PIX/ASA 7.x ASDM: Einschränkung des Netzwerkzugriffs von VPN-Benutzern mit Remote-Zugriff

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Netzwerkdiagramm Konventionen Konfiguration des Zugriffs über ASDM Zugriff über CLI konfigurieren Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument enthält eine Beispielkonfiguration mit dem Cisco Adaptive Security Device Manager (ASDM), um festzulegen, auf welche internen Netzwerke Remote-Access-VPN-Benutzer hinter der PIX Security Appliance oder der Adaptive Security Appliance (ASA) zugreifen können. Sie können Remotezugriff-VPN-Benutzer auf die Bereiche des Netzwerks beschränken, auf die sie zugreifen möchten, wenn Sie:

- 1. Erstellen Sie Zugriffslisten.
- 2. Ordnen Sie sie Gruppenrichtlinien zu.
- 3. Ordnen Sie diese Gruppenrichtlinien Tunnelgruppen zu.

Unter Konfigurieren des Cisco VPN 3000 Concentrator für Blockierung mit Filtern und RADIUS-Filterzuweisung finden Sie weitere Informationen zu dem Szenario, in dem der VPN Concentrator den Zugriff von VPN-Benutzern blockiert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Das PIX kann mithilfe des ASDM konfiguriert werden. **Hinweis:** Informationen zur Konfiguration des PIX durch den ASDM finden Sie unter <u>Zulassen von HTTPS-Zugriff für ASDM</u>.
- Sie haben mindestens eine zweifelsfrei funktionierende VPN-Konfiguration für den Remote-Zugriff eingerichtet. **Hinweis:** Wenn Sie über keine dieser Konfigurationen verfügen, finden Sie im <u>ASA-as-a-Remote-VPN-Server unter Verwendung des ASDM-Konfigurationsbeispiels</u> weitere Informationen zum Konfigurieren einer guten VPN-Konfiguration für den Remote-Zugriff.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure PIX Security Appliance der Serie 500, Version 7.1(1)**Hinweis:** Die Sicherheitslösungen PIX 501 und 506E unterstützen Version 7.x nicht.
- Cisco Adaptive Security Device Manager Version 5.1(1)**Hinweis:** Das ASDM ist nur in PIX oder ASA 7.x verfügbar.

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

• Cisco Adaptive Security Appliance der Serie ASA 5500, Version 7.1(1)

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Konfigurationsbeispiel ist ein kleines Unternehmensnetzwerk mit drei Subnetzen vorgesehen. Dieses Diagramm zeigt die Topologie. Die drei Subnetze sind Intranet, Engineering und Payroll. Ziel dieses Konfigurationsbeispiels ist es, dem Gehaltsabrechnungspersonal den Remote-Zugriff auf die Subnetze für Intranet und Payroll zu ermöglichen und diesen den Zugriff auf das Engineering-Subnetz zu verwehren. Außerdem sollten die Techniker remote auf die Subnetze Intranet und Engineering, nicht aber auf das Payroll-Subnetz zugreifen können. Der Payroll-Benutzer in diesem Beispiel ist "controller1". Der technische Benutzer in diesem Beispiel ist "engineering1".

Konventionen

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

Konfiguration des Zugriffs über ASDM

Gehen Sie wie folgt vor, um die PIX Security Appliance mithilfe von ASDM zu konfigurieren:

1. Wählen Sie Konfiguration > VPN > Allgemein > Gruppenrichtlinie aus.

Elsco ASDM 5.1 for PIX - 10.89.129.147	Help			=OX
Home Configuration Monitoring	Back Forward Search	h Refresh Save	? Help	CISCO SYSTEMS
Configuration > VPN > General >	Group Policy			
Interfaces	Aroun Paliny			
Security Policy	Manage VPN group poli pairs that may be stored policy information is refe	cies. A VPN group policy is I internally on the device or a renced by VPN tunnel grou	a collection of user-oriented attribut externally on a RADIUS server. The ps and user accounts.	le/value group
🕰 😐 🕅 IKE	Name	Type Tunneling #	Protocol AAA Server Group	Add 👻
VPN BallP Address Manageme	payroll engineering DftGmPolicy (System D	Internal Inherited Internal Inherited Internal IPSec	NIA NIA	Edit
Routing Routing Global Objects Froperties				Delete
×		Apply	Reset	207-51 PM ITC

2. Basierend auf den Schritten, die zur Konfiguration von Tunnelgruppen auf dem PIX unternommen wurden, existieren möglicherweise bereits Gruppenrichtlinien für die Tunnelgruppen, deren Benutzer Sie beschränken möchten. Wenn bereits eine geeignete Gruppenrichtlinie vorhanden ist, wählen Sie diese aus, und klicken Sie auf **Bearbeiten**. Andernfalls klicken Sie auf **Hinzufügen** und wählen **Interne Gruppenrichtlinie aus....**

- 3. Geben Sie ggf. den Namen der Gruppenrichtlinie am oberen Rand des sich öffnenden Fensters ein, oder ändern Sie diesen.
- 4. Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen **Erben** neben Filter, und klicken Sie dann auf **Verwalten**.

Check an Inherit checkbo	x to let the corn	esponding setting take	its value from the default group policy.
Tunneling Protocols:	🔽 Inherit	🗖 IPSec	
Filter:	🗆 Inherit	None	Manage
Connection Settings			~~
Access Hours:	🔽 Inherit		▼ New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Tim	e: 🔽 Inherit	Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

5. Klicken Sie auf **ACL hinzufügen**, um im daraufhin angezeigten Fenster ACL Manager eine neue Zugriffsliste zu erstellen.

1	ACL Ma	nager										×
С	onfigure	e ACLs.										
	*	Rule Enabled	Action	Source Host/Netwo	urk	Destination Host/Netwo	ork	Service	Log l Interv	.evel al	Time Range	Add ACL
												Add ACE
												EditACE
												Delete
												Move Up
												Move Down
	🖌 Allo	ow traffic	0) eny traffic								
						- 1		1		1		
				_	0K		Cancel		Help			

6. Wählen Sie eine Nummer für die neue Zugriffsliste aus, und klicken Sie auf

	🔂 Add New A	CL			×
	ACL ID:	10			[
OK.		OK	-R	Cancel	

7. Wenn Ihre neue ACL links ausgewählt ist, klicken Sie auf Add ACE (ACE hinzufügen), um der Liste einen neuen Zugriffssteuerungseintrag hinzuzufügen.

📬 A	EL Mar	nager							×
Co	nfigure	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
									EditACE
									Delete
									Move Up
									Move Down
1								•	
•	🖉 Allo	w traffic	(3 (Deny traffic					
				01	Cance		Help		

 Definieren Sie den hinzuzufügenden Zugriffssteuerungseintrag (ACE). In diesem Beispiel erlaubt der erste ACE in ACL 10 den IP-Zugriff auf das Payroll-Subnetz von einer beliebigen Quelle. Hinweis: Standardmäßig wählt ASDM nur TCP als Protokoll aus. Sie müssen IP auswählen, wenn Sie den Benutzern vollständigen IP-Zugriff erlauben oder verweigern möchten. Klicken Sie abschließend auf OK.

dd Extended Access List Rule	
Action	Time Range
	Time Range: Not Applied 💌 New
Permit C Deny	Syslog
	Default Syslog More Options
Source Host/Network	Destination Host/Network
● IP Address C Name C Group	● IP Address C Name C Group
IP address: 0.0.0.0	IP address: 10.8.28.0
Mask 0.0.0.0	Mask: 255,255,255,0
Protocol and Service	
	Manage Service Groups
IP Protocol	
IP protocol: any	
lease enter the description below (optional):	
permit IP access from ANY source to the payroll su	ubnet (10.8.28.0 /24)
4	F

9. Der gerade hinzugefügte ACE wird nun in der Liste angezeigt. Wählen Sie erneut ACE hinzufügen, um weitere Zeilen zur Zugriffsliste hinzuzufügen.

1	AC	L Mar	nager							×
(Con	figure	ACLs.							
		#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
ľ	8	10								Add ACE
ŀ		1		1	🏟 any	10.8.28.0/24	💌 ip		Not Applied	Edit ACE
										Delete
										Мруе Up
										Move Down
L	•	2 Allo	w traffic	3	Deny traffic				•	
					0	K Cance	ı	Help		

In diesem Beispiel wird ACL 10 ein zweiter ACE hinzugefügt, um den Zugriff auf das Intranet-Subnetz zu ermöglichen.

id Extended Access	List Rule	
Action		Time Range
		Time Range: Not Applied 💌 New
Permit	C Deny	Syslog
		Default Syslog More Options
Source Host/Networ	k	Destination Host/Network
IP Address	C Name C Group	
IP address: 0.0	0.0	IP address: 10.8.27.0
Mask: 0.0.	0.0	Mask: 255.255.255.0 💌
TCP CUDP IP Protocol IP protocol: a	CICMP © IP	Manage Service Groups
lease enter the desc ermit IP access from	ription below (optional):	sed by all employees (10.8.27.0./24)
access for	And source to the subliet o	sed by an employees (10.0.27.0724)
]		_

10. Klicken Sie nach dem Hinzufügen von ACEs auf OK.

📬 A	CL Ma	nager							×
Co	nfigur	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
	1	V	~	🧼 any	A 10.5.28.0/24	💌 ip		Not Applied	EditACE
	2		1	🧇 any	ga 10.8.27.0/24	💌 ip		Not Applied	<u></u>
									Delete
									Move Up
									Move Down
•	2 01L	austro@io		Donutroffic				•	
	All	ow trainic	U (Jeny trainic					
					1 0amer	. 1	Helm 1		
				0	- R - Cance		Lieih		

11. Wählen Sie die in den letzten Schritten definierte und ausgefüllte ACL aus, um als Filter für Ihre Gruppenrichtlinie zu dienen. Klicken Sie abschließend auf **OK**.

Check an Inherit checkbo	x to let the com	esponding setting take i	ts value from the default group policy
Tunneling Protocols:	🔽 Inherit	🗖 IPSec	
Filter:	🗖 Inherit	10	Manage
Connection Settings		None 10	
Access Hours:	🔽 Inherit		New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Tim	e: 🔽 Inherit		minutes
Idle Timeout	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

12. Klicken Sie auf **Apply**, um die Änderungen an PIX zu senden.

File Rules Se	1 for PIX - 10.89.129.147 arch Options Tools Wizards	; Help				<u>_ </u>
Home C	Sonfiguration Monitoring	Back Forward Search	h Refresh	🔜 🤶 Save Help		CISCO SYSTEMS
Interfaces Security Policy NAT Security Policy NAT Clobal Objects Clobal Objects Properties	Configuration > VPN > General Configuration > VPN > General Configuration > VPN Wizard Configuration = VPN Wizard Configuration = VPN Wizard Configuration = VPN Ventor Trunnel Group Trunnel Grou	Group Policy Group Policy Manage VPN group policy Manage VPN group policy Manage VPN group policy policy information is reference Name payroll engineering DftGrpPolicy (System D)	cles. A VPN grou I internally on the erenced by VPN 1 Internal - Internal Internal IPSe Internal IPSe	Ip policy is a collection of edvice or externally on tunnel groups and user funneling Protocol herited heri	of user-oriented attribute a RADIUS server. The raccounts.	Add Add Add Add Add Add Add Add

13. Wenn Sie dies unter **Optionen > Voreinstellungen** konfiguriert haben, zeigt der ASDM im Voraus die Befehle an, die er an den PIX senden möchte. Klicken Sie auf **Senden**.

Preview CLI Commands		
The following CLI command	are generated based on the chang	ges you made in ASDM. To
send the commands to the l	IX, click Send. To not send the com	mands and continue making
hanges in ASDM, click Can	el.	
access-list 10 line 1 rem	ark permit IP access from ANY sour	rce to the payroll subnet (10.8.28.0 /24 🔺
access-list 10 line 2 exte	nded permit ip any 10.8.28.0 255.25	55.255.0
access-list 10 line 3 rem	ark permit IP access from ANY sour	rce to the subnet used by all employee
access-list 10 line 4 exte group-policy payroll attri	nded permit ip any 10.8.27.0 255.25 utes	00.200.0
vpn-filter value 10	100	
		-
4		
	Send Cano	el
	Lý	

📬 Cisco ASDM 5.	1 for PIX - 10.89.129.147				
File Rules Se	arch Options Tools Wizards	Help			
Sin and America	Sonfiguration Monitoring	Back Forward Sea	ch Refresh S	Save Help	Cisco Systems
Interfaces Security Policy NAT Routing Global Objects Properties	Configuration > VPN > General	Tunnel Group Tunnel Group Manage VPN tunnel gr IPSec or WebVPN con Name payroll engineering DefaultRAGroup DefaultL2LGroup Specify the delimeter to are received when tunn Group Delimiter:	oups. A VPN tunnel gr nection. Type Ipsec-ra Ipsec-ra Ipsec-ra Ipsec-l2i	roup represents a connection s Group Policy payroll engineering DftGrpPolicy DftGrpPolicy IftGrpPolicy Reset	e user name that
Configuration cha	anges saved successfully.		cisco NA	(2)	3/1 3/06 3:22:11 PM UTC

15. Wählen Sie die Tunnelgruppe aus, auf die Sie die Gruppenrichtlinie anwenden möchten, und klicken Sie auf Bearbeiten.

File Rodres Configuration Mankoring Back Forward Search Refresh Save Heip Hone Configuration Mankoring Back Forward Search Refresh Save Heip Wantoo Back Forward Search Refresh Save Heip Image Wantoo Back Forward Search Refresh Save Heip Image Wantoo Configuration - VFN > Deneral > Tunnel Group Image VPN tunnel groups: A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection. Tunnel Group Manage VPN tunnel groups: A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection. IPSec or WebVPN connection. Wange VPN tunnel groups: A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection. IPSec or WebVPN connection. Image VPN tunnel group constraints Image VPN tunnel group constraints Image VPN tunnel group constraints Image VPN tunnel group constraint Tunnel Group Name Tunnel Group Image VPN tunnel group constraint Tunnel Group Image VPN tunnel group constraints Add Image VPN tunnel group constonton. Image	🚰 Cisco ASDM 5	.1 for PIX - 10.89.129.147				
Image Image <th< th=""><th>File Rules Sa</th><th>arch Options Tools Wizards He</th><th>qlp</th><th></th><th></th><th></th></th<>	File Rules Sa	arch Options Tools Wizards He	qlp			
Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Name Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Security Policy Image: Securi	Kome (Configuration Montoring Bas	ck Forward Search	h Refresh Sav	re Help	CISCO SYSTEMS
Configuration changes saved surressfully	Evented as a constraint of the second as constraint of the second as constraint of the second as	Configuration - VFN - General - Tu	Annel Group Manage VPN tunnel gro IP Sec or WebVPN conn Rame Payroll angineering DefaulttRAGroup DefaulttL2LGroup Specify the delimeter to are received when tunne Group Delimiter:	ups. A VPN tunnel grou ection. Type ipsec-ra ipsec-ra ipsec-ra ipsec-121 be used when parsing els are being negotiater None Y Apply	up represents a connection s Group Policy payroll engineering DftDrpPolicy DftGrpPolicy tunnel group names from tf d. Reset	specific record for a Add ▼ Edit Delete the user name that

16. Wenn Ihre Gruppenrichtlinie automatisch erstellt wurde (siehe Schritt 2), überprüfen Sie, ob die soeben konfigurierte Gruppenrichtlinie im Dropdown-Feld ausgewählt ist. Wenn Ihre Gruppenrichtlinie nicht automatisch konfiguriert wurde, wählen Sie sie aus dem Dropdown-Feld aus. Klicken Sie abschließend auf OK.

🔂 Edit Tunnel Group	×
Name: payroll Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabs.	
Basic AAA Client Address Assignment Advanced	
Group Policy: payroll	
Strip the realm from username before passing it on to the AWA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

- 17. Klicken Sie auf Übernehmen und, wenn Sie dazu aufgefordert werden, auf Senden, um die Änderung zur PIX-Konfiguration hinzuzufügen.Wenn die Gruppenrichtlinie bereits ausgewählt wurde, erhalten Sie möglicherweise die Meldung "Es wurden keine Änderungen vorgenommen." Klicken Sie auf OK.
- 18. Wiederholen Sie die Schritte 2 bis 17 f
 ür alle zus
 ätzlichen Tunnelgruppen, denen Sie Einschr
 änkungen hinzuf
 ügen m
 öchten. In diesem Konfigurationsbeispiel muss auch der Zugang der Techniker eingeschr
 änkt werden. Obwohl das Verfahren identisch ist, gibt es einige Fenster, in denen Unterschiede erkennbar sind:Neue Zugriffsliste 20

💼 A	CL Ma	nager							x
Co	nfigur	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
G	10								Add ACE
	1	N	~	🧼 any	A 10.8.28.0/24	😕 ip		Not Applied	EditACE
	2	V	~	🧼 any	A 10.8.27.0/24	😕 ip		Not Applied	Editrice
G	20								Delete
	1	V	~	🧼 any	A 192.168.1.0/24	😕 ip		Not Applied	Manalia
	2		1	🧇 any	10.8.27.0/24	🕑 ip		Not Applied	Move Op
									Move Down
4								•	
	Allo	ow traffic	8	Denytraffic					
					1		1		
				0	Cance	9I	Help		

Wählen Sie **Zugriffsliste 20** als Filter in der Richtlinie der Technikergruppe aus.

Check an innent checkbo	cto let the com	esponding setting take	its value from the default group po	DIICY.
Tunneling Protocols:	🗹 Inherit	F IPSec		
Filter:	🗖 Inherit	20	Manage	
Connection Settings				
Access Hours:	🔽 Inherit		Vew	
Simultaneous Logins:	🔽 Inherit			
Maximum Connect Time	e: 🔽 Inherit	🗖 Unlimited	minutes	
Idle Timeout:	🔽 Inherit	Unlimited	minutes	
Servers				
DNS Servers:	🔽 Inherit	Primary:	Secondary:	
WINS Servers:	🔽 Inherit	Primary:	Secondary:	
DHCP Scope:	🔽 Inherit			

Überprüfen Sie, ob die Richtlinien der Engineering Group für die Engineering Tunnel Group festgelegt sind.

🚰 Edit Tunnel Group	×
Name: engineering Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabs.	
Basic AAA Client Address Assignment Advanced	
Group Policy: engineering	
Strip the realm from username before passing it on to the AAA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

Zugriff über CLI konfigurieren

Gehen Sie wie folgt vor, um die Sicherheits-Appliance mithilfe der CLI zu konfigurieren:

Hinweis: Einige der Befehle in dieser Ausgabe werden aus räumlichen Gründen auf eine zweite Zeile herabgesetzt.

 Erstellen Sie zwei verschiedene Zugriffskontrolllisten (15 und 20), die auf Benutzer angewendet werden, wenn diese eine Verbindung zum VPN für den Remote-Zugriff herstellen. Diese Zugriffsliste wird später in der Konfiguration aufgerufen. ASAwCSC-CLI(config)#access-list 15 remark permit IP access from ANY source to the payroll subnet (10.8.28.0/24)

ASAwCSC-CLI(config)#access-list 15 extended permit ip any 10.8.28.0 255.255.0

```
ASAWCSC-CLI(config)#access-list 15 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0)
ASAWCSC-CLI(config)#access-list 15 extended permit ip
any 10.8.27.0 255.255.255.0
ASAWCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
source to the Engineering subnet (192.168.1.0/24)
ASAWCSC-CLI(config)#access-list 20 extended permit ip
any 192.168.1.0 255.255.255.0
ASAWCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0/24)
ASAWCSC-CLI(config)#access-list 20 extended permit ip
any 10.8.27.0 255.255.255.0
```

2. Erstellen Sie zwei verschiedene VPN-Adresspools. Erstellen Sie eine Gehaltsabrechnung und eine für die Remote-Benutzer Engineering. ASAwCSC-CLI(config)#ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.2

```
ASAwCSC-CLI(config)#ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0
```

 Erstellen Sie Richtlinien f
ür die Gehaltsabrechnung, die nur f
ür sie gelten, wenn sie eine Verbindung herstellen.

ASAwCSC-CLI(config)#group-policy Payroll internal

ASAwCSC-CLI(config)#group-policy Payroll attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 15

!--- Call the ACL created in step 1 for Payroll. ASAwCSC-CLI(config-group-policy)#vpntunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value payroll.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Payroll-VPN

!--- Call the Payroll address space that you created in step 2.

4. Dieser Schritt ist mit Schritt 3 identisch, mit Ausnahme der Engineering-Gruppe. ASAwCSC-CLI(config)#group-policy Engineering internal

ASAwCSC-CLI(config)#group-policy Engineering attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 20

!--- Call the ACL that you created in step 1 for Engineering. ASAwCSC-CLI(config-grouppolicy)#vpn-tunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value Engineer.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Engineer-VPN

!--- Call the Engineering address space that you created in step 2.

5. Erstellen Sie lokale Benutzer, und weisen Sie diesen Benutzern die soeben erstellten Attribute zu, um den Zugriff auf Ressourcen zu beschränken. ASAwCSC-CLI(config)#username engineer password cisco123

ASAwCSC-CLI(config)#username engineer attributes ASAwCSC-CLI(config-username)#vpn-group-policy Engineering ASAwCSC-CLI(config-username)#vpn-filter value 20 ASAwCSC-CLI(config)#username marty password cisco456 ASAwCSC-CLI(config)#username marty attributes ASAwCSC-CLI(config-username)#vpn-group-policy Payroll ASAwCSC-CLI(config-username)#vpn-filter value 15

6. Erstellen Sie Tunnelgruppen, die Verbindungsrichtlinien für die Payroll-Benutzer enthalten. ASAwCSC-CLI(config)#tunnel-group Payroll type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Payroll general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Payroll-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Payroll

ASAwCSC-CLI(config)#tunnel-group Payroll ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key time1234

7. Erstellen Sie Tunnelgruppen, die Verbindungsrichtlinien für die Engineering-Benutzer enthalten.

ASAwCSC-CLI(config)#tunnel-group Engineering type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Engineering general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Engineer-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Engineering

ASAwCSC-CLI(config)#tunnel-group Engineering ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key Engine123

Nach Eingabe der Konfiguration wird dieser hervorgehobene Bereich in Ihrer Konfiguration angezeigt:

Gerätename 1

```
ASA-AIP-CLI(config)#show running-config
ASA Version 7.2(2)
!
hostname ASAwCSC-ASDM
domain-name corp.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
```

```
interface Ethernet0/0
nameif Intranet
security-level 0
ip address 10.8.27.2 255.255.255.0
interface Ethernet0/1
nameif Engineer
security-level 100
ip address 192.168.1.1 255.255.255.0
1
interface Ethernet0/2
nameif Payroll
security-level 100
ip address 10.8.28.0
1
interface Ethernet0/3
no nameif
no security-level
no ip address
1
interface Management0/0
no nameif
no security-level
no ip address
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
access-list Inside_nat0_outbound extended permit ip any
172.10.1.0 255.255.255.0
access-list Inside_nat0_outbound extended permit ip any
172.16.2.0 255.255.255.0
access-list 15 remark permit IP access from ANY source
to the
  Payroll subnet (10.8.28.0/24)
access-list 15 extended permit ip any 10.8.28.0
255.255.255.0
access-list 15 remark Permit IP access from ANY source
to the subnet
  used by all employees (10.8.27.0)
access-list 15 extended permit ip any 10.8.27.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the Engineering
  subnet (192.168.1.0/24)
access-list 20 extended permit ip any 192.168.1.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the subnet used
  by all employees (10.8.27.0/24)
access-list 20 extended permit ip any 10.8.27.0
255.255.255.0
pager lines 24
mtu MAN 1500
mtu Outside 1500
mtu Inside 1500
ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask
255.255.255.0
ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
```

```
no asdm history enable
arp timeout 14400
global (Intranet) 1 interface
nat (Inside) 0 access-list Inside_nat0_outbound
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy Payroll internal
group-policy Payroll attributes
dns-server value 10.8.27.10
vpn-filter value 15
vpn-tunnel-protocol IPSec
default-domain value payroll.corp.com
address-pools value Payroll-VPN
group-policy Engineering internal
group-policy Engineering attributes
dns-server value 10.8.27.10
vpn-filter value 20
vpn-tunnel-protocol IPSec
default-domain value Engineer.corp.com
address-pools value Engineer-VPN
username engineer password LCaPXI.4Xtvclaca encrypted
username engineer attributes
vpn-group-policy Engineering
vpn-filter value 20
username marty password 6XmYwQ009tiYnUDN encrypted
privilege 0
username marty attributes
vpn-group-policy Payroll
vpn-filter value 15
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set
ESP-3DES-SHA
crypto map Outside_map 65535 ipsec-isakmp dynamic
Outside_dyn_map
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
tunnel-group Payroll type ipsec-ra
tunnel-group Payroll general-attributes
address-pool vpnpool
default-group-policy Payroll
tunnel-group Payroll ipsec-attributes
pre-shared-key *
tunnel-group Engineering type ipsec-ra
tunnel-group Engineering general-attributes
```

```
address-pool Engineer-VPN
 default-group-policy Engineering
tunnel-group Engineering ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
1
policy-map type inspect dns migrated_dns_map_1
parameters
 message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
 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
prompt hostname context
Cryptochecksum:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

<u>Überprüfen</u>

Überprüfen Sie Ihre Konfiguration mithilfe der Überwachungsfunktionen des ASDM:

 Wählen Sie Monitoring > VPN > VPN Statistics > Sessions aus. Sie sehen die aktiven VPN-Sitzungen auf dem PIX. Wählen Sie die Sitzung aus, die Sie interessieren, und klicken Sie auf Details.

Gisco ASDM 5.1 for PIX - 10.89.129.147 File Rules Search Options Tools W	ards Help			
Home Configuration Monitoring	Back Forward Se	Q Q Ú tarch Refresh S	ave Help	CISCO SYSTEMS
Image: second	atisbus > Sessions apl Sessions Remote Access stic c 8 Filter By: Remote Access Username controller1 D atisbus Image: Second Seco	LAN-to-LAN 1 CLAN-to-LAN 1 CLA	Total 0 ns ssigned IP Address ublic IP Address 0.8.27.50 IP 2.221165 30 10.2 Refresh	Total Cumulative 1 3 Filter Protocol Encryption Cessions Ping ot Order from popup menu. gout Sessions
Data Refreshed Successfully.		cisco NA	(2) 🛛 📓 🔂	🔒 3/13/06 8:36:34 PM UTC

2. Wählen Sie die Registerkarte ACL aus.Die Zugriffskontrolllisten reflektieren den Datenverkehr, der den Tunnel vom Client zu den zulässigen Netzwerken durchläuft.

Session Details					2
Remote Detailed					
Usemame	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Client Type Version
controller1	DrittGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES	20:35:08 UTC Mon Mar 13 2006 0h:09m:58s	WinNT 4.8.00.0440
Details ACL	CL is being applie 2 elements line 1 remark pern line 2 extended per line 3 remark pern line 4 extended per	ed to this session: ent IP access from ermit ip any 10.8.2 ent IP access from ermit ip any 10.8.2	ANY source to the p 8.0 255.255.255.0 n ANY source to the s 7.0 255.255.255.0 n	payroll subnet (10.8.28.0 /2 (hitcnt=8) 0x25954260 subnet used by all employees (hitcnt=4) 0xd52617df	.4) 2 (10.8.27.0 /2
		Refresh	Close	Last Update	d: 3/13/06 2:47:17 PM-

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances ASA der Serie ASA 5500 als Remote-VPN-Server mit</u> <u>ASDM - Konfigurationsbeispiel</u>
- Konfigurationsbeispiele für Sicherheitsgeräte der Cisco PIX 500-Serie und technische <u>Hinweise</u>
- Konfigurationsbeispiele für Cisco Adaptive Security Appliances der Serie ASA 5500 und technische Hinweise
- Konfigurationsbeispiele für Cisco VPN-Clients und technische Hinweise
- <u>Technischer Support und Dokumentation Cisco Systems</u>