PIX/ASA 7.x ASDM: De netwerktoegang van VPN-gebruikers die toegang hebben tot Remote Access beperken

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Netwerkdiagram Conventies Toegang configureren via ASDM Toegang via CLI configureren Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document biedt een voorbeeldconfiguratie met behulp van Cisco Adaptieve Security Devices Manager (ASDM) voor het beperken van wat interne netwerken voor VPN-gebruikers die toegang hebben tot externe netwerken achter de PIX security applicatie of adaptieve security applicatie (ASA). U kunt de externe toegang tot VPN-gebruikers beperken tot alleen de gebieden van het netwerk waartoe u toegang wilt hebben wanneer u:

- 1. Toegangslijsten maken.
- 2. Associeer ze met groepsbeleid.
- 3. Associeer dat groepsbeleid met tunnelgroepen.

Raadpleeg <u>de Cisco VPN 3000 Concentrator configureren voor blokkering met filters en RADIUS-filtertoewijzing</u> om meer te weten te komen over het scenario waarin de VPN-Concentrator de toegang van VPN-gebruikers blokkeert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

• De PIX kan worden ingesteld met behulp van de ASDM. Opmerking: Raadpleeg HTTPS-

toegang voor ASDM om de PIX te kunnen configureren door de ASDM.

 U hebt ten minste één bekende goede VPN-configuratie voor toegang op afstand. Opmerking: Als u geen van dergelijke configuraties hebt, raadpleegt u <u>ASA als een Remote VPN-server</u> met behulp van het ASDM Configuration Voorbeeld voor informatie over de configuratie van een goede externe VPN-configuratie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure PIX 500 Series security applicatie versie 7.1(1)**Opmerking:** De PIX 501 en 506E security applicaties ondersteunen versie 7.x niet.
- Cisco Adaptieve Security Adapter Manager versie 5.1(1)**Opmerking:** ASDM is alleen beschikbaar in PIX of ASA 7.x.

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.

Verwante producten

Deze configuratie kan ook worden gebruikt in combinatie met deze hardware- en softwareversies:

• Cisco ASA 5500 Series adaptieve security applicatie, versie 7.1(1)

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



In dit configuratievoorbeeld is een klein bedrijfsnetwerk met drie subnetten verondersteld. Dit diagram illustreert de topologie. De drie subnetten zijn Intranet, Engineering en Payroll. Het doel van dit configuratievoorbeeld is om salarissen personeel op afstand toegang tot het Intranet en Loonsubnetwerk toe te staan en hen te verhinderen om toegang te krijgen tot het subnet van de Bouwnijverheid. Ook zouden de ingenieurs in staat moeten zijn om op afstand toegang te hebben tot het Intranet en de technische subnetten, maar niet tot het Subnet van de Betaling. De loonwerker in dit voorbeeld is "controller1". De technische gebruiker in dit voorbeeld is "ingenieur1".

Conventies

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

Toegang configureren via ASDM

Volg deze stappen om de PIX security applicatie te configureren met ASDM:

1. Selecteer Configuration > VPN > General > Group Policy.

Cisco ASDM 5.1	l for PIX - 10.89.129.147					_ O ×
File Rules Sea	arch Options Tools Wizards	Help				
Home C	onfiguration Monitoring	Back Forward Search	h Refres	h Save Help		CISCO SYSTEMS
	Configuration > VPN > General >	 Group Policy 				
Interfaces		Group Policy Manage VPN group poli pairs that may be stored	cies. A VPN g	roup policy is a collectio the device or externally	n of user-oriented attribu on a RADIUS server. The	te/value group
NAT	- Dunnel Group	policy information is refe	erenced by VP	'N tunnel groups and us	er accounts.	
	⊕ % IKE	Name	Type	Tunneling Protocol	AAA Server Group	Add 👻
VPN	🖽 🏪 IP Address Manageme	payroll	Internal	Inherited	N/A	Edit
3.	E - Birsec	engineering DftfGmPolicy (System D	Internal IP	PSec	NIA	
Routing		omorpi ener (ayeren o	in the street of	000	- ferri -	Delete
Global Objects						
	4		Ap	oly Rese	t	2-07-51 PM ITA
			cisco	NA (2)	🖉 🎦 🔰 🔂 🖉	3:07:51 PM UTC

2. Op basis van welke stappen zijn ondernomen om tunnelgroepen op de PIX te configureren bestaat groepsbeleid al voor tunnelgroepen waarvan u de gebruikers wilt beperken. Als er al een geschikt groepsbeleid bestaat, kiest u het programma en klikt u op **Bewerken**. Klik anders op **Toevoegen** en kies **intern groepsbeleid...**.

🔂 Cisco ASDM 5.1 for PIX	- 10.89.129.147						_IO ×
File Rules Search Op	tions Tools Wizards Help)					
Home Configura	tion Monitoring Back	Forward Search	n Refre	esh Save	? Help		Cisco Systems
Interfaces Interfaces Security Policy Interfaces Security Policy Interfaces Interfaces	ration > VPN > General > Grou PN Wizard Seneral Client Update Default Tunnel Gab Tunnel Group VPN System Option KE P Address Manageme PSec Diff	In Policy	cies. A VPN Internally of renced by ' Type Internal Internal Internal	I group policy is on the device or o VPN tunnel grou Tunneling F Inherited - Inherited IPSec	a collection of u externally on a R ps and user acc Protocol Av - 1 - 1 - 1 - 1 - 1	ser-oriented attribu ADIUS server. The counts. AA Server Group WA WA WA	Add Add Add Add Add Add Add Add

- 3. Indien nodig voert u de naam van het groepsbeleid in of wijzigt u dit boven in het venster dat nu wordt geopend.
- 4. Schakel op het tabblad Algemeen het vakje Inherit naast Filter uit en klik vervolgens op **Bewerken**.

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

5. Klik op Add ACL om een nieuwe toegangslijst in het venster van ACL Manager te maken dat verschijnt.

1	ACL Ma	nager								×
С	onfigure	e ACLs.								
	*	Rule Enabled	Action	Source Host/Network	Destina Host/Ne	tion stwork	Service	Log Level Interval	Time Range	Add ACL
										Add ACE
										EditACE
										Delete
										Move Up
										Move Down
	-								•	
	🖌 Allo	ow traffic	O (Deny traffic						
					av 1	Onned	1	Linin [
						Cancel		нер		

6. Kies een nummer voor de nieuwe toegangslijst en klik op

	🔂 Add New A	CL				×
	ACL ID:	10				
OK.		ок	-b	Ca	ancel	

7. Als uw nieuwe ACL links is geselecteerd, klikt u op **ACE toevoegen** om een nieuwe toegangscontrole aan de lijst toe te voegen.

1	ACL Mai	nager							×
C	onfigure	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
									EditACE
									Delete
									Мруе Up
									Move Down
Ŀ	·							•	
	🖌 Allo	w traffic	() [Deny traffic					
				0	Cance		Help		

8. Defineer de toegangscontrole ingang (ACE) die u wilt toevoegen. In dit voorbeeld, het eerste ACE in ACL 10 staat IP toegang tot het Subnet van de Loon van elke bron toe. Opmerking: standaard selecteert ASDM alleen TCP als protocol. U moet IP kiezen als u gebruikers volledige IP-toegang wilt toestaan of weigeren. Klik op OK wanneer u klaar bent.

Id 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	
C TCP C UDP C ICMP C P	Manage Service Groups
IP protocol: any	
lease enter the description below (optional):	
ermit IP access from ANY source to the payroll sub	net (10.8.28.0 /24)

9. Het ACE dat u zojuist hebt toegevoegd, verschijnt nu in de lijst. Kies nogmaals ACE toevoegen om extra lijnen aan de toegangslijst toe te voegen.

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	Ξ	10								Add ACE
ŀ		1		1	🏟 any	10.8.28.0/24	💌 ip		Not Applied	Edit ACE
										Delete
										Move Up
										Move Down
I.	•								•	
	*	 Allo 	wtraffic	00	Deny traffic					
					0	K Cance	н	Help		

In dit voorbeeld, wordt een tweede ACE aan ACL 10 toegevoegd om toegang tot Intranet toe te

staan.

Action Time Range Time Range Time Range Time Range Sysiog Default Sysiog Destination Host/Network © IP Address © Name © Group IP address: 0.0.0.0 Mask: 0.0.0.0 Protocol and Service Protocol and Service TCP © UDP © ICMP © IP IP protocol IP protocol IP protocol ease enter the description below (optional): ermit IP access from ANY source to the subnet used by all employees (10.8.27.072/2012)	
Permit O Deny Source Host/Network IP Address O Name O Group IP address: 0.0.0 Mask: 0.0.0 Protocol and Service O TOP O UDP O ICMP O IP IP Protocol IP protocol: any IP protocol: any IP access from ANY source to the subnet used by all employees (10.8.27.0/24)	
Permit C Deny Syslog Default Syslog Source Host/Network IP Address C Name C Group IP address: 0.0.0.0 Mask: 0.0.0 Mask: 0	ied 💌 New
Default Syslog Source Host/Network IP Address IP address: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Protocol and Service TCP IP protocol: any IP protocol: any IP access from ANY source to the subnet used by all employees (10.8.27.0/24)	
Source Host/Network IP Address Name Group IP address: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Mask: 0.0.0 Manage IP Protocol IP protocol IP protocol: any Rease enter the description below (optional): ermit IP access from ANY source to the subnet used by all employees (10.8.27.0/24	More Options
IP Address O Name O Group IP address: 0.0.0.0 Mask: 0.0.0.0 Mask: 255.255.2 Protocol and Service O TCP O UDP O ICMP O IP IP Protocol IP protocol: any IP protocol: any ease enter the description below (optional): ermit IP access from ANY source to the subnet used by all employees (10.8.27.0/24)	k
IP address: 0.0.0.0 IP address: 10.8.27.0 Mask: 0.0.0.0 Mask: 255.255.2 Protocol and Service C TCP C UDP C ICMP © IP Marrag IP protocol IP protocol: any	ame 🔿 Group
Mask: 0.0.0 Image: Contract of the subnet used by all employees (10.8.27.0724) Mask: 0.0.0 Image: Contract of the subnet used by all employees (10.8.27.0724)	D
Protocol and Service TCP UDP ICMP IP Manage IP Protocol IP IP Manage IP protocol: any IP ease enter the description below (optional): armit IP access from ANY source to the subnet used by all employees (10.8.27.0/24)	255.0 💌
ease enter the description below (optional): ermit IP access from ANY source to the subnet used by all employees (10.8.27.0/24	ge Service Groups
1	24)
OK Cancel Hein	1

10. Klik op **OK** zodra u klaar bent met het toevoegen van ACE's.

sta P	CL M	anager							×
Co	Infigu	re ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	1 10								Add ACE
	1	V	~	🧼 any	AD:5.28.0/24 🚮	😕 ip		Not Applied	EditACE
	2		1	🧇 any	g ²³ 10.8.27.0/24	💌 ip		Not Applied	1
									Delete
									Move Up
									Move Down
	🖌 AI	low traffic	1	Deny traffic					
				0	K Cance	I	Help		

11. Selecteer ACL die u in de laatste stappen hebt gedefinieerd en ingevuld om het filter voor uw groepsbeleid te zijn. Klik op **OK** wanneer u klaar bent.

check an innent checkbo	x to let the com	esponding setting take it	is value from the default group policy
Tunneling Protocols:	🔽 Inherit	F IPSec	
Filter:	🗖 Inherit	10	Manage
Connection Settings		None 10	
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		

12. Klik op **Toepassen** om de wijzigingen in de PIX te verzenden.

File Rules Search Options Tools Wizards Help		_0×
Home Configuration Monitoring Back Forward Se	Q Q 🧔 🦓 earch Refresh Save Help	Cisco Systems
Image: Security Policy Image: Properties Image: Properties Image: Properties Image: Properties	policies. A VPN group policy is a collection of user-oriente pred internally on the device or externally on a RADIUS ser referenced by VPN tunnel groups and user accounts. Type Tunneling Protocol AAA Server G Internal Inherited N/A Internal Inherited N/A D Internal IPSec N/A D Internal IPSec N/A	d attribute.waiue ver. The group Add Edit Delete

13. Als u dit onder **Opties > Voorkeuren** hebt ingesteld, wordt de opdracht in de ASDM gepresteerd dat deze naar de PIX wordt verzonden. Klik op **Verzenden**.

📬 Preview CLI Commands				×
The following CLI comm send the commands to changes in ASDM, click	nands are generated based the PIX, click Send. To not Cancel.	d on the changes you r send the commands :	made in ASDM. To and continue making	
access-list 10 line 1 access-list 10 line 2 access-list 10 line 3 access-list 10 line 4 group-policy payroll vpn-filter value 10	remark permit IP access f extended permit ip any 10 remark permit IP access f extended permit ip any 10 attributes	rom ANY source to the .8.28.0 255.255.255.0 rom ANY source to the .8.27.0 255.255.255.0	payroll subnet (10.8 subnet used by all e	28.0 /24 📩 mploye¢
				<u>_</u>
•	Send	Cancel		

14. Pas het beleid van de Groep toe dat net tot de juiste tunnelgroep werd gemaakt of aangepast. Klik op **Tunnelgroep** in het linker kader.



15. Kies de tunnelgroep waarop u het groepsbeleid wilt toepassen en klik op **Bewerken**.

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. Wange VPN tunnel group consection. IPSec or WebVPN connection. Edit Back Back IPSec or WebVPN connection. Edit Back Back IPSec or WebVPN connection. Edit Default RAGroup Back Back IPSec or WebVPN connection. Edit Default	🚰 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 DftOrpPolicy DftGrpPolicy tunnel group names from tf d. Reset	specific record for a Add ▼ Edit Delete the user name that

16. Als uw groepsbeleid automatisch is gemaakt (zie stap 2), controleer of het groepsbeleid dat u zojuist hebt ingesteld, in het vervolgkeuzevenster is geselecteerd. Als uw groepsbeleid niet automatisch is ingesteld, selecteert u dit in het uitrolvak. Klik op **OK** wanneer u klaar bent.

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	
	I
OK Cancel Help	

- 17. Klik op Toepassen en klik, indien dit wordt gevraagd, op Verzend om de verandering in de PIX-configuratie toe te voegen. Als het groepsbeleid al was geselecteerd, ontvangt u een bericht dat luidt: "Er zijn geen wijzigingen aangebracht". Klik op OK.
- 18. Herhaal stap 2 tot en met 17 voor alle extra tunnelgroepen waaraan u beperkingen wilt toevoegen. In dit configuratievoorbeeld is het ook noodzakelijk de toegang van de ingenieurs te beperken. Hoewel de procedure hetzelfde is, zijn er hier een paar etappes waar grote verschillen bestaan: Nieuwe toegangslijst 20

1	CL Ma	nager							x
Co	nfigure	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	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	Latrice
	20								Delete
	1	V	~	🧇 any	A 192.168.1.0/24	😕 ip		Not Applied	Maustin
	2		 Image: A second s	🧇 any	10.8.27.0/24	🕑 ip		Not Applied	Move Op
									Move Down
1								<u> </u>	
1	Allo	iw traffic	8	Denytraffic					
					1				
				0	Cance	el	Help		

Kies **toegangslijst 20** als een filter in het beleid van de technische groep.

	cio lei ine com	esponding setting take i	s value from the default group polic
unneling Protocols:	🔽 Inherit	🗖 IP Sec	
ilter:	🗌 Inherit	20	Manage
connection Settings			
Access Hours:	✓ Inherit		Vew
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Time	e: 🔽 Inherit	🗖 Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
ervers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
	-		

Controleer dat het beleid van de Engineering Group voor de Engineering Tunnel Group is ingesteld.

🚰 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	

Toegang via CLI configureren

Volg deze stappen om het security apparaat te configureren met behulp van de CLI:

Opmerking: Sommige opdrachten in deze uitvoer worden vanwege ruimtelijke redenen naar een tweede regel teruggebracht.

 Maak twee verschillende toegangscontrolelijsten (15 en 20) die op gebruikers worden toegepast terwijl ze verbinding maken met de externe VPN-toegang. Deze toegangslijst wordt later in de configuratie ingeschakeld. 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. Maak twee verschillende VPN-adrespools. Maak er een voor Payroll en één voor de technische externe gebruikers. 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
```

3. Creëer beleid voor loonlijst dat alleen op hen van toepassing is wanneer ze zich verbinden. 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. Deze stap is hetzelfde als stap 3, behalve voor de technische groep. 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.

Maak lokale gebruikers en wijs de eigenschappen toe die u net aan die gebruikers hebt

gemaakt om hun toegang tot middelen te beperken. 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 marty attributes ASAwCSC-CLI(config-username)#vpn-group-policy Payroll ASAwCSC-CLI(config-username)#vpn-filter value 15

6. Maak tunnelgroepen die verbindingsbeleid bevatten voor de gebruikers van de loonlijst. 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. Maak tunnelgroepen die verbindingsbeleid bevatten voor de gebruikers van de Engineering. 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

Nadat u de configuratie hebt ingevoerd, kunt u dit gemarkeerde gebied in uw configuratie zien:

Asa-AIP-CLI(config)#show running-config 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 10.8.27.2 255.255.0

```
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
!
interface Ethernet0/3
no nameif
no security-level
no ip address
interface Management0/0
no nameif
no security-level
no ip address
1
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 espsha-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
!
!
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)#
```

Verifiëren

Gebruik de bewakingsfuncties van ASDM om uw configuratie te controleren:

 Selecteer Monitoring > VPN > VPN Statistieken > Sessies.U ziet de actieve VPN sessies op de PIX. Selecteer de sessie waarin u geïnteresseerd bent en klik op Details.

Cisco ASDM 5.1 for PIX - 10.89. File Rules Search Options 1	129.147 Fools Wizards Help				
👘 🦓 Home Configuration N	Aunitoring Back Forward	Search Refresh	🔜 🤶 Save Help	Crea	CO SYSTEMS
Image: Second	V > VPN Statistics > Sessions nection Grapi : Tunnels istics o Statistics ption Statistic al IKE/IPSec 5 col Statistics tons Filter By: Rem Username confroller1 * To sort VPN session Logout By: - A	ass LAN-to-LAN 1 ote Access I All Sessi Group Policy Tunnel Group DflGrpPolicy payroll ons, right-click on the above All Sessions I (Total 0 Interferesh	Total Cumulative 1 Protocol Encryption PSec 3DES Soft Order from popup m agout Sessions	3 Details Logout Ping enu.
Data Refreshed Successfully.		cisco N	IA (Z) 🛛 🔡 🏧	🔂 3/13/06 8:36	34 PM UTC

2. Selecteer het tabblad ACL.De ACL-signalering geeft verkeer weer dat door de tunnel stroomt van de client naar het (de) toegestane netwerk(en).

Session Details						
Remote Detailed						
Usemame	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Client Type Version	
ontroller1	DftGrpPolicy 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 The following ACL is being applied to this session: access-list 10; 2 elements access-list 10 line 1 remark permit IP access from ANY source to the payroll submet (10.8.28.0 /24) access-list 10 line 2 extended permit IP access from ANY source to the submet used by all exployees (10.8.27.0 /2 access-list 10 line 4 extended permit ip any 10.8.27.0 255.255.0 (hitcnt=4) 0xd52617df						
		Refresh	Close	Help Last Update	d: 3/13/06 2:47:17 PM	

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties ASA als externe VPN-server met ASDM-configuratievoorbeeld
- Cisco PIX 500 Series security applicaties en configuratie voorbeelden van TechNotes
- Cisco ASA 5500 Series adaptieve security applicaties en configuratie voorbeelden van <u>TechNotes</u>
- <u>Cisco VPN-clientconfiguratie voorbeelden en TechNotes</u>
- Technische ondersteuning en documentatie Cisco Systems