SDM : Exemple de configuration site à site VPN IPSec VPN entre ASA/PIX et un routeur IOS

Contenu

Introduction Conditions préalables **Conditions requises** Composants utilisés **Produits connexes** Conventions Configuration Diagramme du réseau Configuration ASDM du tunnel VPN Configuration SDM du routeur Configuration de l'interface de ligne de commande ASA Configuration de la CLI du routeur Vérifiez Dispositif de sécurité ASA/PIX - Commandes show Routeur IOS distant - Commandes show Dépannez Informations connexes

Introduction

Ce document fournit un exemple de configuration pour le tunnel IPsec LAN à LAN (site à site) entre des dispositifs de sécurité Cisco (ASA/PIX) et un routeur Cisco IOS. Des routes statiques sont utilisées à des fins de simplicité.

Consultez <u>Exemple de configuration d'un dispositif de sécurité PIX/ASA 7.x sur un tunnel IPsec</u> <u>LAN à LAN de routeur IOS</u> pour en savoir plus sur le même scénario où le dispositif de sécurité PIX/ASA exécute la version du logiciel *7.x*.

Conditions préalables

Conditions requises

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

- La connectivité IP de bout en bout doit être établie avant de commencer cette configuration.
- La licence du dispositif de sécurité doit être activée pour le chiffrement Data Encryption

Standard (DES) (à un niveau de chiffrement minimal).

Composants utilisés

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

- Dispositif de sécurité adaptatif dédié (ASA) Cisco avec la version 8.x et versions ultérieures
- ASDM version 6.x. et ultérieures
- Routeur Cisco 1812 avec le logiciel Cisco IOS® Version 12.3
- Cisco Security Device Manager (SDM) version 2.5

Remarque: Référez-vous à <u>Permettre l'accès HTTPS pour l'ASDM</u> afin de permettre l'ASA d'être configuré par l'ASDM.

Remarque: Consultez <u>Configuration de routeur de base à l'aide de SDM</u> afin de permettre la configuration du routeur par SDM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

Remarque: Référez-vous à la <u>Configuration Professional : Site à site IPsec VPN entre ASA/PIX et</u> <u>un exemple de configuration de routeur IOS</u> pour une configuration semblable utilisant le Cisco Configuration Professional sur le routeur.

Produits connexes

Cette configuration peut également être utilisée avec le dispositif de sécurité de la gamme Cisco PIX 500, qui exécute la versions 7.x et les versions ultérieures.

Conventions

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

Configuration

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses <u>RFC 1918</u> qui ont été utilisées dans un environnement de laboratoire.

- <u>Configuration ASDM du tunnel VPN</u>
- Configuration SDM du routeur
- <u>Configuration de l'interface de ligne de commande ASA</u>
- <u>Configuration de la CLI du routeur</u>

Configuration ASDM du tunnel VPN

Pour créer le tunnel VPN, exécutez les étapes suivantes :

 Ouvrez votre navigateur et entrez https://<Adresse IP de l'interface d'ASA qui a été configurée pour l'accès à ASDM> pour accéder à l'ASDM sur l'ASA.Prenez soin d'autoriser tous les avertissements que votre navigateur vous donne en ce qui concerne l'authenticité de certificat SSL. Le nom d'utilisateur par défaut et le mot de passe sont tous deux vides.L'ASA présente cette fenêtre pour permettre le téléchargement de l'application ASDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet Java.



- 2. Cliquez sur **Download ASDM Launcher and Start ASDM** pour télécharger le programme d'installation de l'application ASDM.
- 3. Une fois le lanceur d'ASDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco ASDM.
- 4. Entrez l'adresse IP pour l'interface que vous avez configurée avec la commande http -, ainsi qu'un nom d'utilisateur et un mot de passe, le cas échéant.Cet exemple utilise cisco123 comme nom d'utilisateur et cisco123 comme mot de

	📬 Cisco ASDM Launch	er v1.5(30)	
		cisco	
	Device IP Address / Name:	10.77.241.111	*
	Username:	cisco123	
	Password:	****	
	🔄 Run in Demo Mode		
passe.		.0	1 🗐 👙 🔒

5. Exécutez l'**Assistant IPsec VPN** une fois que l'application ASDM se connecte à l'ASA.

isco ASDM 6.1 for ASA - 10.77.241.111		
File View Tools Wizards Window Help	Look For:	cisco
Home IPsec VPN Wizard SSL VPN Wizard SSL VPN Wizard High Availability and Scalability Wizard Packet Capture Wizard	ntion Interface Status	
General License Host Name: ciscoasa.default.domain.invalid ASA Version: 8.0(2) Device Uptime: 14d 3h 1m 51s ASDM Version: 6.1(3) Device Type: ASA 5510 Firewall Mode: Routed Context Mode: Single	Interface IP Address/Mask Li dmz 10.77.241.111/26 • inside 10.10.10.1/24 • outside 172.16.1.1/24 •	ne Li up O up O up O
Total Flash: 64 MB Total Memory: 256 MB VPN Tunnels IKE: 0 IPSec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0	Select an interface to view input and output Kbp Traffic Status Connections Per Second Usage	5
System Resources Status CPU CPU Usage (percent)	0 20:41 20:42 20:43 UDP: 0 TCP: 0 Total: 0	20:44
cisco123	15 🛃 💽 4/6/0	9 8:45:42 PM UTC

6. Choisissez le type de tunnel IPSec VPN **Site-to-Site** et cliquez sur **Next**, comme indiqué ici.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Franch	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type: Site-to-Site VPN
THE REAL	Site-to-Site
	Remote Access Remote Access
G \$-	VPN Tunnel Interface:
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

7. Spécifiez l'adresse IP externe du partenaire distant. Entrez les informations d'authentification à utiliser, qui sont la clé pré-partagée dans cet exemple. La clé pré-partagée utilisée dans cet exemple est cisco123. La valeur Tunnel Group Name sera votre adresse IP externe par défaut si vous configurez un VPN L2L. Cliquez sur Next (Suivant).

🖆 VPN Wizard		×
VPN Wizard	Remote Site Peer (Step 2 of 6)	
VPN Wizard	Remote Site Peer (Step 2 of 6) Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 172.17.1.1 Authentication Method • Pre-shared key Pre-Shared Key: clsco123 • Certificate Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: • Certificate Name: • Challenge/response authentication (CRACK)	
	peer's identity.	
	Tunnel Group Name: 172.17.1.1	
	< Back Next > Finish Cancel Help	

 Spécifiez les attributs à utiliser pour l'IKE, également connus sous le nom de « Phase 1 ». Ces attributs doivent être identiques sur l'ASA et sur le routeur IOS. Cliquez sur Next (Suivant).

🖆 VPN Wizard		\mathbf{X}		
VPN Wizard	IKE Policy (Step 3 of 6)			
Branch Branch Fisp Homo Homo	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.			
Notwork	Encryption: DES			
A A A A A A A A A A A A A A A A A A A	Authentication: SHA			
	DH Group:			
	< Back Next Finish Cancel Help	2		

 Spécifiez les attributs à utiliser pour IPsec, également connus sous le nom de « Phase 2 ». Ces attributs doivent correspondre sur l'ASA et sur le routeur IOS. Cliquez sur Next (Suivant).

🖆 VPN Wizard	
VPN Wizard	IPsec Encryption and Authentication (Step 4 of 6)
Branch Branch Fisp Hanve Natiwork	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.
	Encryption: DES
	Authentication: SHA
C.A.	
	< Back Next > Finish Cancel Help

10. Spécifiez les hôtes dont le trafic devrait être autorisé à passer par le tunnel VPN. Dans cette étape, vous devez fournir les valeurs **Local Networks** et **Remote Networks** pour le tunnel VPN. Cliquez sur le bouton en regard de **Local Networks**, comme indiqué ici, pour choisir l'adresse du réseau local dans la liste déroulante.

🖆 VPN Wizard		\times
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Branch Branch	An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.	
	Action: Protect: Do not Protect	
Home	Local Networks: any	
Corporatu Network	Remote Networks: any	
	Exempt ASA side host/network from address translation:	
	< Back Next > Finish Cancel Help	2

11. Choisissez l'adresse **Local Network**, puis cliquez sur **OK**, comme indiqué ici.

🖆 Browse Local Netw	orks			
🗣 Add 👻 📝 Edit 🗊	Delete Q			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
-Network Objects	1		•	
	0.0.0.0	0.0.0		
- 🛃 dmz-network	10.77.241.64	255.255.255.192		
🚽 📑 🖬 inside-network	10.10.10.0	255.255.255.0		
	k 172.16.1.0	255.255.255.0		
Selected Local Networks -				
Local Networks ->	any			
	J [,			
			0	K Cancel

12. Cliquez sur le bouton en regard de **Remote Networks**, comme indiqué ici, pour choisir l'adresse du réseau distant dans la liste déroulante.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protects remote sites. Please ider	s data exchanged by selected hosts and networks at the local and htify hosts and networks to be used in the IPsec tunnel.
	Action: (Protect O Do not Protect
Home	Local Networks: in	nside-network/24
Network	Remote Networks: a	any R
	🔽 Exempt ASA side ho	ost/network from address translation:
		< Back Next > Finish Cancel Help

13. Choisissez l'adresse Remote Network, puis cliquez sur OK, comme indiqué ici. Remarque: Si le réseau distant ne figure pas dans la liste, il doit être ajouté à la liste en cliquant sur

Add.

🖆 Browse Remote Net	tworks			
🗣 Add 🝷 🗭 Edit 🁔	Delete 🔍			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
Network Objects				
	0.0.0.0	0.0.0		
- 📑 dmz-network	10.77.241.64	255.255.255.192		
🚮 inside-network	10.10.10.0	255.255.255.0		
📲 outside-netwo	k 172.16.1.0	255.255.255.0		
in 10.20.10.0	10.20.10.0	255.255.255.0		
Remote Network	5			
Remote Networks ->				
				K Cancel

14. Activez la case à cocher **Exempt ASA side host/network from address translation** afin d'empêcher le trafic du tunnel de subir la **traduction d'adresses de réseau**. Cliquez ensuite sur

Next.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protec remote sites. Please id	ts data exchanged by selected hosts and networks at the local and entify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Home	Local Networks:	inside-network/24
Network	Remote Networks:	10.20.10.0/24
	Exempt ASA side	host/network from address translation:
		< Back Next Finish Cancel Help

15. Les attributs définis par l'assistant VPN sont affichés dans ce récapitulatif. Vérifiez une deuxième fois la configuration et cliquez sur **Finish** quand vous êtes sûr que les paramètres sont

corrects.



Configuration SDM du routeur

Exécutez les étapes suivantes pour configurer le tunnel VPN site à site sur le routeur Cisco IOS :

 Ouvrez votre navigateur et entrez https://<Adresse IP de l'interface du routeur qui a été configurée pour l'accès à SDM> pour accéder au SDM sur le routeur.Prenez soin d'autoriser tous les avertissements que votre navigateur vous donne en ce qui concerne l'authenticité de certificat SSL. Le nom d'utilisateur par défaut et le mot de passe sont tous deux vides.Le routeur présente cette fenêtre pour permettre le téléchargement de l'application SDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet



- Le téléchargement de SDM commence alors. Une fois le lanceur de SDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco SDM.
- 3. Entrez les valeurs **Username** et **Password** si vous en avez spécifié une, puis cliquez sur **OK**.Cet exemple utilise **cisco123** comme nom d'utilisateur et **cisco123** comme mot de

	Authenticatio	on Required 🛛 🔊 🔊 🔊	<	
	کن Java			
	Enter login det /10.77.241.10	ails to access level_15 or view_access on 9:		
	User name:	cisco123		
	Password:	•••••		
	Save this password in your password list			
		OK Cancel		
passe.	Authentication	scheme: Basic		

4. Choisissez Configure->VPN->Site-to-Site VPN et cliquez sur la case d'option en regard de

Create Site-to-Site VPN sur la page d'accueil de SDM. Cliquez ensuite sur Launch The selected Task, comme indiqué



5. Choisissez **Step by step wizard** pour poursuivre la configuration :



6. Dans la fenêtre suivante, indiquez les informations VPN Connection Information dans les espaces respectifs. Sélectionnez l'interface du tunnel VPN dans la liste déroulante. Ici, FastEthernet0 est choisi. Dans la section Peer Identity, choisissez Peer with static IP address et fournissez l'adresse IP de l'homologue distant. Fournissez ensuite la valeur Preshared key (cisco123 dans cet exemple) dans la section Authentication, comme indiqué. Cliquez ensuite sur Next.

Site-to-Site VPN Wizard		
VPN Wizard	VPN Connection Information Select the interface for this VPN connection:	FastEthernet0 Details
	Peer Identity Select the type of peer(s) used for this VPN connection: Enter the IP address of the remote peer:	Peer with static IP address
RA	Authentication Authentication ensures that each end of the Pre-shared Keys pre-shared key: Re-enter Key:	VPN connection uses the same secret key.
		<back next=""> Finish Cancel Help</back>

7. Cliquez sur Add pour ajouter des propositions d'IKE qui spécifient l'algorithme de chiffrement, l'algorithme d'authentification et la méthode d'échange de clés.

Site-to-Site VPN Wizard		\times			
VPN Wizard IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key ex- method that is used by this router when negotiating a VPN connection with the remotive device. For the VPN connection to be established with the remote device, the remotive device should be configured with at least one of the policies listed below. Click the Add button to add more policies and the Edit button to edit an existing					
	Priority Encryption Hash D-H Group Authentication Type				
	Add Edit				
	Sack Next > Finish Cancel Help	,			

8. Fournissez l'algorithme de chiffrement, l'algorithme d'authentification et la méthode d'échange de clés, comme indiqué ici, puis cliquez sur OK. Les valeurs d'algorithme de chiffrement, d'algorithme d'authentification et de méthode d'échange de clés doivent correspondre aux données fournies dans

Add IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
Encryption:	D-H Group: group2
Hash: SHA_1	Lifetime: 24 0 0 HH:MM:SS
<u>ok</u>	Cancel Help
Α.	

9. Cliquez sur **Next**, comme indiqué ici.

Site-to-Site VPN Wizard							
VPN Wizard	IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below. Click the Add button to add more policies and the Edit button to edit an existing policy.						
	Priorit	Encryption	Hash	D-H Group	Authentication	Туре	
	1	3DES	SHA_1	group2	PRE_SHARE	User Defined	
	2	DES	SHA_1	group1	PRE_SHARE	User Defined	
	Add	Edit					
				« Back Next	t» Finish C	ancel Help	

10. Dans cette nouvelle fenêtre, les détails Transform Set doivent être fournis. Le jeu de transformations (Transform Set) spécifie les algorithmes de chiffrement et d'intégrité utilisés pour protéger les données dans le tunnel VPN. Cliquez alors sur Add pour fournir ces détails. Vous pouvez ajouter autant de jeux de transformations que nécessaire en cliquant sur Add et en fournissant les détails.

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel. Since communicate, the remote dev one selected below. Click the Add button to add a transform set. Select Transform Set SDM Default Transform Details of the specified tra	encryption and aut the two devices mo ice must be config a new transform se a Set nsform set	nentication algorithm ust use the same alg ured with the same t it and the Edit butto	is used to protect the porithms to transform set as the in to edit the specified	1
	Name ESP-3DES-SHA	ESP Encryption ESP_3DES	ESP Integrity ESP_SHA_HMAC	AH Integrity	
		< <u>{</u>	Back Next > Fini	sh Cancel He	lp

11. Fournissez les détails du jeu de transformations **Transform Set** (**Encryption Algorithm et Integrity Algorithm**), puis cliquez sur **OK**, comme

	Add Transform Set 🛛 🛛 🔀
	Name: ASA-IPSEC
	✓ Data integrity with encryption (ESP)
	Integrity Algorithm: ESP_SHA_HMAC 💌
	Encryption Algorithm: ESP_DES
	Show Advanced >>
indiqué	OK Cancel Help

12. Choisissez le jeu de transformations requis **Transform Set** à utiliser dans la liste déroulante, comme indiqué.

Site-to-Site VPN Wizard		×
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set SDM Default Transform Set SDM Default Transform Set	
	Add Edit	
	Back Next > Finish Cancel Hei	р

13. Cliquez sur **Next** (Suivant).

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the o data in the VPN tunnel. Since communicate, the remote dev one selected below. Click the Add button to add a transform set. Select Transform Set ASA IPSEC Details of the specified tra	encryption and aut the two devices mo ice must be config a new transform se new transform set	hentication algorithm ust use the same alg ured with the same t t and the Edit butto	ns used to protect the gorithms to transform set as the in to edit the specified	
	Add Edit	ESP Encryption ESP_DES	ESP Integrity ESP_SHA_HMAC	AH Integrity	
		< [Back Next > Fini	sh Cancel Hel	р

14. Dans la fenêtre suivante, fournissez les détails relatifs au trafic à protéger (Traffic to protect) via le tunnel VPN. Fournissez les réseaux sources et de destination du trafic à protéger de sorte que le trafic entre les réseaux sources et de destination spécifiés soit protégé. Dans cet exemple, le réseau source est 10.20.10.0 et le réseau de destination est 10.10.10.0. Cliquez ensuite sur Next.

Site-to-Site VPN Wizard		
	Traffic to protect IPSec rules define the traffic, such as file transferenced by this VPN connection. Other data tradevice. You can protect all traffic between a part specify an IPSec rule that defines the traffic type Protect all traffic between the following subnet Local Network Enter the IP address and subnet mask of the network where IPSec traffic originates. IP Address: 10.20.10.0 Subnet Mask:	ers (FTP) and e-mail (SMTP) that will be affic will be sent unprotected to the remote icular source and destination subnet, or is to be protected. ts Remote Network Enter the IP Address and Subnet Mask of the destination Network. IP Address: 10.10.10.0 Subnet Mask 255.255.255.0 or 24
		Back Next > Finish Cancel Help

15. Cette fenêtre montre le résumé de la configuration VPN site à site effectuée. Activez la case à cocher Test VPN Connectivity after configuring si vous voulez tester la connectivité VPN. Ici, la case est cochée car la connectivité doit être vérifiée. Cliquez ensuite sur Finish.

Site-to-Site VPN Wizard						
VPN Wizard	Summary of the Co	nfiguration				
	Click Finish to delive Interface:FastEtherr Peer Device:172.16 Authentication Type pre-shared key:***** IKE Policies: Hash DI SHA_1 gr SHA_1 gr SHA_1 gr Transform Sets: Name:ASA ESP Encry ESP Integr Mode:TUN	er the configuration to the net0 3.1.1 .: Pre-shared key *** H Group roup1 roup2 VIPSEC ption:ESP_DES ity:ESP_SHA_HMAC INEL	Authentication PRE_SHARE PRE_SHARE	Encryption DES 3DES		
			<back next≻<="" th=""><th>Finish</th><th>ancel H</th><th>Help</th></back>	Finish	ancel H	Help

16. Cliquez sur **Start**, comme indiqué, pour vérifier la connectivité VPN.

VPN Troubleshooting	
Tunnel Details	
Interface: FastEthernet0	Peer: 172.16.1.1
	🔳 Summany 🖉 Details
Activity	Status
Failure Reason(s)	Recommended Action(s)
Start Save Report.	t Close Help

17. La fenêtre suivante présente le résultat du **test de connectivité VPN**. Ici, vous pouvez voir si le tunnel est activé ou désactivé (**Up ou Down**). En cet exemple de configuration, le tunnel est **Up**, comme indiqué en vert.

VPN Troubleshooting		X
Tunnel Details		
Interface: FastEthernet0	Peer: 172.16.1.1	
	🔲 Summary	🕰 Details
Activity	State	at a st
Checking the tunnel status	QU	p
Failure Reason(s)	Recommended Action(s)	
Start Save Report	Close Help	

Cela termine la configuration sur le routeur Cisco IOS.

Configuration de l'interface de ligne de commande ASA

ASA
ASA# show run : Saved ASA Version 8.0(2) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted names ! !
Configure the outside interface. ! interface Ethernet0/1
nameif outside security-level 0 ip address 172.16.1.1
255.255.255.0 ! Configure the inside interface. !
interface Ethernet0/2 nameif inside security-level 100
ip address 10.10.10.1 255.255.255.0 ! Output
<pre>suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode</pre>
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list 100 extended permit
ip any any access-list inside_nat0_outbound extended
permit ip 10.10.10.0 255.255.255.0 10.20.10.0
255.255.255.0 ! This access list
(inside_nat0_outbound) is used ! with the nat zero
command. This prevents traffic which ! matches the

access list from undergoing network address translation (NAT). !--- The traffic specified by this ACL is traffic that is to be encrypted and !--- sent across the VPN tunnel. This ACL is intentionally !--- the same as (outside_1_cryptomap). !--- Two separate access lists should always be used in this configuration. access-list outside_1_cryptomap extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (outside_cryptomap) is used !--- with the crypto map **outside_map** !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside_nat0_outbound). !--- Two separate access lists should always be used in this configuration. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm-613.bin asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 1 10.10.10.0 255.255.255.0 nat (inside) 0 access-list inside_nat0_outbound !--- NAT 0 prevents NAT for networks specified in !--- the ACL inside_nat0_outbound. access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 http server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location no snmp-server contact !---PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 1 match address outside_1_cryptomap !--- Define which traffic should be sent to the IPsec peer. crypto map outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec peer crypto map outside_map 1 set transform-set ESP-DES-SHA !--- Sets the IPsec transform set "ESP-AES-256-SHA" !--- to be used with the crypto map entry "outside_map". crypto map outside_map interface outside !--- Specifies the interface to be used with !--- the settings defined in this configuration. !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 10 authentication pre-share encryption des hash sha group 1 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 threatdetection basic-threat threat-detection statistics access-list ! tunnel-group 172.17.1.1 type ipsec-121 !--- In order to create and manage the database of connection-specific !--- records for ipsec-121-IPsec (LAN-to-LAN) tunnels, use the command !--- tunnel-group in global configuration mode. !--- For L2L connections the name of the tunnel group **MUST** be the IP !--- address of the IPsec peer. tunnel-group 172.17.1.1 ipsecattributes pre-shared-key * !--- Enter the pre-sharedkey in order to configure the !--- authentication method. telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! class-map inspection_default match default-inspection-traffic ! ! !-- Output suppressed! username ciscol23 password ffIRPGpDSOJh9YLq encrypted privilege 15 Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end

Configuration de la CLI du routeur

Routeur Building configuration ... Current configuration : 2403 bytes version 12.3 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! hostname R3 ! boot-start-marker boot-end-marker ! no logging buffered ! username ciscol23 privilege 15 password 7 1511021F07257A767B no aaa new-model ip subnet-zero ! ! ip cef ! 1 ip ips po max-events 100 no ftp-server write-enable ! !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and Policy details are hidden as the default values are chosen. crypto isakmp policy 2 authentication pre-share !---Specifies the pre-shared key "cisco123" which should !--- be identical at both peers. This is a global !--configuration mode command. crypto isakmp key cisco123 address 172.16.1.1 ! ! !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ASA-IPSEC espdes esp-sha-hmac ! !--- !--- Indicates that IKE is used to establish !--- the IPsec Security Association for protecting the !--- traffic specified by this crypto map entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to172.16.1.1 !--- !--- Sets the IP address of the remote end. set peer 172.16.1.1 !--- !--- Configures IPsec to use the transform-set !--- "ASA-IPSEC" defined earlier in this configuration. set transform-set ASA-**IPSEC** !--- Specifies the interesting traffic to be encrypted. match address 100 ! ! ! !--- Configures the interface to use the !--- crypto map "SDM_CMAP_1" for **IPsec.** interface FastEthernet0 ip address 172.17.1.1 255.255.255.0 duplex auto speed auto crypto map SDM_CMAP_1 ! interface FastEthernet1 ip address 10.20.10.2 255.255.255.0 duplex auto speed auto ! interface FastEthernet2 no ip address ! interface Vlan1

```
ip address 10.77.241.109 255.255.255.192 ! ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2 ip route
10.77.233.0 255.255.255.0 10.77.241.65 ip route
172.16.1.0 255.255.255.0 172.17.1.2 ! ! ip nat inside
source route-map nonat interface FastEthernet0 overload
! ip http server ip http authentication local ip http
secure-server ! !--- Configure the access-lists and map
them to the Crypto map configured. access-list 100
remark SDM_ACL Category=4 access-list 100 remark IPSec
Rule access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255 ! ! ! ! --- This ACL 110 identifies
the traffic flows using route map access-list 110 deny
ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255 access-list
110 permit ip 10.20.10.0 0.0.0.255 any route-map nonat
permit 10 match ip address 110 ! control-plane ! ! line
con 0 login local line aux 0 line vty 0 4 privilege
level 15 login local transport input telnet ssh ! end
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'<u>Outil Interpréteur de sortie</u> (clients <u>enregistrés</u> uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- <u>Dispositif de sécurité PIX Commandes show</u>
- Routeur IOS distant Commandes show

Dispositif de sécurité ASA/PIX - Commandes show

• show crypto isakmp sa — Affiche toutes les SA IKE en cours au niveau d'un

hOmologue.ASA#**show crypto isakmp sa** Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 172.17.1.1 Type : L2L Role : initiator Rekey : no State : MM_ACTIVE

• show crypto ipsec sa — Affiche toutes les SA IPsec en cours au niveau d'un

homologue.ASA#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1 local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.20.10.0/255.255.0/0/0) current_peer: 172.17.1.1 #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp sas: spi: 0xB7C1948E (3082917006) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x434C4A7F (1129073279) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y

Routeur IOS distant - Commandes show

• show crypto isakmp sa — Affiche toutes les SA IKE en cours au niveau d'un homologue.Router#show crypto isakmp sa dst src state conn-id slot status 172.17.1.1

172.16.1.1 **QM_IDLE** 3 0 **ACTIVE**

• show crypto ipsec sa — Affiche toutes les SA IPsec en cours au niveau d'un

homologue.Router#show crypto ipsec sa interface: FastEthernet0 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) current_peer 172.16.1.1 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68 #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500 current outbound spi: 0xB7C1948E(3082917006) inbound esp sas: spi: 0x434C4A7F(1129073279) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3004) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xB7C1948E(3082917006) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3002) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:

• show crypto engine connections active — Affiche les connexions actuelles et les informations relatives aux paquets chiffrés et déchiffrés (routeur seulement).Router#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 3 FastEthernet0 172.17.1.1 set HMAC_SHA+DES_56_CB 0 0 2001 FastEthernet0 172.17.1.1 set DES+SHA 0 59 2002 FastEthernet0 172.17.1.1 set DES+SHA 59 0

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'<u>Outil Interpréteur de sortie</u> (clients <u>enregistrés</u> uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Remarque: Consultez <u>Informations importantes sur les commandes debug</u> et <u>Dépannage de la</u> <u>sécurité IP - Présentation et utilisation des commandes debug</u> avant d'utiliser les commandes **debug**.

- debug crypto ipsec 7 Affiche les négociations IPsec de la phase 2.debug crypto isakmp 7
 Affiche les négociations ISAKMP de la phase 1.
- debug crypto ipsec Affiche les négociations IPsec de la phase 2.debug crypto isakmp affiche les négociations ISAKMP de la phase 1.

Reportez-vous à <u>Solutions de dépannage les plus courantes concernant un VPN IPsec L2L et</u> <u>d'accès à distance</u> pour plus d'informations sur le dépannage d'un VPN site à site.

Informations connexes

- Logiciels pare-feu Cisco PIX
- <u>Cisco Adaptive Security Device Manager</u>
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- <u>Configuration Professional : Site à site IPsec VPN entre ASA/PIX et un exemple de</u> <u>configuration du routeur IOS</u>
- <u>Références des commandes du pare-feu Cisco Secure PIX</u>
- Routeur Cisco et Security Device Manager

- <u>Demandes de commentaires (RFC)</u>
 <u>Support et documentation techniques Cisco Systems</u>