Configuration d'un tunnel IPSec entre un concentrateur Cisco VPN 3000 et un pare-feu Checkpoint NG

Contenu

Introduction Conditions préalables **Conditions requises Components Used Conventions** Diagramme du réseau Configurations Configurer le concentrateur VPN 3000 Configurer le contrôleur NG Vérification Vérification de la communication réseau Afficher l'état du tunnel sur le contrôleur NG Afficher l'état du tunnel sur le concentrateur VPN Dépannage Récapitulation de réseau Déboques pour Checkpoint NG Déboques pour le concentrateur VPN Informations connexes

Introduction

Ce document explique comment configurer un tunnel IPSec avec des clés pré-partagées pour communiquer entre deux réseaux privés. Dans cet exemple, les réseaux de communication sont le réseau privé 192.168.10.x à l'intérieur du concentrateur Cisco VPN 3000 et le réseau privé 10.32.x.x à l'intérieur du pare-feu de nouvelle génération Checkpoint.

Conditions préalables

Conditions requises

- Le trafic à partir du concentrateur VPN et à l'intérieur du contrôleur NG vers Internet représenté ici par les réseaux 172.18.124.x doit circuler avant de commencer cette configuration.
- Les utilisateurs doivent être familiarisés avec la négociation IPSec. Ce processus peut être

divisé en cinq étapes, dont deux phases IKE (Internet Key Exchange).Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois les homologues authentifiés, un tunnel sécurisé est créé avec l'Association de sécurité Internet et le protocole ISAKMP (Key Management Protocol).Dans IKE Phase 2, les homologues IPSec utilisent le tunnel authentifié et sécurisé afin de négocier les transformations de SA IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.Le tunnel IPSec est créé et les données sont transférées entre les homologues IPSec en fonction des paramètres IPSec configurés dans les jeux de transformation IPSec.Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.

Components Used

Cette configuration a été développée et testée avec les versions de logiciel et de matériel suivantes :

- Concentrateur de la gamme VPN 3000 3.5.2
- Pare-feu GN Checkpoint

Conventions

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque : Le schéma d'adressage IP utilisé dans cette configuration n'est pas routable légalement sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations

Configurer le concentrateur VPN 3000

Complétez ces étapes afin de configurer le concentrateur VPN 3000 :

1. Accédez à Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN afin de

configurer la session LAN-to-LAN. Définissez les options d'authentification et d'algorithmes IKE, de clé pré-partagée, d'adresse IP d'homologue et de paramètres de réseau local et distant. Cliquez sur Apply.Dans cette configuration, l'authentification a été définie comme ESP-MD5-HMAC et le chiffrement a été défini comme

3DES.

2

Configuration System Tunneling Protocols IPSec LAN-te	o-LAN Modify
Modify an IPSec LAN-to-LAN connection.	
Name Checkpoint	Enter the name for this LAN-to-LAN connection.
Interface Ethernet 2 (Public) (172.18.124.131) 💌	Select the interface to put this LAN-to-LAN connection on.
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital None (Use Preshared Keys)	Select the Digital Certificate to use.
Certificate C Entire certificate chain Transmission @ Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key ciscontprules	Enter the preshared key for this LAN-to-LAN connection.
Authentication ESP/MD5/HMAC-128 •	Specify the packet authentication mechanism to use.
Encryption 3DES-168 ·	Specify the encryption mechanism to use.
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Routing None	Choose the routing mechanism to use.Parameters below are ignored if Network Autodiscovery is chosen.
Local Network	
Network List Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 192.168.10.0	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A
Wildcard Mask 0.0.0.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Remote Network	
Network List Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 10.32.0.0	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A
Wildcard Mask 0.0.127.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Apply Cancel	

2. Accédez à Configuration > System > Tunneling Protocols > IPSec > IKE Propositions et définissez les paramètres requis.Sélectionnez la proposition IKE IKE-3DES-MD5 et vérifiez les paramètres sélectionnés pour la proposition. Cliquez sur Apply afin de configurer la session LAN à LAN.Voici les paramètres de cette configuration

Configuration System Tunneling Protocols IPSec I	KE Proposals Modify
Modify a configured IKE Proposal.	
Proposal Name IKE-3DES-MD5	Specify the name of this IKE Proposal.
Authentication Mode Preshared Keys	 Select the authentication mode to use.
Authentication Algorithm MD5/HMAC-128 -	Select the packet authentication algorithm to use.
Encryption Algorithm 3DES-168 -	Select the encryption algorithm to use.
Diffie-Hellman Group Group 2 (1024-bits) -	Select the Diffie Hellman Group to use.
Lifetime Measurement Time	Select the lifetime measurement of the IKE keys.
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime 86400	Specify the time lifetime in seconds.
Apply Cancel	

3. Accédez à Configuration > Policy Management > Traffic Management > Security Associations, sélectionnez l'association de sécurité IPSec créée pour la session et vérifiez les paramètres de l'association de sécurité IPSec sélectionnés pour la session LAN à LAN.Dans cette configuration, le nom de la session LAN à LAN était « Checkpoint », de sorte que la SA IPSec a été créée automatiquement en tant que « L2L : Point de contrôle.

»		
Configuration Policy Management Traffic Mana	agement Security Associatio	ns Save Needed 🖶
This section lets you add, configure, modify, an negotiate IKE parameters.	d delete IPSec Security Assoc	iations (SAs). Security Associations use IKE Proposals to
Click Add to add an SA, or select an SA and cli	ck Modify or Delete.	
	IPSec SAs ESP-DES-MD5 ESP-3DES-MD5 ESP/IKE-3DES-MD5 ESP-3DES-NONE ESP-12TP-TRANSPORT ESP-3DES-MD5-DH7 I2L: Checkpoint	Actions Add Modify Delete

Voici les paramètres de cette SA

Configuration Policy Management Traffic Management	Security Associations Modify
Modify a configured Security Association.	
SA Name L2L: Checkpoint	Specify the name of this Security Association (SA).
Inheritance From Rule 💌	Select the granularity of this SA.
IPSec Parameters	
Authentication Algorithm ESP/MD5/HMAC-128 -	Select the packet authentication algorithm to use.
Encryption Algorithm 3DES-168 -	Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled	Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time 💌	Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime 86400	Specify the time lifetime in seconds.
IKE Parameters	
IKE Peer 172.18.124.157	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode Main	Select the IKE Negotiation mode to use.
Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
Certificate Transmission ^o Entire certificate chain ^(*) Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.
Apply Cancel	

Configurer le contrôleur NG

Les objets et les règles réseau sont définis sur le contrôleur NG afin de définir la stratégie relative à la configuration VPN à configurer. Cette stratégie est ensuite installée avec l'Éditeur de stratégie de GN Checkpoint pour compléter le côté GN Checkpoint de la configuration.

 Créez les deux objets réseau pour le réseau Checkpoint NG et le réseau de concentrateur VPN qui chiffreront le trafic intéressant.afin de créer des objets, sélectionnez Gérer > Objets réseau, puis sélectionnez Nouveau > Réseau. Saisissez les informations réseau appropriées, puis cliquez sur OK.Ces exemples montrent la configuration d'objets réseau appelés CP_inside (le réseau interne du contrôleur NG) et CONC_INSIDE (le réseau interne du concentrateur

Network Prop	erties - CP_inside		×
General NA	r		
<u>N</u> ame:	CP_inside		
IP <u>A</u> ddres	x 10.32.0.0		
Net <u>M</u> ask:	255.255.128.0		
<u>C</u> omment:	CPINSIDE		
Color:			
Broadca <u>I</u> nclu	st address: ded <u>O No</u> t included		
	OK Cancel	Help	
L			

Network Proper	ties - CONC_INSIDE	×
General NAT		
<u>N</u> ame:	CONC_INSIDE	
IP <u>A</u> ddress:	192.168.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:	Concentrator network	
Color:		
Broadcast <u>I</u> nclude	address: ed <u>O</u> N <u>o</u> t included	
	OK Cancel Help	

2. Accédez à Manage > Network Objects et sélectionnez New > Workstation afin de créer des objets de station de travail pour les périphériques VPN, Checkpoint NG et le concentrateur VPN.Remarque : Vous pouvez utiliser l'objet de station de travail Checkpoint NG créé lors de la configuration initiale de Checkpoint NG. Sélectionnez les options pour définir la station de travail en tant que passerelle et périphérique VPN interopérable, puis cliquez sur OK.Ces exemples montrent la configuration d'objets appelés ciscocp (Checkpoint NG) et CISCO_CONC (concentrateur VPN 3000)

2

Workstation Properties - c	iscocp	×
Workstation Properties - c	iscocp General Name: Ciscocp IP Address: 172.18.124.157 Genment: Checkpoint External IP Color:	×
	Type: C Host C Gateway Check Point Products ✓ Check Epint products installed: Version NG ✓ Get Version ✓VPN-1 & FireWall-1 ✓FloodGate-1 Policy Server ✓ Primary Management Station	
	Object Management Image: Managed by this Management Server (Internal) Image: Managed by another Management Server (External) Secure Internal Communication Image: Description of the transformation Image: Description of the transformation <td< td=""><td></td></td<>	
	OK Cancel He	alp

Workstation Properties -	CISCO_CONC	×
General	General	
- NAT	Name: CISCO_CONC	
VPN Advanced	IP Address: 172.18.124.131 Get address	
	Comment: VPN Concentrator	
	Cojor:	
	Type: C Host C Gate <u>w</u> ay	
	Check Point Products	
	Check Point products installed: Version NG Get Version	
	VPN-1 & FireWall-1 FloodGrate-1 Policy Server Management Station	
	Object Management	
	C Managed by this Management Server (Internal)	
	C Managed by another Management Server (External)	
	Interoperable ⊻PN Device	
	OK Cancel Help	

3. Accédez à Manage > Network Objects > Edit afin d'ouvrir la fenêtre Workstation Properties pour Checkpoint NG workstation (ciscocp dans cet exemple). Sélectionnez Topologie dans les choix situés à gauche de la fenêtre, puis sélectionnez le réseau à chiffrer. Cliquez sur Edit afin de définir les propriétés de l'interface.Dans cet exemple, CP_inside est le réseau interne du contrôleur NG.

/orkstation Properties - c	iscocp				2
General	Topology				
Topology NAT	<u>G</u> et Interfaces]			
VPN	Name	IP Address	Network Mask	IP Addresses behind	
Authentication	E100B0	10.32.50.50	255.255.128.0	CP inside	
⊡ Management ⊞-Advanced	E100B1	172.18.124.157	255.255.255.0	External	
	4			•	
	Add	<u>E</u> dit	<u>R</u> emove	Show	
	Show all IPs beh	nind Gateway			
	 All IP Addresse information. 	es <u>b</u> ehind Gateway b	ased on Topology	Show	
	C Manually Defin	ned	Y	Sho <u>w</u>	
	Exportable for	SecuRemote			
			OK (Cancel Help	

4. Dans la fenêtre Propriétés de l'interface, sélectionnez l'option permettant de désigner la station de travail comme interne, puis spécifiez l'adresse IP appropriée. Click OK.Les sélections de topologie affichées désignent la station de travail comme interne et spécifient les adresses IP derrière l'interface CP_inside

Interface Properties	×
General Topology QoS	_
Topology	
<u>External (leads out to the internet)</u>	
 Internal (leads to the local network) 	
IP Addresses behind this interface:	
○ <u>N</u> ot Defined	
Network defined by the interface IP and Net Mask	
Specific: CP_inside	
Anti-Spoofing	
Perform Anti-Spoofing based on interface topology	
Spoof Tracking: O N <u>o</u> ne 💿 <u>L</u> og O <u>A</u> lert	
OK Cancel Help	

5. Dans la fenêtre Propriétés de la station de travail, sélectionnez l'interface externe sur l'indicateur Checkpoint NG qui mène à Internet, puis cliquez sur **Modifier** afin de définir les propriétés de l'interface. Sélectionnez l'option pour désigner la topologie comme externe,

General Topology Topology ● External (leads out to the internet) ● Internal (leads to the local network) IP Addresses behind this interface: ● Not Defined ● Network defined by the interface IP and Net Mask ● Specific: ✓ Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: None Log Alert	terface	Properties				
Topology ● External (leads out to the internet) ● Internal (leads to the local network) IP Addresses behind this interface: ● Not Defined ● Network defined by the interface IP and Net Mask ● Specific: ✓ Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ● None ● Log ● Alert	General	Topology	QoS			
 External (leads out to the internet) Internal (leads to the local network) IP Addresses behind this interface: Not Defined Network defined by the interface IP and Net Mask Specific: Anti-Spoofing Anti-Spoofing based on interface topology Spoof Tracking: ○ None ○ Log ○ Alert 	Topolo	gy				_
 Internal (leads to the local network) IP Addresses behind this interface: ○ Not Defined ○ Network defined by the interface IP and Net Mask ○ Specific: ○ Specific: Anti-Spoofing Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None ○ Log ○ Alert 	● <u>E</u> xt	ernal (leads o	ut to the inter	net)		
IP Addresses behind this interface: ○ Not Defined ○ Network defined by the interface IP and Net Mask ○ Specific: ✓ Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None ○ Log ○ Alert	O <u>I</u> nte	ernal (leads to	the local net	vork)		
 ○ Network defined by the interface IP and Net Mask. ○ Specific: ✓ Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None ○ Log ○ Alert 	IP/	Addresses bel	hind this interf	ace:		
 ○ Network defined by the interface IP and Net Mask ○ Specific: ✓ Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None ○ Log ○ Alert 	0	D <u>N</u> ot Define	d			
 ○ <u>Specific:</u> ✓ Anti-Spoofing ✓ <u>Perform Anti-Spoofing based on interface topology</u> Spoof Tracking: ○ None ○ Log ○ Alert 	0	🗅 Network de	efined by the i	nterface IP a	nd Net Mask	
Anti-Spoofing ✓ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None ● Log ○ Alert	C) <u>S</u> pecific:				-
Perform Anti-Spoofing based on interface topology Spoof Tracking: O None O Log O Alert	Anti-Sp	oofing				
Spoof Tracking: 🔿 N <u>o</u> ne 💿 <u>L</u> og 🔿 <u>A</u> lert	<mark>▼</mark> <u>P</u> er	form Anti-Spo	ofing based c	n interface to	pology	
	Spo	oof Tracking:	O N <u>o</u> ne (• Log C	Alert	
	[Halp	
					Help	

puis cliquez sur OK.

6. Dans la fenêtre Propriétés de la station de travail sur Checkpoint NG, sélectionnez VPN dans les choix à gauche de la fenêtre, puis sélectionnez les paramètres IKE pour les algorithmes de chiffrement et d'authentification. Cliquez sur Edit afin de configurer les propriétés IKE.

General Topology NAT VEN Authentication Management Advanced	VPN Encryption gchemes Image: Image	
	Nickname DN Certificate Authority Image: Constraint of the second seco	

7. Définissez les propriétés IKE pour qu'elles correspondent aux propriétés du concentrateur VPN.Dans cet exemple, sélectionnez l'option de chiffrement pour **3DES** et l'option de

IKE Properties	×
General	
Support key exchange encryption v	with: Support data integrity with:
	▲ <u>▼</u> MD <u>5</u>
CAST	
Support authentication methods:	
Pre-Shared Secret	Edit <u>S</u> ecrets
Public Key Signatures	Specify
□ VPN-1 & FireWall-1 authentica	ation for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
OK Ca	ancel Help

hachage pour MD5.

8. Sélectionnez l'option d'authentification pour **Secrets pré-partagés**, puis cliquez sur **Modifier les secrets** pour définir la clé pré-partagée comme compatible avec la clé pré-partagée sur le concentrateur VPN. Cliquez sur **Modifier** afin d'entrer votre clé comme indiqué, puis cliquez

Shar	ed Secret				×
Г ⁹	Shared Secrets List: -				1
	Peer Name CISCO_CONC	Shared Se	cret	<u>E</u> dit	
				<u>R</u> emove	
	Enter secret: cisco	rtprules	Set		
	ОК	Cano	el	Help	

sur Définir, OK

Dans la fenêtre des propriétés IKE, cliquez sur Avancé... et modifiez ces paramètres
 Désélectionnez l'option Support agressif mode.Sélectionnez l'option d'échange de clés de support pour les sous-réseaux.Lorsque vous avez terminé, cliquez sur OK,

Advanced IKE properties			×
Use <u>UDP</u> encapsulation			
Support Diffie-Hellman groups	UDP VPN1_IPS	SEC_encapsi 💌]
	Group 1 (76	i8 bit)	
	Group 2 (10	(24 bit) (36 bit)	
Rekeying Parameters			J
Renegotiate IKE security assoc	iations	1440 🕂	Minutes
Renegotiate IPSEC Security as:	sociations every	3600 📑	Seconds
Renegotiate IPSEC Security	associations eve	ary 50000 🚊	KBytes
Misc			
Support IP <u>compression</u> for	SecureClient		
Support <u>aggresive</u> mode	. h t.		
Support Key exchange for s	ubnets		
ОК	Cancel	Help	

10. Accédez à Manage > Network Objects > Edit afin d'ouvrir la fenêtre Workstation Properties pour le concentrateur VPN. Sélectionnez Topologie dans les choix situés à gauche de la fenêtre afin de définir manuellement le domaine VPN.Dans cet exemple, CONC_INSIDE (le réseau interne du concentrateur VPN) est défini comme domaine VPN.

Workstation Properties	- CISCO_CONC			Ē.	×
- General	Topology				
NAT	<u>G</u> et Interfaces				
VPN Advanced	Name	IP Address	Network Mask		
	Add Show all IPs beh	Edt	<u>B</u> emove	how	
	VPN Domain C All IP Addresse information. C <u>M</u> anually Defin	ed + CONC INS	ased on Topology	Sh <u>o</u> w Sho <u>w</u>	_] 1
	Egortable for 9	SecuRemote			,
			ок с	ancel Help	»

11. Sélectionnez **VPN** dans les choix situés à gauche de la fenêtre, puis sélectionnez **IKE** comme schéma de cryptage. Cliquez sur **Edit** afin de configurer les propriétés IKE.

Workstation Properties -	CISCO_CONC			×
General Topology NAT Advanced	VPN Encryption schemes			
		OK	Cancel	Help

12. Définissez les propriétés IKE pour refléter la configuration actuelle sur le concentrateur VPN.Dans cet exemple, définissez l'option de chiffrement pour **3DES** et l'option de hachage

IKE Properties	×
General	
Support key exchange encryption with:	- Support data integrity with:
	✓ MD <u>5</u>
I I I I I I I I I I I I I I I I I I I	C SHA1
Support authentication methods:	
Pre-Shared Secret Ed	it <u>S</u> ecrets
Public Key Signatures Matc	hing Criteria
□ VPN-1 & FireWall-1 authentication fo	r SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
OK Cancel	Help

pour MD5.

13. Sélectionnez l'option d'authentification pour **Secrets pré-partagés**, puis cliquez sur **Modifier les secrets** afin de définir la clé pré-partagée. Cliquez sur **Modifier** afin d'entrer votre clé comme indiqué, puis cliquez sur **Définir**,

Share	ed Secret				×
- ۲ ⁹	Shared Secrets List:				1
	Peer Name	Shared Secret			
	CISCOCP			<u>E</u> dit	
				<u>R</u> emove	
	Enter secret: cisc	ortprules S	et		
	0K	Cancel		<u>H</u> elp	

14. Dans la fenêtre des propriétés IKE, cliquez sur Avancé... et modifiez ces paramètres :Sélectionnez le groupe Diffie-Hellman approprié aux propriétés IKE.Désélectionnez l'option Support agressif mode.Sélectionnez l'option d'échange de clés de support pour les sousréseaux.Lorsque vous avez terminé, cliquez sur OK,

Advanced IKE properties			×
✓ Use UDP encapsulation ———			
	UDP VPN1_IP	SEC_encapsi 💌]
Support Diffie-Hellman groups —			त्त
	Group 1 (76	i8 bit)	
	Group 2 (10	i24 bitj Gelsky	
		136 DIQ	
Rekeying Parameters			
Renegotiate IKE security asso	ciations	1440 📑	Minutes
Penegatista IDSEC Security a	sociations queru	3600	- I Seconds
	ssociations every		
I Renegotiate IPSEC Securi	ty associations eve	sry 50000 🚊	KBytes
Misc			
Support IP compression for	SecureClient		
Support aggresive mode	e e e e e e e e e e e e e e e e e e e		
Support key exchange for	subnets		
,,,,,,, _			
OK	Carrow	L I a la	1
	Lancel		

15. Sélectionnez Règles > Ajouter des règles > Haut afin de configurer les règles de chiffrement pour la stratégie. Dans la fenêtre Éditeur de stratégie, insérez une règle avec la source comme CP_inside (réseau interne du contrôleur NG) et la destination comme CONC_INSIDE (réseau interne du concentrateur VPN). Définissez des valeurs pour Service = Any, Action = Encrypt et Track = Log. Lorsque vous avez ajouté la section Action de chiffrement de la règle, cliquez avec le bouton droit sur Action et sélectionnez Modifier les propriétés.

CISCOCP - Check Point Policy Editor	- Standard				anarorora)a	
File Edit View Manage Rules Policy	Topology Search Window	Help				
」■● X℃間 畳塑液	A] 🗉 🖳 🗗 🏜	° = 1 ↔ ♥	54 🛛 🖄 🚠			
1 °% 🛄 📰 🖓 🖓 84 🗛 🤇	1 Q Q 🖸 💊 🍈	6				
\$ € 4 @ 8 8 0 %	🗱 Security - Standard 🗮	Address Translation - St	andard 🙀 QoS - S	tandard 🛄 Desktop Se	scurity - Standard	
E-St Network Objects	NO SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
Workstation	Ho. Sounce	DESTIMATION	SERVICE	PACTION	THEFT	INSTRUCT
- CISCO_CONC	1 부 CP_inside 부 CONC_INSIDE	부 CONC_NSIDE 부 CP_inside	* Any	Edit propert	ies	Gateway:
-+ CONC_INSIDE	2 44 CP_inside	* Any	* Any	Add Encryp	.on	Gateway
Orgendae Orgendae	Name CISCO_CONC ciscocp	IP 172.18. 172.18.	Comment 124.131 VPN Conc 124.157 Checkpoil	Auth Auth Client Auth Client Auth Client Auth Client Auth Client Auth Client Client Client Encrypt Client Encrypt Client Client Clien	ypt	1

16. Sélectionnez IKE et cliquez sur

Encryption Pro	perties			×
General				
Encryption	<u>s</u> chemes defined: - :E WZ			
<u> </u>				
	ОК	Cancel	Help	

Modifier.

17. Dans la fenêtre Propriétés IKE, modifiez les propriétés pour les mettre en accord avec la transformation du concentrateur VPN.Définissez l'option Transform sur Encryption + Data Integrity (ESP).Définissez l'algorithme de chiffrement sur 3DES.Définissez l'intégrité des données sur MD5.Configurez la passerelle d'homologue autorisée pour qu'elle corresponde au concentrateur VPN (CISCO_CONC).Lorsque vous avez terminé, cliquez sur

IKE Properties	
General	
Transform	
Encryption + Data Integrit	ty (ESP)
🔘 Data Integrity Only (AH)	
Encryption Algorithm:	3DES 💌
<u>D</u> ata Integrity	MD5
<u>C</u> ompression method:	None
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit)
Perform IP Pool NAT	
OK Ca	ancel Help

18. Une fois que Checkpoint NG est configuré, enregistrez la stratégie et sélectionnez **Policy > Install** afin de

l'activer.						
CISCOCP - Check Point Policy	Editor - Standard		ARRENDE -	1		
File Edit View Manage Rules	Policy Topology Search Window	Help				
🖬 🕘 🐰 🔁 🛍 🛛 🐇	Verify Instal	° ॡ Щ ↔ 🗍 🤻	₽ 📥 😤 🗍 4	8		
Pta 🔲 🗶 🌮 🕹 👫	Uninstall					
₽ <u></u>	Access Lists	ddress Translation - St	andard 🔛 QoS	- Standard 🎦 Desktop	Security - Standard	
E Stewark Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL OF
B- Workstation	Management High Availability					
ciscocp	Global Properties	CONC_NSDE	🖈 Any	Encrypt	🔳 Log	Gateways
Network		and the second se	Figure 1 States and a state	undusi 👝 edea nung tituntu un		
	CP_inside	T ANY	Arty	C accept	Log	Gateways
CP_inside						
OSE Device	10					
Embedded Device	10					
- III Group						
- W Logical Server	10					
Address Range						
Gateway Cluster						-
Dynamic Object	Name	IP	Comm	ent		
	CISCO_CONC	172.18.1	124.131 VPN O	oncentrator		
	discorp	172.18.1	124.157 Cheda	point External IP		

La fenêtre d'installation affiche les notes de progression lors de la compilation de la stratégie.



e la fenêtre d'installation indique que l'installation de la stratégie est terminée, cliquez sur **Fermer** pour terminer la

 Install Policy

 Standard.W: Security Policy Script generated into Standard.pf

 Standard:

 Compiled OK.

 Installing VPN-1/FireWall-1 policy On: ciscocp ...

 VPN-1/FireWall-1 policy installed successfully on ciscocp...

 VPN-1/FireWall-1 policy Installation for all modules was successful

Vérification

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

Vérification de la communication réseau

Afin de tester la communication entre les deux réseaux privés, vous pouvez lancer une requête ping de l'un des réseaux privés vers l'autre réseau privé. Dans cette configuration, une requête ping a été envoyée du côté de Checkpoint NG (10.32.50.51) au réseau du concentrateur VPN

```
(192.168.10.2).
```

```
C:\WINNT\System32\cmd.exe
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = Oms, Maximum = 10ms, Average =
                                                5ms
C:\>
C:\>
C:\>
C:\>
```

Afficher l'état du tunnel sur le contrôleur NG

Pour afficher l'état du tunnel, accédez à l'Éditeur de stratégie et sélectionnez **Fenêtre > État du** système.

CISCOCP - Check Point System Status								
Ele Yew Modules Products Iools Window Help								
🕽 🗩 🖻 🗛 🛄 🔦 🎫 🇞 🚛 🕋 🛠	段							
Modules IP Address	VPN-1 Details							
	Status:	ок						
E-Ciscocp 172.18.124.157	Packets							
FireWal-1	Encrypted:	19						
FloodGate-1	Decrypted:	18						
Management	Errors							
SVN Foundation	Encryption errors:	0						
	Decryption errors:	0						
	IKE events errors:	3						
	Hardware							
	HW Vendor Name:	none						
	HW Status:	none						
For Help, press F1		Last updated:09:34:14 PM						

Afficher l'état du tunnel sur le concentrateur VPN

Afin de vérifier l'état du tunnel sur le concentrateur VPN, accédez à **Administration > Administre Sessions**.

his screen shows st formation on a sess	inister Sessions atistics for sessions. sion, click on that ses on, click Ping	To refresh the statis sion's name. To log	tics, click Refre out a session, cl	esh. Sel ick Log	ect a Group	Vednes to filter ble belo	day, 11 Sept the sessions w. To test th	ember 2002 20:37:0 Reset @ Refresh a. For more he network
Froup [All ogout All: <u>PPTP U</u> Session Summa	ser L2TP User IPS	ec User L2TP/IPSe	ec User IPSec/U	JDP Us	er IPSec/TC	P User	IPSec LAN	-to-LAN
ocoston ounne								
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak S	Concurrent essions	Con Sessio	current ons Limit	Total Cumulative Sessions
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions 3	Total Active Sessions 4	Peak S	Concurrent essions 4	Con Sessio	current ons Limit	Total Cumulative Sessions 17
Active LAN-to- LAN Sessions	Active Remote Access Sessions 0	Active Management Sessions 3	Total Active Sessions 4	Peak S	Concurrent essions 4 [Remote Acc	Con Session 1 cess Se	current ons Limit 500 ssions Man	Total Cumulative Sessions 17 agement Sessions
Active LAN-to- LAN Sessions 1 LAN-to-LAN S Connection Nam	Active Remote Access Sessions 0 essions ne IP Address	Active Management Sessions 3 Protoco	Total Active Sessions 4	Peak S	Concurrent essions 4 [Remote Acc Login T	Con Session 1 Cess Ser	current ons Limit 500 ssions Man Duration	Total Cumulative Sessions 17 agement Sessions] Actions

Sous Sessions LAN à LAN, sélectionnez le nom de connexion du point de contrôle pour afficher les détails sur les SA créées et le nombre de paquets transmis/reçus.

Connection Name	IP Add	iress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	
Checkpoint	172.18.12	4.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	25	
	Canalan TD	1	IK	E Session	Energy then Alexandri	2000 1	20		
			IK	E Session		1			
	Session ID	1			Encryption Algorith	m 3DES-1	68		
Hashing	Algorithm	MD5		1	Diffie-Hellman Gro	up Group 2	Group 2 (1024-bit)		
Authentics	tion Mode	Pre-Sha	ared Keys	I	KE Negotiation Mo	de Main	Main		
Rekey Tin	ie Interval	86400	seconds						
			IPS	ec Session					
Session ID 2					Remote Addre	ss 10.32.0	10.32.0.0/0.0.127.255		
-	al Address	192.16	8.10.0/0.0.0.255		Encryption Algorith	m 3DES-1	3DES-168		
Loc						1	1		
Loc Hashing	Algorithm	MD5			SI	sp 1			
Loc Hashing Encapsula	Algorithm tion Mode	MD5 Tunnel			SI Rekey Time Interv	al 28800 s	econds		

Dépannage

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

Remarque : le trafic ne doit pas être PATed sur le tunnel IPSec à l'aide de l'adresse IP publique du concentrateur VPN (interface externe). Sinon, le tunnel échoue. Ainsi, l'adresse IP utilisée pour PATing doit être une adresse autre que l'adresse configurée sur l'interface externe.

Récapitulation de réseau

Lorsque plusieurs réseaux internes adjacents sont configurés dans le domaine de chiffrement sur le point de contrôle, le périphérique peut automatiquement résumer les réseaux en fonction du trafic intéressant. Si le concentrateur VPN n'est pas configuré pour correspondre, le tunnel risque d'échouer. Par exemple, si les réseaux internes 10.0.0.0 /24 et 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ces réseaux peuvent être résumés sur 10.0.0.0 /23.

Débogues pour Checkpoint NG

Pour afficher les journaux, sélectionnez **Fenêtre > Visionneuse de journaux**.

ā	ISCOCP - C	heck Poi	int Log Vie	wer - [fv	e.log]		1998		2323.55							X
Ele	Ele Mode Edit Selection Yew Iools Window Help											1.1				
69	(1) (1) Log · · · · · · · · · · · · · · · · · · ·															
	Date	Time	Product	1.1.1	Inter.	Orig	Туре	Action	Source	Destinati	Pr.,	Rule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireN.	🖶 dae	ciscocp	📕 log	0- key instali	ciscoop	CISCO_CONC						
2	13Aug2002	21:32	VPN-1	& FireWV.	. 🕒 dee	ciscocp	🔲 log	Over key install	ciscocp	CISCO_CONC				0x5879f30d	0xt1351129	
																- 3

Débogues pour le concentrateur VPN

Afin d'activer les débogages sur le concentrateur VPN, accédez à **Configuration > System > Events > Classes**. Activez AUTH, AUTHDBG, IKE, IKEDBG, IPSEC et IPSECDBG pour la gravité à enregistrer en tant que 1 - 13. Afin d'afficher les débogages, sélectionnez **Monitoring > Filterable Event Log**.

1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128 3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157 processing SA payload 4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157 Oakley proposal is acceptable 14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157 processing VID payload 15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157 processing IKE SA 16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3 26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp 27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157

27 09/11/2002 20:36:03.610 SEV=8 TREDBG/0 RPT=515 1/2.18.124.15/ SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157

RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE 35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send TOS VID 41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256 48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash

53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157] Starting group lookup for peer 172.18.124.157 54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10 AUTH_Open() returns 9 55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9 56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH_PutAttrTable(9, 748174) 57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH_GroupAuthenticate(9, 2f1b19c, 49c648) 58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(51a6b48, 0, 0) 59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1 60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH_CreateTimer(51a6b48, 0, 0) 61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018 62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(51a6b48, 0, 0) 63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(51a6b48, 0, 0) 64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 3000065 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(51a6b48, 0, 0) 66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB_Decode(3825300, 156) 67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB_Xmt(51a6b48) 68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 $xmit_cnt = 1$ 69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20 IntDB_Xmt(51a6b48) 70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB_Match(51a6b48, 3eb7ab0) 71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(51a6b48, 0, 0) 72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB_Decode(3eb7ab0, 298) 73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB_Rcv(51a6b48)

74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10 AUTH_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.15778 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED 91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157

Keep-alives configured on but peer does not support keep-alives (type = None) 93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms) 94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected 95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(51a6b48, 0, 0) 96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH_Int_FreeAuthCB(51a6b48) 98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9 99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156 102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash 103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload 104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload 105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID 106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0 109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157] Processing ID 110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157 Group [172.18.124.157] Received local IP Proxy Subnet data in ID Payload: Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0 113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM IsRekeyed old sa not found by addr 114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157 Group [172.18.124.157]

IKE Remote Peer configured for SA: L2L: Checkpoint

115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157] processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157 Group [172.18.124.157] IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10 Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10 IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 Group [172.18.124.157] oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157] constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157 Group [172.18.124.157] constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id: Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157 Group [172.18.124.157] constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48

139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157 Group [172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 0000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msghdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147 Processing KEY_UPDATE msg!

165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148 Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150 No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151 KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152 KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547 pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157 Group [172.18.124.157] PHASE 2 COMPLETED (msgid=54796f76)

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support technique Cisco Systems