-Appliance ermöglicht maximal fünf gleichzeitige SSH-Verbindungen für jeden <u>Sicherheitskontext</u>, sofern verfügbar, und ein globales Maximum von 100 Verbindungen für alle Kontexte zusammen.

In diesem Konfigurationsbeispiel wird die PIX Security Appliance als SSH-Server angesehen. Der Datenverkehr von SSH-Clients (10.1.1.2/24 und 172.16.1.1/16) zum SSH-Server wird verschlüsselt. Die Sicherheits-Appliance unterstützt die SSH-Remote-Shell-Funktionalität der SSH-Versionen 1 und 2 und unterstützt DES- (Data Encryption Standard) und 3DES-Verschlüsselungen. SSH-Versionen 1 und 2 sind unterschiedlich und nicht interoperabel.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco PIX Firewall Software, Version 7.1 und 8.0.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: SSHv2 wird in PIX/ASA Version 7.x und höher unterstützt und in Versionen vor 7.x nicht unterstützt.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance der Serie ASA 5500 mit den Softwareversionen 7.x und höher verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Jeder Konfigurationsschritt enthält die erforderlichen Informationen für die Verwendung der Befehlszeile oder des Adaptive Security Device Manager (ASDM).

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



SSH-Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- <u>SSH-Zugriff auf die Sicherheits-Appliance</u>
- <u>Verwenden eines SSH-Clients</u>
- PIX-Konfiguration

SSH-Zugriff auf die Sicherheits-Appliance

Gehen Sie wie folgt vor, um den SSH-Zugriff auf die Sicherheits-Appliance zu konfigurieren:

1. SSH-Sitzungen erfordern für die Authentifizierung immer einen Benutzernamen und ein Kennwort. Es gibt zwei Möglichkeiten, diese Anforderung zu erfüllen.Konfigurieren Sie einen Benutzernamen und ein Kennwort, und verwenden Sie AAA:Syntax: pix(config)#username username password password pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}

Hinweis: Wenn Sie eine TACACS+- oder RADIUS-Servergruppe für die Authentifizierung verwenden, können Sie die Sicherheits-Appliance so konfigurieren, dass sie die lokale Datenbank als Fallbackmethode verwendet, wenn der AAA-Server nicht verfügbar ist. Geben Sie den Namen der Servergruppe und anschließend LOCAL an (LOCAL ist Groß- und Kleinschreibung zu beachten). Es wird empfohlen, in der lokalen Datenbank denselben Benutzernamen und dasselbe Kennwort wie beim AAA-Server zu verwenden, da bei der Aufforderung zur Sicherheitsappliance nicht angegeben wird, welche Methode verwendet wird.**Hinweis:** Beispiel:

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

Hinweis: Alternativ können Sie die lokale Datenbank als Hauptauthentifizierungsmethode ohne Fallback verwenden. Geben Sie dazu nur LOCAL ein.Beispiel: pix(config)#aaa authentication ssh console LOCAL

ODERVerwenden Sie den Standardbenutzernamen **pix** und das Telnet-Standardkennwort von **cisco**. Sie können das Telnet-Kennwort mit dem folgenden Befehl ändern: pix(config) **#passwd** password

Hinweis: In dieser Situation kann der Befehl **password** verwendet werden. Beide Befehle tun dasselbe.

2. Generieren Sie ein RSA-Schlüsselpaar für die PIX-Firewall, das für SSH erforderlich ist: pix(config)#crypto key generate rsa modulus modulus_size

Hinweis: Die modulus_size (in Bits) kann 512, 768, 1024 oder 2048 sein. Je größer die Modulusgröße, desto länger dauert die Generierung des RSA-Schlüsselpaars. Der Wert von 1024 wird empfohlen.**Hinweis:** Der Befehl zum <u>Generieren eines RSA-Schlüsselpaars</u> unterscheidet sich für PIX-Softwareversionen vor 7.x. In früheren Versionen muss ein Domänenname festgelegt werden, bevor Schlüssel erstellt werden können.**Hinweis:** Im Mehrfachkontextmodus müssen Sie die RSA-Schlüssel für jeden Kontext generieren. Darüber hinaus werden Krypto-Befehle im Systemkontextmodus nicht unterstützt.

- 3. Geben Sie die Hosts an, die eine Verbindung zur Sicherheits-Appliance herstellen dürfen.Mit diesem Befehl werden die Quelladresse, die Netzmaske und die Schnittstelle des Hosts angegeben, der bzw. die eine Verbindung mit SSH herstellen darf. Sie kann für mehrere Hosts, Netzwerke oder Schnittstellen mehrfach eingegeben werden. In diesem Beispiel ist ein Host auf der Innenseite und ein Host auf der Außenseite zulässig. pix(config)#ssh 172.16.1.1 255.255.255 inside pix(config)#ssh 10.1.1.2 255.255.255 outside
- 4. **Optional:** Standardmäßig ist die Sicherheits-Appliance für SSH-Version 1 und -Version 2 zulässig. Geben Sie diesen Befehl ein, um Verbindungen auf eine bestimmte Version zu beschränken:

pix(config)# ssh version

Hinweis: Die Versionsnummer kann 1 oder 2 sein.

5. **Optional:** Standardmäßig werden SSH-Sitzungen nach fünf Minuten Inaktivität geschlossen. Diese Zeitüberschreitung kann so konfiguriert werden, dass sie 1 bis 60 Minuten lang andauert.

pix(config)#ssh timeout minutes

Verwenden eines SSH-Clients

Geben Sie beim Öffnen der SSH-Sitzung den Benutzernamen und das Anmeldekennwort der Sicherheitslösung der Serie PIX 500 an. Wenn Sie eine SSH-Sitzung starten, wird in der Konsole der Sicherheitslösung ein Punkt (.) angezeigt, bevor die Aufforderung zur SSH-Benutzerauthentifizierung angezeigt wird:

hostname(config)# .

Die Anzeige des Punkts hat keinen Einfluss auf die Funktionalität von SSH. Der Punkt wird an der Konsole angezeigt, wenn ein Serverschlüssel generiert oder eine Nachricht mit privaten Schlüsseln entschlüsselt wird, bevor die Benutzerauthentifizierung erfolgt. Diese Aufgaben können bis zu zwei Minuten oder länger dauern. Der Punkt ist eine Fortschrittsanzeige, die überprüft, ob die Sicherheits-Appliance besetzt ist und nicht geklingelt hat.

SSH-Versionen 1.x und 2 sind völlig unterschiedliche Protokolle und nicht kompatibel. Laden Sie einen kompatiblen Client herunter. Weitere Informationen finden Sie im Abschnitt <u>SSH-Client</u> im Abschnitt <u>Erweiterte Konfigurationen</u>.

In diesem Dokument wird diese Konfiguration verwendet:

PIX-Konfiguration 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, !-



Hinweis: Führen Sie folgenden Befehl aus, um über SSH auf die Verwaltungsschnittstelle von ASA/PIX zuzugreifen: SSH 172.16.16.160 Verwaltung 255.255.255.255

Konfiguration mit ASDM 5.x

Gehen Sie wie folgt vor, um das Gerät für SSH mithilfe von ASDM zu konfigurieren:

 Wählen Sie Configuration > Properties > Device Administration > User Accounts (Konfiguration > Eigenschaften > Geräteverwaltung > Benutzerkonten), um einen Benutzer mit ASDM hinzuzufügen.

💰 Home	Configuration Monitoring E	Sack Forward	Q Q Search Refresh	調 🦓 Save Help		CISCO SYSTEMS
Herfaces Security Policy NAT Security Policy NAT Security NAT Security Routing Global Objects Forperties	Configuration > Properties > Devic Configuration > Properties > Device Startup Wizard AAA Setup AAA Setup	Le Administration > Us Le Administration > Us Jser Accounts Create entries in the user account privileg User Name enable_15 ciscouser	PIX local user databa es to be enforced. To Privilege (Level) NA (15) NA (2)	se. Command author enable command aut VPN Group Policy NA DiftGrpPolicy	tzation must be enable thortzation, go to <u>Autho</u> VPN Group Lock N/A Inherit Group Po	d in order for the tzetion. Add Edit Delete
	Control Contents Content Co		Apply	Rese	t	

2. Wählen Sie **Configuration > Properties > Device Access > AAA Access > Authentication**, um die AAA-Authentifizierung für SSH mit ASDM einzurichten.

G Home	Configuration Ma	() Initoring	Back Forward	Q (Search Re	rresh Save	?	Cisco Systems
Interfaces Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy Properties	Configuration > Pi Configuration > Pi Startup Wiz Configuration > Pi Startup Wiz Configuration > Pi Startup Wiz Configuration > Pi AAA Setup Configuration > Pi AAA Setup Configuration > Pi AAA Setup Configuration > Pi Configuration	roperties > Dev roperties > Dev ard ng e ess ess ASDM Shell ninistration rices t rics eue Server 15	Authentication Authori Authentication Authori Authentication Authori Authentication Authori Require authenticati Require authen Enable Require authen Enable Require authen Enable Require authen Enable Require authen Enable Require authen Enable Require authen Enable	search Free ses - Authentica ization/Accountin authorization) an for administr toation to allow Server Group: Server Group: Server Group: Server Group:	Accounting Accounting ator access to th use of privileged LOCAL LOCAL LOCAL LOCAL	Page e PIX . I mode commar P Use connections P Use P Use P Use P Use P Use	Inds LOCAL when server group fails LOCAL when server group fails LOCAL when server group fails LOCAL when server group fails LOCAL when server group fails
Device configura	tion loaded success	sfully		ciscou	ser NA (2)		B 5/23/06 6:24:28 PM UTC

3. Wählen Sie Configuration > Properties > Device Administration > Password (Konfiguration > Eigenschaften > Geräteverwaltung > Kennwort), um das Telnet-Kennwort mit ASDM zu ändern.

G Home	Configuration Monitoring	Sack Forward Search Refresh Save Help	ISCO STATEMA
Interfaces Security Policy NAT VPN Routing Global Objects	Configuration > Properties > D	Image: Second	
Device configura	ation loaded successfully.	ciscouser NA (2) 🛃 🔂 5/23/06 6:	30:38 PM UTC

4. Wählen Sie Konfiguration > Eigenschaften > Zertifikat > Schlüsselpaar, klicken Sie auf Hinzufügen, und verwenden Sie die angezeigten Standardoptionen, um die gleichen RSA-Schlüssel mit ASDM zu generieren.



5. Wählen Sie Configuration > Properties > Device Access > Secure Shell, um ASDM zum Festlegen von Hosts zu verwenden, die eine Verbindung mit SSH herstellen dürfen, und um die Version und die Timeout-Optionen anzugeben.

		n Nellesh Save	Helip	tilltutilltu
anation > Properties > De The Properties > De Startup Wizard AAA Setup Anti-Spoofing ARP Auto Update Certificate Device Access AAA Access AA	exice Access - Secure Shell Secure Shell Allowed SSH Version(s): Specify the addresses of all using Secure Shell (SSH). Interface inside outside	Time I hosts/networks which are IP Address 172.16.1.1 10.1.1.2	out 60 minutes allowed to access the PIX Mask 255 255 255 255 255 255 255 255	Add Edit Delete
TCP Options Timeouts URL Filtering		Apply	Reset	

6. Klicken Sie auf **Datei > Running Configuration in Flash speichern**, um die Konfiguration zu speichern.

🞼 Cisco ASDM 5.2 for ASA - 172.16.3	3.1			
File Options Tools Wizards Help				
Refresh ASDM with the Running Config Reset Device to the Factory Default Co Show Running Configuration in New W	uration on the Device	l Packe		Refre
Save Running Configuration to Flash	Istrat /Confi	ion > Boot iguration—	image/Co	oniigur:
Save Running Configuration to TFTP Se Save Running Configuration to Standby Save Internal Log Buffer to Flash Print	rver Unit nfigur the b	ration e boot imag oot system image in the	es from an . Only one T e list.	externa FTP bo
Clear Internal Log Buffer	loot O	rder		
Exit	1	dis	sk0:/pix722.	bin
VPN	je/Config pt			

Konfiguration mit ASDM 6.x

Gehen Sie wie folgt vor:

1. Wählen Sie **Configuration > Device Management > Users/AAA > User Accounts**, um einen Benutzer mit ASDM

Here Configuration Provide Management Provide Provide	ninzuzutugen.					-	
	🚳 Home 🚳 Configuration 🔯 Monitori	ing 🔚 Save 🔇 Re	fresh 🕓 Back 🔘 Form	ed 💡 Help			CISCO
And Access Username Privilege Levil (Role) Access Redrictions VPN Group Doley VPN Group Lock Acd Confricts Planagement 2 Full ->>heit Group Poley VPN Group Lock Acd Confricts Planagement 2 Full ->>heit Group Poley VPN Group Lock Acd Confricts Planagement 2 Full ->>heit Group Poley VPN Group Lock Acd Confricts Planagement 2 Full N/A N/A N/A Dalate Confricts Planagement 2 Full N/A N/A N/A Dalate Confricts Planagement 2 Confrict State Management Confrict	Device Management P × P Management P × P Management Access System Image/Configuration P High Availability P Logging P Logging P AAA Server Groups A Access	Configuration > Der Create entries in th Command authoriz AAA authentication go to Authentication	vice Management > Users/ te ASA local user database, ation must be enabled in order in tonsole commands must be en the	<pre>/AAA > User Accounts for the user account privileges abled in order for certain acce</pre>	s to be enforced. To enable ess restrictions to be enforce	command authorization, go to ed. To enable AAA authentica	Authorization.
Image: Access Policies Image: Access Policies Image: Prevention Image: Access Policies Image: Policies Image: Access Policies <t< td=""><td>- AAA Access</td><td>Username</td><td>Privilege Level (Role)</td><td>Access Restrictions</td><td>VPN Group Policy</td><td>VPN Group Lock</td><td>Add</td></t<>	- AAA Access	Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add
igg Excercised Management	- Dynamic Access Policies	ssluser1	2	Ful	Inherit Group Policy	Inherit Group Policy	
Image: Second	User Accounts	enable_15	15	rul	N/A	N/A	Edit
Advanced Advanced Device Setup Device Setup Device Setup Device Setup Device Setup Device Setup Device Management Apriv Reset cadmin> 15	R-M DHCP						Delete
Perice Setup Perice Management	自一是 DNS						
Rest Sprive Setup Sprive Setup Sprive Access VPN Sprive Rest Apply Rest	E-B Advanced						
Image: Setup							
Image: Series Setup Image: Series Example Image: Series Example Image: Series VPN Series VPN							
Image: Service Setup Image: Service Setup Image: Service Setup Image: Service Management							
Image: Sector Secup Image: Sector Sec VPN Image: Sector S							
Image: Set up Image: Firewal Image: Set to Set VPN Image: Set VPN							
Image: Set up Image: Set up <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>							
Image: Service Secup Image: Type and Image: Service Secup Image: Service Secup Image: Secure Secup Image: Secure Secure Image: Secure Secure <	9						
Image: Specific Access VPN Image: Specific Management Imagement Image: Spec	Service secup						
Remote Access VPN Reset Perfor Reset	Frend .						
	Remote Access VPN						
	Sterto-Site VPN						
	El anno Maria						
	Device Management				1		
sadmin> 15 😡 🛱 🔂 3/21/00 10:10:29 PM 19	»,			Αρρίγ	Reset		
				<admin></admin>	15 😡	😹 🛛 🙆 3/2	1/00 10:10:29 PM 15

2. Wählen Sie **Configuration > Device Management > Users/AAA > AAA Access > Authentication** aus, um die AAA-Authentifizierung für SSH mit ASDM einzurichten.

Imagement Access Imagement Access Protoc	Device Management D ¹ 4 ×	Configuration > Device Management > Users/AAA > AAA Access > Authentication
Image: Index Availability Image: Inde	E- Anagement Access E-26 System Image/Configuration	Authentication Authorization Accounting
Produbers/AAA Produbers/AAA <td< th=""><th> B-</th><th>Enable authentication for administrator access to the ASA.</th></td<>	 B-	Enable authentication for administrator access to the ASA.
Advances Advances Advances Advances Optimic Access Policies Optimic Access Optimic Acces Optimic Access Optimic Access	AAA Server Groups	Require authentication to allow use of privileged mode commands
Pynamic Access Policies Current Counts	Authentication Prompt	Enable Server Group: LOCAL C Use LOCAL when server group fails
Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL ▼ Use LOCAL when server group fails Image: Server Group: LOCAL	Dynamic Access Policies	Require authentication for the following types of connections
B- P DHCP B- DNS B- Advanced Image: Senial Server Group: Image: Image	E- Certificate Management	HTTP/ASDM Server Group: LOCAL V Use LOCAL when server group fails
B. Wanced Image: Server Group: Image: Server Group: Server Group: Server Group: Server Group: Got All when server group Fails: Image: Server Group: Server Group: Server Group: Server Group: Got All when server group Fails: Image: Server Server Group: Server Group: Server Group: Server Group: Got All when server group Fails: Image: Server Server Group: Server Group: Serv	문- 💕 DHCP 문- 📲 DNS	Serial Server Group: LOCAL V Use LOCAL when server group fails
Image: Server Group: Use LOCAL when server group fails Image: Device Setup Image: Prevail Image: Remote Access VPN Image: Ske-to-Ske VPN	🗄 - 🐻 Advanced	Server Group: LOCAL 💌 🥅 Use LOCAL when server group fails
Pevice Setup		Teinet Server Group: LOCAL V Dise LOCAL when server group fails
Periode Setup Proval		
Service Setup Service Setup Frewal Service Access VPN Service Management		
Image: Second		
Image: Setup		
Image: Second		
Image: Second	Levice Setup	
Remote Access VPN Reto-Ske VPN Device Management	Frewal	
Ske-to-Ske VPN Device Management Apply Reset	Remote Access VPN	
Device Management Apply Reset	Ske-to-Ske VPN	
Apply Reset	Device Management	
		Aurty David

3. Wählen Sie Configuration > Device Setup > Device Name/Password (Konfiguration > Geräteeinrichtung > Gerätename/Kennwort), um das Telnet-Kennwort mit ASDM zu ändern.

đ) Home 🍓 Configuration 🔯 Monitorin	ng 🕞 Save 🔇 Refres	h 🔇 Back 🔘 Forward	🥐 Небр		
	Device Setup Q ×	Configuration > Device	Setup > Device Name/Pa	ssword		
eLis		Hostname and Domain Nar	ne			
Devk	H-++++ Routing	Hostname:	ciscoasa			
	Device Name/Password System Time	Domain Name:	default.domain.invalid			
		Enable Password				
		Change the privilege	ed mode password.			
		Old Password:				
		New Password:				
		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></admin>	15	😡 🍻 🛛 🔒

4. Wählen Sie Konfiguration > Gerätemanagement > Zertifikatsverwaltung > Identitätszertifikate, klicken Sie auf Hinzufügen, und verwenden Sie die angegebenen Standardoptionen, um dieselben RSA-Schlüssel mit ASDM zu

appor	noron
YCHEI	
0	

SNMP Issued To Issued Dy Expiry Date Usage System Image(Configuration Activation Key Auto Update X	ncunkerrace						
System Image/Configuration System Image/Configuration Additionation Key Additionation Key Additionation Confidence Confidence Additionation Confidence Certificate Management Certificate Management Certificate Management Certificate Subject DN: CN=dscess Certificate Subject DN: CN=dscess Certificate Subject DN: CN=dscess Advenced A		Issued To	Issued By	Eq	piry Date	Usage	bbA [
Activation Key Advenced Activation Key Activation Key Activation Key Activation Key Activation Key Activation Key Activation	Configuration						Show De
Book Image/Configuratio High Availability Looging Users/AAA Certificate Management Certificates Certificates DHCP DHCP Relay DHCP Server Advanced Advanced Add Certificate Certificates Self-Signed certificate Add Certificate Certificates Add Certificate Cancel Heip	ley 💼 Add	i Identit <mark>y Certificate</mark>			×	1	Dead
Loging Lisers(AAA Certificate Management S. Certificates Mold a meni identity certificates DHCP Rainy DHCP Server DHCP Server DNS Advanced S. Advanced Add Certificate Cancel Heip	Configuratio	Import the identity certif	icate from a file:				Expo
Certificate Management CA Certificates CA Certificates CHOP CHOP CHOP <td></td> <td>Decryption Passphrase:</td> <td></td> <td></td> <td></td> <td></td> <td>Insta</td>		Decryption Passphrase:					Insta
C C Certificates C Add a new identity certificate C Add a new ide	agement	File to Import From:		Brawso	1		
PhOP Relay DHCP Relay DHCP Server DNS DHCP Server DNS Advanced	stes rtificates	Add a new identity certif	sate:		_		
Bolic Decision DNS Advanced Certificate Subject DN: Chi-ciscoesa Select Generate self-signed certificate Act es local certificate authority and issue dynamic certificates to TLS-Proxy given interface. You can go to SS Device Setup Add Certificate Cancel Heip		Key Pain:	<default-rsa-key></default-rsa-key>	* Show	New		
Advanced AAP Add Certificate Cancel Heip	er	Certificate Subject DN:	CN-ciscoasa	Select			
ARP Statk Table ARP Statk Table ARP Statk Table Act as local certificate authority and issue dynamic certificates to TLS-Proxy advanced Advanced Advanced Frewal Remote Access VPN		Cenerate celf-signed	, estificate		_		
Access VPN							
Advanced	atic Table ect	Actives local certain	score authority and issue of	mentic certificates to 1	LB-PYCKY		
Image: Setup Add Certificate Cancel Image: Setup Add Certificate Cancel Image: Setup Add Certificate Cancel Image: Setup Image: Setup Image: Setup	ates				Advanced	given interface. You can go	to <u>SSL Settin</u>
Add Certificate Cancel Help Add Certificate Cancel Help	ines 💌						
Evice Setup Add Certificate Cancel Hep		address	inter a const	1	1		
Remote Access VPN		Add Cerci	carcer Carcer	nep			
Eemate Access VPN						-	
×	/PN						
🖉 Ste to Ste VPN							
Device Management	ent						

5. Klicken Sie unter Neues Identitätszertifikat hinzufügen auf Neu, um ein standardmäßiges

Schlüsselpaar hinzuzufügen, falls es kein solches nicht gibt. Klicken Sie anschließend auf Jetzt

generieren.

Home 🖏 Configuration 🔯 Monitoring	Save 🔇 Refresh 🔾 Back 🗋	Forward 💡 Help			CISCO
Device Management at a × (Configuration > Device Management >	Certificate Management	> Identity Certificates		
Management Access					
E E System Image(Configuration	Issued To	Issued By	Expiry Date	Usage	Add
B- C Logging					Show Details
E-Gel Users/AAA			541		
- Authentication Prompt	Add Idenbity Certificate		X		Delete
- S AAA Access	C Import the identity certificate from	na file:			Export
- Dynamic Access Policies	Decryption Passobrase:				Instal
E- E Certificate Management	Fis to Impact Score		Desures		
- 2 CA Certificates	Harto Import Franc		DOWNER		
Pr P DHCP	Add a new identity certificate:				
E- B DNS	Key Pair: <defau< td=""><td>t-RSA-Keγ> ▼</td><td>Show New</td><td></td><td></td></defau<>	t-RSA-Keγ> ▼	Show New		
₽-103 Advanced	Cett Canada Kasa Bala				
	per Add Key Pair				
	Name: 🛈 Use default	key pair name			
	C Enter new k	ey pair name:			
	See. 1024	-		aiven interface. You can go b	o <u>SSL Settinos</u> to
	Jue. Ince		1		
	Usage: 🕐 General purp	oose C Special			
B Device Setup					
	Generate Now	Cancel	Help		
Firewall					
Kemote Access VPN					
California Statisti					
20 Tre-co-2re with					
Device Management					
*		Apple	y Reset		

6. Wählen Sie Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH), um ASDM zum Festlegen von Hosts zu verwenden, die eine Verbindung mit SSH herstellen dürfen, und um die Version- und Timeout-Optionen anzugeben.

C	Home 🔥 Configuration 📴 Monitorin	ng 🔚 Save 🔇 Refresh 🕻	Back 🔘 Forward 🦻 Help		CISCO
	Device Management 🗗 🤉 🗵	Configuration > Device Man	agement > Management Access > Command L	line (CLI) > Secure Shell (SSH)	
Device List	Anagement Access ADM/HTTPS BORGER CONTRACTOR Command Une (CLI)	Allowed SSH Version(s): 1 & Specify the addresses of all he	Timeout: 5 minutes	ing Secure Shell (SSH).	
	- De CLI Prompt	Interface	IP Address	Mask	Add
	Console Timeout	inside	10.77.241.142	255.255.255.255	
	Secure Shell (SSH)	outside	192.168.200.1	255.255.255.255	Edit
	Ele Arress				Delete
	- CMP				
	- 强 Nanagement Interface				
	- SNMP				
	12. 08 Sustem Image/ConBouration				
	FF W High Availability				
	E- 🔄 Logging				
	E 😥 Users (AAA				
	AAA Server Groups				
	- Authentication Prompt				
	- De Dynamic Access Policies				
	- 😥 User Accounts				
	HI- 🔤 Certificate Management				
	0				
	Device Setup				
	Firewall				
	Remote Access VPN				
	Ste-to-Site VPN				
	Device Management				
			Apply F	leset	

7. Klicken Sie oben im Fenster auf Speichern, um die Konfiguration zu

speichern.



8. Wenn Sie dazu aufgefordert werden, die Konfiguration im Flash-Speicher zu speichern, wählen Sie **Apply (Übernehmen)**, um die Konfiguration zu speichern.

Telnet-Konfiguration

Führen Sie den Befehl **telnet** im globalen Konfigurationsmodus aus, um der Konsole Telnet-Zugriff hinzuzufügen und die Leerlaufzeitüberschreitung festzulegen. Standardmäßig werden Telnet-Sitzungen, die fünf Minuten lang im Leerlauf verbleiben, von der Sicherheits-Appliance geschlossen. Um den Telnet-Zugriff von einer zuvor festgelegten IP-Adresse zu entfernen, verwenden Sie die *no*-Form dieses Befehls.

```
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}}
```

Mit dem **Telnet-**Befehl können Sie festlegen, welche Hosts mit Telnet auf die Konsole der Sicherheitsanwendung zugreifen können.

Hinweis: Sie können Telnet für die Sicherheits-Appliance an allen Schnittstellen aktivieren. Die Sicherheits-Appliance erzwingt jedoch, dass der gesamte Telnet-Datenverkehr zur externen Schnittstelle durch IPsec geschützt wird. Um eine Telnet-Sitzung mit der externen Schnittstelle zu aktivieren, konfigurieren Sie IPsec auf der externen Schnittstelle so, dass der von der Sicherheits-Appliance generierte IP-Datenverkehr enthalten ist, und aktivieren Sie Telnet auf der externen Schnittstelle.

Hinweis: Wenn eine Schnittstelle im Allgemeinen eine Sicherheitsstufe von 0 oder niedriger als jede andere Schnittstelle hat, lässt PIX/ASA Telnet für diese Schnittstelle nicht zu.

Hinweis: Es wird nicht empfohlen, über eine Telnet-Sitzung auf die Sicherheits-Appliance zuzugreifen. Die Anmeldeinformationen für die Authentifizierung, z. B. das Kennwort, werden als Klartext gesendet. Die Telnet-Server- und Client-Kommunikation erfolgt nur mit dem Klartext. Cisco empfiehlt, SSH für eine sicherere Datenkommunikation zu verwenden.

Wenn Sie eine IP-Adresse eingeben, müssen Sie auch eine Netzmaske eingeben. Es gibt keine Standard-Netzmaske. Verwenden Sie nicht die Subnetzmaske des internen Netzwerks. Die Netzmaske ist nur eine Bitmaske für die IP-Adresse. Um den Zugriff auf eine einzelne IP-Adresse zu beschränken, verwenden Sie in jedem Oktett 255. z. B. 255.255.255.255.

Wenn IPsec ausgeführt wird, können Sie einen unsicheren Schnittstellennamen angeben, der in der Regel die externe Schnittstelle ist. Sie können mindestens den Befehl **crypto map**

konfigurieren, um einen Schnittstellennamen mit dem Befehl telnet anzugeben.

Geben Sie den Befehl **password** ein, um ein Kennwort für den Telnet-Zugriff auf die Konsole festzulegen. Der Standardwert ist "cisco". Geben Sie den Befehl "**wer**" ein, um anzuzeigen, welche IP-Adressen derzeit auf die Konsole der Sicherheitslösung zugreifen. Führen Sie den Befehl **kill** aus, um eine aktive Telnet-Konsolensitzung zu beenden.

Um eine Telnet-Sitzung auf der internen Schnittstelle zu aktivieren, sehen Sie sich die folgenden Beispiele an:

Beispiel 1

In diesem Beispiel kann nur der Host 10.1.1.1 über Telnet Zugriff auf die Konsole der Sicherheits-Appliance erhalten:

pix(config)#telnet 10.1.1.1 255.255.255.255 inside
Beispiel 2

In diesem Beispiel kann nur das Netzwerk 10.0.0.0/8 über Telnet Zugriff auf die Konsole der Security Appliance erhalten:

pix(config)#telnet 10.0.0.0 255.0.0.0 inside
Beispiel 3

In diesem Beispiel können alle Netzwerke über Telnet auf die Konsole der Sicherheits-Appliance zugreifen:

pix(config)#telnet 0.0.0.0 0.0.0.0 inside

Wenn Sie den **aaa**-Befehl mit dem console-Schlüsselwort verwenden, muss der Telnet-Konsolenzugriff mit einem Authentifizierungsserver authentifiziert werden.

Hinweis: Wenn Sie den **aaa-**Befehl konfiguriert haben, um eine Authentifizierung für den Telnet-Konsolenzugriff der Sicherheitsappliance zu erfordern und die Konsolenanmeldung das Zeitlimit überschreitet, können Sie von der seriellen Konsole aus auf die Sicherheitsappliance zugreifen. Geben Sie dazu den Benutzernamen und das Kennwort der Security Appliance ein, die mit dem Befehl **enable password** festgelegt wurden.

Geben Sie den Befehl **telnet timeout** ein, um die maximale Zeit festzulegen, die eine Telnet-Konsolensitzung inaktiv sein kann, bevor sie von der Sicherheits-Appliance abgemeldet wird. Der Befehl **no telnet** kann mit dem Befehl **telnet timeout** nicht verwendet werden.

In diesem Beispiel wird veranschaulicht, wie die maximale Leerlaufdauer einer Sitzung geändert wird:

hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

SSH/Telnet-Unterstützung in ACS 4.x

Wenn Sie sich die RADIUS-Funktionen anschauen, können Sie den RADIUS für die SSH-Funktion verwenden.

Wenn versucht wird, über Telnet, SSH, HTTP oder eine serielle Konsolenverbindung auf die Security Appliance zuzugreifen und der Datenverkehr mit einer Authentifizierungsanweisung übereinstimmt, fordert die Security Appliance einen Benutzernamen und ein Kennwort an. Diese Anmeldeinformationen werden dann an den RADIUS-Server (ACS) gesendet, und der CLI-Zugriff wird basierend auf der Antwort des Servers gewährt oder verweigert.

Weitere Informationen finden Sie im Abschnitt <u>AAA-Server- und lokaler Datenbanksupport</u> zum Konfigurieren von AAA-Servern und der lokalen Datenbank.

Beispielsweise benötigt Ihre ASA Security Appliance 7.0 eine IP-Adresse, von der die Sicherheits-Appliance Verbindungen akzeptiert, z. B.:

hostname(config)#ssh source_IP_address mask source_interface

Weitere Informationen finden Sie im Abschnitt <u>Zulassen von SSH-Zugriff</u> unter <u>Konfigurieren von</u> <u>AAA-Servern und in der lokalen Datenbank</u>.

Weitere Informationen finden Sie unter <u>PIX/ASA: Cut-Through-Proxy für Netzwerkzugriff mit</u> <u>TACACS+ und RADIUS-Server-Konfigurationsbeispiel</u> für weitere Informationen zum Konfigurieren des SSH/Telnet-Zugriffs auf PIX mit ACS-Authentifizierung.

<u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Debug-SSH

Führen Sie den Befehl debug ssh aus, um das SSH-Debuggen zu aktivieren.

pix(config)#debug ssh

SSH debugging on

Diese Ausgabe zeigt, dass die Authentifizierungsanfrage von Host 10.1.1.2 (außerhalb von PIX) zu "pix" erfolgreich ist:

```
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:
        ser ver key generation
begin
   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
```

!--- 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

Wenn ein Benutzer einen falschen Benutzernamen angibt, z. B. "pix1" statt "pix", lehnt die PIX-Firewall die Authentifizierung ab. Diese Debug-Ausgabe zeigt die fehlgeschlagene Authentifizierung an:

```
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.
Wenn der Benutzer das falsche Kennwort bereitstellt, wird in diesem Debugausgang auch die
```

venn der Benutzer das falsche Kennwort bereitstellt, wird in diesem Debugausgang auch die fehlgeschlagene Authentifizierung angezeigt.

```
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.
```

Aktive SSH-Sitzungen anzeigen

Geben Sie diesen Befehl ein, um die Anzahl der mit dem PIX verbundenen SSH-Sitzungen und den Verbindungsstatus zu überprüfen:

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	

Wählen Sie **Monitoring > Properties > Device Access > Secure Shell Sessions** aus, um die Sitzungen mit ASDM anzuzeigen.

Öffentlichen RSA-Schlüssel anzeigen

Geben Sie diesen Befehl ein, um den öffentlichen Teil der RSA-Schlüssel auf der Sicherheits-Appliance anzuzeigen:

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

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

```
30819f300d06092a864886f70d010101050003818d0030818902818100c172f495f66c342c2ced37aa3442d812158c93131480dd967985ab1d7b92d95290f6958e9b5b0dd88c04396169184cd8fb951c19023347d6b3f93999ac2814950f442269b67328f64916b182e1534107590da2390fbefd387588887319196cde61aef1165c4bab03d081d5ddaf15ccc9ddb204c2b451e0f19ce0f3485b1d698b0203010001
```

Wählen Sie Konfiguration > Eigenschaften > Zertifikat > Schlüsselpaar aus, und klicken Sie auf Details anzeigen, um RSA-Schlüssel mit ASDM anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Entfernen der RSA-Schlüssel aus dem PIX

In bestimmten Situationen, z. B. wenn Sie die PIX-Software aktualisieren oder die SSH-Version im PIX ändern, müssen Sie möglicherweise RSA-Schlüssel entfernen und neu erstellen. Geben Sie diesen Befehl ein, um das RSA-Schlüsselpaar aus dem PIX zu entfernen:

pix(config)#crypto key zeroize rsa

Wählen Sie Konfiguration > Eigenschaften > Zertifikat > Schlüsselpaar aus, und klicken Sie auf Löschen, um RSA-Schlüssel mit ASDM zu entfernen.

SSH-Verbindung fehlgeschlagen

Fehlermeldung auf PIX/ASA:

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

Die entsprechende Fehlermeldung auf dem SSH-Client-Computer:

Selected cipher type

Um dieses Problem zu beheben, entfernen und erstellen Sie die RSA-Schlüssel erneut. Führen Sie diesen Befehl aus, um das RSA-Schlüsselpaar aus der ASA zu entfernen:

ASA(config)#crypto key zeroize rsa

Geben Sie diesen Befehl ein, um den neuen Schlüssel zu generieren:

Zugriff auf ASA mit SSH nicht möglich

Fehlermeldung:

ssh_exchange_identification: read: Connection reset by peer Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- 1. Laden Sie entweder die ASA neu, oder entfernen Sie alle SSH-bezogenen Konfigurationen und RSA-Schlüssel.
- 2. Konfigurieren Sie die SSH-Befehle neu, und generieren Sie die RSA-Schlüssel neu.

Zugriff auf sekundäre ASA mit SSH nicht möglich

Wenn sich ASA im Failover-Modus befindet, ist eine SSH-Verbindung zum Standby-ASA über den VPN-Tunnel nicht möglich. Der Grund hierfür ist, dass der Antwortverkehr für das SSH die externe Schnittstelle der Standby-ASA übernimmt.

Zugehörige Informationen

- <u>Cisco Security Appliances der Serie PIX 500</u>
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Konfigurieren von SSH-Verbindungen Cisco Router und Cisco Concentrators
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>