PIX/ASA 7.x ASDM : limiter l'accès réseau des utilisateurs VPN d'accès à distance

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Produits connexes Diagramme du réseau Conventions Configurer l'accès via ASDM Configurer l'accès via CLI Vérifier Dépannage Informations connexes

Introduction

Ce document fournit un exemple de configuration du Cisco Adaptive Security Device Manager (ASDM) pour limiter ce à quoi les utilisateurs du VPN d'accès à distance des réseaux internes peuvent accéder derrière l'appliance de sécurité PIX ou l'appliance de sécurité adaptable (ASA). Vous pouvez limiter les utilisateurs du VPN d'accès à distance aux seules zones du réseau auxquelles vous souhaitez qu'ils puissent accéder lorsque vous :

- 1. Créez des listes de contrôle d'accès.
- 2. Associez-les aux stratégies de groupe.
- 3. Associez ces stratégies de groupe à des groupes de tunnels.

Référez-vous à <u>Configuration du concentrateur Cisco VPN 3000 pour le blocage avec des filtres et</u> <u>l'affectation de filtre RADIUS</u> afin d'en savoir plus sur le scénario où le concentrateur VPN bloque l'accès des utilisateurs VPN.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

• Le PIX peut être configuré en utilisant l'ASDM.

Remarque : référez-vous à <u>Autoriser l'accès HTTPS pour ASDM</u> afin de permettre au PIX d'être configuré par l'ASDM.

• Vous disposez d'au moins une configuration VPN d'accès à distance correcte connue.

Remarque : si vous n'avez pas de telles configurations, référez-vous à <u>ASA en tant que</u> <u>serveur VPN distant utilisant l'exemple de configuration ASDM</u> pour plus d'informations sur la façon de configurer une configuration VPN d'accès distant correcte.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• Appliance de sécurité de la gamme Cisco Secure PIX 500 version 7.1(1)

Remarque : les appliances de sécurité PIX 501 et 506E ne prennent pas en charge la version 7.x.

• Cisco Adaptive Security Device Manager version 5.1(1)

Remarque : l'ASDM est uniquement disponible dans PIX ou ASA 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

• Appliance de sécurité adaptatif de la gamme Cisco ASA 5500 version 7.1(1)

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cet exemple de configuration, un petit réseau d'entreprise avec trois sous-réseaux est supposé. Ce schéma illustre la topologie. Les trois sous-réseaux sont Intranet, Ingénierie et Paie. L'objectif de cet exemple de configuration est d'autoriser le personnel de paie à accéder à distance aux sous-réseaux Intranet et Payroll et de l'empêcher d'accéder au sous-réseau Ingénierie. En outre, les ingénieurs doivent pouvoir accéder à distance aux sous-réseaux Intranet et Ingénierie, mais pas au sous-réseau Paie. L'utilisateur de paie dans cet exemple est « controller1 ». L'utilisateur ingénieur dans cet exemple est "ingénieur1".

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux <u>Conventions relatives aux conseils techniques Cisco.</u>

Configurer l'accès via ASDM

Complétez ces étapes pour configurer l'appliance de sécurité PIX à l'aide de l'ASDM :

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



2. En fonction des étapes suivies pour configurer les groupes de tunnels sur le PIX, des stratégies de groupe peuvent déjà exister pour les groupes de tunnels dont vous souhaitez restreindre les utilisateurs. Si une stratégie de groupe appropriée existe déjà, sélectionnez-la et cliquez sur Modifier. Sinon, cliquez sur Ajouter et choisissez Stratégie de groupe interne....

Gisco ASDM 5.1 for PIX - 10.89 File Rules Search Options	.129.147 Tools Wizards Help						
Home Configuration	Monitoring Back	Forward Search	Refres	h Save	? Help		CISCO SYSTEMS
Interfaces Interfaces Security Policy NAT Image: Security Policy Image: Security Polic	VPN General Group A Control Contro Control Control Control Control Control Control Control	Policy Po	Internal Pointernally or enced by Vi Internal - Internal II	proup policy is a in the device or ext PN tunnel groups Tunneling Pro- Inherited PSec	collection of use ternally on a RAD and user account official AAA - N/A - N/A - N/A - N/A	r-oriented attribute DIUS server. The g Ints. Berver Group	Add Add Belete

- 3. Si nécessaire, entrez ou modifiez le nom de la stratégie de groupe en haut de la fenêtre qui s'ouvre.
- 4. Dans l'onglet Général, décochez la case Hériter en regard de Filtre, puis cliquez sur Gérer.

Check an Inherit checkbo	to let the corr	esponding setting take i	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 Time	e: 🗹 Inherit	🗖 Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

5. Cliquez sur Add ACL pour créer une nouvelle liste d'accès dans la fenêtre ACL Manager qui s'affiche.

1	ACL Mar	nager							×
1	Configure	ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
									Add ACE
									EditACE
									Delete
									Move Up
									Move Down
l	• <u>•</u> • • • •	utraffic	0.5	lonutraffic				•	
	♥ All0	witamic	U L	reny trainc					
				01	Cance		Help		

6. Choisissez un numéro pour la nouvelle liste d'accès et cliquez sur OK.

付 Add New A	CL		×
ACL ID:	10		
	ок	Cancel	

7. La nouvelle liste de contrôle d'accès étant sélectionnée à gauche, cliquez sur Add ACE pour ajouter une nouvelle entrée de contrôle d'accès à la liste.

🔯 ACL Ma	nager										×
Configur	e ACLs.										
#	Rule Enabled	Action	Source Host/Ne	etwork	Destination Host/Netwo	ı ork	Service	Log Le Interva	avel I	Time Range	Add ACL
10				İ							Add ACE
											EditACE
											Delete
											Move Up
											Move Down
•										•	
🖌 🔨	ow traffic	O C) eny traffic								
				0K		Cancel		Help]		

8. Définissez l'entrée de contrôle d'accès (ACE) que vous souhaitez ajouter.

Dans cet exemple, le premier ACE de la liste de contrôle d'accès 10 autorise l'accès IP au sous-réseau Payroll à partir de n'importe quelle source.

Remarque : par défaut, ASDM sélectionne uniquement TCP comme protocole. Vous devez choisir IP si vous souhaitez autoriser ou refuser aux utilisateurs un accès IP complet. Cliquez sur OK quand vous avez terminé.

d Excellued 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: 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	
ease enter the description below (ontional):	
ampil ID accore from Ably accore to the new roll such	ant (10 0 20 0 (24)
ermit in access from ANY source to the payroll sub	net (10.8.20.0724)
]	Þ

9. L'ACE que vous venez d'ajouter apparaît maintenant dans la liste. Choisissez à nouveau Add ACE pour ajouter des lignes supplémentaires à la liste d'accès.

Configure ACLs.	
# Rule Enabled Action Source Host/Network Destination Host/Network Service Log Level Interval Time Range	Add ACL
□ 10	Add ACE
1 🔽 🗹 🏶 any 🗖 🖬 10.8.28.0/24 😰 ip Not Applied	Edit ACE
	Delete
	Mauritin
	Move up
	Move Down
Allow traffic O Deny traffic	
OK Cancel Help	

Dans cet exemple, une deuxième ACE est ajoutée à la liste de contrôle d'accès 10 afin d'autoriser l'accès au sous-réseau Intranet.

Rotion		Time Denge
Action		Time Range
Permit	C Denv	
	,	Default Syslog More Options
Source Host/N	etwork	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 💌
Protocol and S	ervice	
СТСР С	UDP CICMP CIP	Manage Service Groups
IP Protocol		
IP protocol:	any	
	description below (optional):	
lease enter the		
lease enter the ermit IP access	; from ANY source to the subnet use	d by all employees (10.8.27.0 /24)
lease enter the ermit IP access	s from ANY source to the subnet use	d by all employees (10.8.27.0/24)
lease enter the ermit IP access	s from ANY source to the subnet use	d by all employees (10.8.27.0/24)

10. Cliquez sur OK une fois que vous avez terminé d'ajouter des ACE.

ĩ¢/	CL Ma	nager							×
Co	nfigur	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
E	10								Add ACE
	1	V	~	🧼 any	A 10.5.28.0/24	. ™ ip		Not Applied	EditACE
	2		1	🧇 any	g ^{GI} 10.8.27.0/24	📂 ip		Not Applied	<u></u>
									Delete
									Move Up
									Move Down
•								Þ	
	🖉 Allo	ow traffic	Q (Denytraffic					
				0	Canc	el	Help		

11. Sélectionnez la liste de contrôle d'accès que vous avez définie et renseignée au cours des dernières étapes comme filtre de votre stratégie de groupe. Cliquez sur OK lorsque vous avez terminé.

Check an Inherit checkbo	x to let the corr	esponding setting take i	ts value from the default group pol
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		minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary;
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🗵 Inherit		

12. Cliquez sur Apply pour envoyer les modifications au PIX.



13. Si vous l'avez configuré pour le faire sous Options > Préférences, l'ASDM prévisualise les commandes qu'il est sur le point d'envoyer au PIX. Cliquez sur Envoyer.

🖆 Preview CLI Commands	×
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the PIX, click Send. To not send the commands and continue making changes in ASDM, click Cancel.	
access-list 10 line 1 remark permit IP access from ANY source to the payroll subnet (10.8.28.0 /24 access-list 10 line 2 extended permit ip any 10.8.28.0 255.255.255.0 access-list 10 line 3 remark permit IP access from ANY source to the subnet used by all employed access-list 10 line 4 extended permit ip any 10.8.27.0 255.255.255.0 group-policy payroll attributes vpn-filter value 10	
▼ Send Cancel	-

14. Appliquez la stratégie de groupe qui vient d'être créée ou modifiée au groupe de tunnels correct. Cliquez sur Tunnel Group dans le cadre de gauche.



15. Choisissez le groupe de tunnels auquel vous souhaitez appliquer la stratégie de groupe et cliquez sur Edit.

File Rules Ser	1 for PIX - 10.89.129.147 arch Options Tools Wizards H	qle			
Home C	Configuration Monitoring Ba	ck Forward Search	h Refresh	Save Help	CISCO STREES
Nterfaces Security Policy NAT NAT Security Policy NAT Security NAT Security Routing Clobel Objects Froperties	Configuration - VFN - General - Tu Configuration - VFN - General - Tu Configuration - VFN - General - Tu Configuration - Tu	Innel Group	ups. A VPN tunnel g ection. Type ipsec-ra ipsec-ra ipsec-ra ipsec-l2l be used when parsi als are being negotia None V	roup represents a connection Group Policy engineering DittomPolicy DittomPolicy DittomPolicy	specific record for a
Configuration cha	nges særed successfullv		icisco ina	A (2)	∰ 3/13/06 3:22:31 PM UTC

16. Si votre stratégie de groupe a été créée automatiquement (voir l'étape 2), vérifiez que la stratégie de groupe que vous venez de configurer est sélectionnée dans la liste déroulante. Si votre stratégie de groupe n'a pas été configurée automatiquement, sélectionnez-la dans la liste déroulante. Cliquez sur OK lorsque vous avez terminé.

📸 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 AAA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

17. Cliquez sur Apply et, si vous y êtes invité, cliquez sur Send pour ajouter la modification à la configuration PIX.

Si la stratégie de groupe a déjà été sélectionnée, vous pouvez recevoir un message indiquant « Aucune modification n'a été apportée ». Click OK.

18. Répétez les étapes 2 à 17 pour tous les groupes de tunnels supplémentaires auxquels vous souhaitez ajouter des restrictions.

Dans cet exemple de configuration, il est également nécessaire de restreindre l'accès des ingénieurs. Bien que la procédure soit la même, voici quelques fenêtres sur lesquelles les différences sont notables :

• Nouvelle liste d'accès 20

🖆 ACL Manager									
Co	Configure ACLs.								
	#	Rule Enabled	Action	Source HastNetwork	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
	1	S	~	🧼 any	A 10.8.28.0/24	😕 ip		Not Applied	EditACE
	2	V	~	🧼 any	AD 10.8.27.0/24	💌 ip		Not Applied	Lantie
G	20								Delete
	1	V	~	🧼 any	A 192.168.1.0/24	😕 ip		Not Applied	- Hannellin - [
	2		1	🤹 any	10.8.27.0/24	🕑 ip		Not Applied	Move Up
Г									Moye Down
								×	
Allow traffic 3 Deny traffic									
				04	Cance	a [Help		

• Sélectionnez Access List 20 comme filtre dans la politique de groupe Engineering.

Check an Inherit checkbox	to let the com	esponding setting take	its value from the default group po
Tunneling Protocols:	🔽 Inherit	F IPSec	
Filter:	🗆 Inherit	20	▼ Manage
Connection Settings Access Hours:	Inherit		New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Time	: 🔽 Inherit	Unlimited	minutes
Idle Timeout:	🔽 Inherit	🗖 Unlimited 🗌	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🗹 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

 Vérifiez que la stratégie de groupe Engineering est définie pour le groupe de tunnels Engineering.

薩 Edit Tunnel Group	×
Name: engineering Type: ipsec-ra	
General IPSec	
Configure concrete access attributes from the following cub take	
Regis Add Client Address Assignment Advensed	
Dasine [Avvv] Cilent 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 Hain	

Configurer l'accès via CLI

Complétez ces étapes pour configurer l'appliance de sécurité à l'aide de l'interface CLI :

Remarque : certaines des commandes affichées dans ce résultat sont ramenées à une deuxième ligne pour des raisons spatiales.

1. Créez deux listes de contrôle d'accès différentes (15 et 20) qui sont appliquées aux utilisateurs lorsqu'ils se connectent au VPN d'accès à distance. Cette liste d'accès est appelée ultérieurement dans la configuration.

<**#root>** 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 10.8.28.0 255.255.255.0
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
```

 Créez deux pools d'adresses VPN différents. Créez-en un pour Payroll et un pour les utilisateurs distants Engineering.

<#root>

```
ASAwCSC-CLI(config)#
ip local pool Payroll-VPN
172.10.1.100-172.10.1.200 mask 255.255.255.0
```

ASAwCSC-CLI(config)#

ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0 3. Créez des stratégies pour Payroll qui ne s'appliquent qu'à leur connexion.

```
<#root>
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)#
vpn-tunnel-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. Cette étape est identique à l'étape 3, sauf qu'elle concerne le groupe Ingénierie.

```
<#root>
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-group-policy)# 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. Créez des utilisateurs locaux et affectez les attributs que vous venez de créer à ces utilisateurs pour limiter leur accès aux ressources.

```
<#root>
ASAwCSC-CLI(config)#
username engineer password ciscol23
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. Créez des groupes de tunnels qui contiennent des stratégies de connexion pour les utilisateurs de la paie.

```
<#root>
```

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. Créez des groupes de tunnels qui contiennent des stratégies de connexion pour les utilisateurs Engineering.

<#root> 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
```

Une fois votre configuration entrée, vous pouvez voir cette zone en surbrillance dans votre configuration :

Nom du périphérique 1 <#root> ASA-AIP-CLI(config)# show running-config ASA Version 7.2(2) ! hostname ASAwCSC-ASDM domain-name corp.com enable password 9jNfZuG3TC5tCVH0 encrypted names I interface Ethernet0/0 nameif Intranet security-level 0 ip address 10.8.27.2 255.255.255.0 I interface Ethernet0/1 nameif Engineer security-level 100 ip address 192.168.1.1 255.255.255.0 I 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
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 6XmYwQOO9tiYnUDN 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
I
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
ļ
service-policy global_policy global
prompt hostname context
Cryptochecksum:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

Vérifier

Utilisez les fonctionnalités de surveillance de l'ASDM pour vérifier votre configuration :

1. Sélectionnez Monitoring > VPN > VPN Statistics > Sessions.

Vous voyez les sessions VPN actives sur le PIX. Sélectionnez la session qui vous intéresse et cliquez sur Détails.

File Rules Sear	for PIX - 10.89.129.147 ch Options Tools Wizards	Help			X
Home Co	onfiguration Monitoring	Back Forward Sea	rch Refresh	🔜 🢡 Save Help	Cisco Systems
Interfaces	Monitoring > VPN > VPN Statistic VPN Connection Grapi IPSec Tunnels VPN Statistics Crypto Statistics Crypto Statistics Global IKE/IPSec S Protocol Statistics Sessions	s > Sessions Sessions Remote Access Filter By: Remote Acc Username confrollert Df ga to sort VPN sessions, rig Logout By: - All Sess	LAN-to-LAN	Total 0 sions I Assigned IP Address Public IP Address 10 8:27:50 172:22:1:165	Total Cumulative 1 3 Fitter Protocol Encryption Logout 3DES Ping Soft Order from popup menu. ogout Sessions
Data Refreshed Su	ccessfully.		cisco I	NA (2) 🔰 🛃 🐱	🔒 🔰 🔓 3/13/06 8:36:34 PM UTC

2. Sélectionnez l'onglet ACL.

Les hits de liste de contrôle d'accès reflètent le trafic qui circule dans le tunnel depuis le client vers le ou les réseaux autorisés.

🔂 Session Details					x				
-Remote Detailed -									
Usemame	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Client Type Version				
controller1	DfttGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES	20:35:08 UTC Mon Mar 13 2006 0h:08m:58s	WinNT 4.8.00.0440				
controlleri DftOrpPolicy 10.8.27.50 IPSec 20.35.08 UTC Mon Mar 13 2006 WinNT s									
				Last Update	a: 3/13/06 2:47:17 PM				

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Exemple de configuration des appareils de sécurité adaptatifs Cisco ASA 5500 ASA en tant que serveur VPN distant à l'aide de l'ASDM
- <u>Exemples de configuration et notes techniques des appareils de sécurité de la gamme Cisco</u>
 <u>PIX 500</u>
- <u>Exemples de configuration et notes techniques des appareils de sécurité adaptatifs Cisco</u> <u>ASA 5500</u>
- <u>Exemples de configuration de client VPN Cisco et notes techniques</u>
- <u>Assistance et documentation techniques Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.