# Exemple de configuration de tunnel IPSec LAN à LAN entre un concentrateur Cisco VPN 3000 et un routeur avec AES

## Contenu

Introduction Conditions préalables **Conditions requises Components Used Conventions** Configuration Diagramme du réseau Configurations Configurez le concentrateur VPN Vérification Vérifiez la configuration du routeur Vérifiez la configuration du concentrateur VPN Dépannage Dépanner le routeur Dépannage du concentrateur VPN Informations connexes

## **Introduction**

Ce document explique comment configurer un tunnel IPSec entre un concentrateur Cisco VPN 3000 et un routeur Cisco en utilisant Advance Encryption Standard (AES) comme algorithme de chiffrement.

AES est une nouvelle publication de la norme FIPS (Federal Information Processing Standard) créée par le NIST (National Institute of Standards and Technology), qui sert de méthode de chiffrement. Cette norme détermine un algorithme de chiffrement symétrique AES qui remplace la norme DES (Data Encryption Standard) comme fonction de transformation de la confidentialité pour IPSec et IKE (Internet Key Exchange). L'AES comporte trois longueurs de clé différentes : 128 bits (valeur par défaut), 192 bits et 256 bits. La fonction AES de Cisco IOS® vient renforcer la nouvelle norme de chiffrement AES, grâce au mode avec enchaînement de blocs (CBC), vers IPSec.

Consultez le site du <u>Computer Security Resource Center du NIST</u> pour de plus amples renseignements sur l'AES.

Examinez l'exemple de configuration du tunnel IPSec LAN à LAN entre le concentrateur Cisco

VPN 3000 et le pare-feu PIX pour en savoir plus sur le sujet.

Examinez l'exemple de <u>configuration du tunnel IPSec entre le pare-feu PIX 7.x et le concentrateur</u> VPN 3000 pour en savoir plus sur le pare-feu PIX doté de la version 7.1 du logiciel.

## **Conditions préalables**

#### **Conditions requises**

Ce document exige une connaissance de base du protocole IPSec. Consultez la section Introduction au chiffrement IPSec pour de plus amples renseignements sur IPSec.

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

- Exigences du routeur : la fonction AES a été introduite dans la version du logiciel Cisco IOS 12.2(13)T. Afin d'activer AES, votre routeur doit prendre en charge IPSec et exécuter une image IOS avec des longues clés de type « K9 » (sous-système « K9 »). Remarque : La prise en charge matérielle de AES est également disponible sur les modules VPN d'accélération Cisco 2600XM, 2691, 3725 et 3745 AES. Cette fonction n'a aucune incidence sur la configuration, et le module matériel est automatiquement sélectionné si les deux sont disponibles.
- Exigences du concentrateur VPN : le soutien logiciel de la fonction AES a été introduit dans la version 3.6. Le soutien matériel est fourni par la version améliorée du processeur de chiffrement évolutif (SEP-E). Cette fonction n'a aucune incidence sur la configuration.Remarque : Dans la version 3.6.3 du concentrateur Cisco VPN 3000, les tunnels ne négocient pas avec AES en raison de l'ID de bogue Cisco <u>CSCdy88797</u> (clients enregistrés uniquement). Ce problème a été résolu dès la version 3.6.4.Remarque : le concentrateur Cisco VPN 3000 utilise des modules SEP ou SEP-E, et non les deux. N'installez pas les deux modules sur un même périphérique. Si vous installez un module SEP-E sur un concentrateur VPN qui comprend déjà un module SEP, le concentrateur VPN désactive alors le module SEP pour utiliser uniquement le module SEP-E.

#### **Components Used**

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

- Routeur Cisco de série 3600 avec Cisco IOS, version logicielle 12.3(5)
- Concentrateur Cisco VPN 3060 avec la version logicielle 4.0.3

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.

### **Conventions**

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

## **Configuration**

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque :** utilisez l'<u>outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

#### Diagramme du réseau

Ce document utilise la configuration réseau suivante :



#### **Configurations**

Ce document utilise les configurations suivantes :

- Routeur IPSec
- <u>Concentrateur VPN</u>

Configuration ipsec_router
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!

```
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
I
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
```

```
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

**Remarque :** Bien que la syntaxe de la liste de contrôle d'accès soit inchangée, les significations sont légèrement différentes pour les listes de contrôle d'accès cryptées. Pour les ACL avec chiffrement, « permit » indique que les paquets correspondants doivent être chiffrés, tandis que « deny » signifie le contraire.

#### Configurez le concentrateur VPN

Dans leurs paramètres d'usine, les concentrateurs VPN préprogrammés ne comportent aucune adresse IP. Vous devez utiliser le port de la console pour la configuration initiale, qui consiste en une interface de ligne de commande (CLI) reposant sur des menus. Pour en savoir plus sur la configuration des concentrateurs VPN par la console, consultez la section correspondante.

Une fois que l'adresse IP de l'interface Ethernet 1 (privée) est configurée, le reste peut être configuré à son tour au moyen de l'interface de ligne de commande ou de celle du navigateur. L'interface du navigateur prend en charge les protocoles HTTP et HTTP sur SSL (Secure Socket Layer).

Les paramètres suivants sont configurés par la console :

- Date/heure Il est très important que la bonne date et la bonne heure soient programmées. Elles permettent l'exactitude des entrées de journalisation et de gestion des comptes et la création par le système d'un certificat de sécurité valide.
- Interface Ethernet 1 (privée) : L'adresse IP et le masque (de notre topologie de réseau 172.16.1.1/24).

Àce stade, le concentrateur VPN est accessible par un navigateur HTML à partir du réseau interne. Pour plus de renseignements sur la configuration du concentrateur VPN en mode CLI, consultez la section sur la <u>configuration rapide au moyen de l'interface CLI</u>.

 Entrez l'adresse IP de l'interface privée à partir du navigateur Web pour activer l'interface GUI.Cliquez sur l'icône save needed [enregistrement nécessaire] pour enregistrer les modifications apportées à la mémoire. La valeur d'usine par défaut attribuée au nom d'utilisateur et au mot de passe est « admin » et est sensible à la casse.



 Lorsque l'interface GUI est activée, sélectionnez Configuration > Interfaces > Ethernet 2 (Public) [configuration > interfaces > Ethernet 2 (public)] pour configurer l'interface Ethernet 2.

<u>Configuration</u> <u>interfaces</u>	Config	guration   Interfaces	;   Ethernet 2			
EPSzstem EPUser Management EPolicy Management	Config	uring Ethernet luterfa	ce 2 (Public).			
	Gene	ral RIP OSPF B	andwidth			
Contraining in the	General Parameters					
	Sel	Attribute	Value		Description	
	0	Disabled			Select to disable this interface.	
	c	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.	
	C.	Static IP Addressing				
		IP Address	20.20.20.1		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this	
		Subnet Mask	255.255.255.0		monthce.	
		Public Interface 🗹 0 MAC Address 00.90 A4.00.4LF9 7		Check to make this interface a "public" interface.		
				The MAC address for this interface.		
		Filter	2. Public (Default)	•	Select the filter for this interface.	
		Speed	10/100 auto 💌		Select the speed for this interface.	
		Duplex	Auto 💌		Select the duplex mode for this interface.	
		MTU	1500		Enter the Maximum Transmit Unit for this interface (62 - 1500).	
			C Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission		agment prior to interface transmission.	
		Public Interface IPSec Fragmentation Policy	<sup>1</sup> C Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)		MTU Discovery (ICMP)	
		The manufacture of the second	C Frigment prior to IPSec encupsulation without Path MTU Discovery (Clear DF bit)			
CISCO SYSTEMS	Aş	oply Cancel				

3. Allez à Configuration > System > IP Routing > Default Gateways [configuration > système > routage IP > passerelles par défaut] pour configurer la passerelle par défaut (Internet) ainsi que la passerelle par défaut du tunnel (interne) pour qu'IPSec atteigne les autres sous-réseaux du réseau privé.Dans cet exemple, un seul sous-réseau est disponible sur le réseau interne.

Configuration		
	Configuration   System   IP Routing   De	fault Gateways
- <del>()</del> System		
- Bervers	Configure the default gateways for your system.	
- Internal Protocols	B-6-th Cotomer 20.00.00.0	Particulty ID address of the definition of contraction Particulty O 0.0 for us definition
- G-P Routing	Detaunt Gateway (20.20.20.2	Ealer the IP address of the delaun gasway or rotter. Ealer 0.0.00 for an delaun rotter.
Static Routes	Metric 1	Enter the metric, from 1 to 16.
Default Gateways		
<u>OGPT</u>	Turnel Default Transferrer 172.16.1.2	Enter the IP address of the default gateway or router for funnels. Enter 0.0.0.0 for no default seater.
OSPF Areas	cananaà .	- CRIBILL TOURE.
UHCP Paranteners	Override Default	Check to allow learned default gateways to override the configured default gateway.
Unce iselay	Gateway	
Resuman Equation	Apply Concel	
Alternanement Protocolo	- 44-2 	
- Fill uents		
- m General		
- Elient Update		
Load Balancing		
- EHuser Management		
Policy Management		
Administration		
• E Monitoring		

4. Allez à Configuration > Policy Management > Traffic Management > Network Lists > Add [configuration > gestion des politiques > gestion du trafic > listes des réseaux > ajouter] pour créer les listes des réseaux précisant le trafic à chiffrer.Les réseaux figurant dans la liste sont accessibles par le réseau distant. Les réseaux répertoriés dans la liste ci-dessous sont des réseaux locaux. Vous pouvez également générer automatiquement la liste des réseaux locaux au moyen de la fonction RIP si vous cliquez sur Generate Local List [produire la liste des réseaux

locaux].				
	Configurati	on   Policy Management   Traff	ic Management   N	stwork Lists   Modify
- (F) System				
- Oser Management	Modify a confi	gued Network List. Click on <b>Generate</b>	Local List to generate a	network list based on routing entries on the Private interface.
Access Hours				
- Inatfic Management	List Name	vpn_local_network	Name	of the Network List you are adding. The name must be unique.
Network Lists		172.16.0.0/0.0.255.255	×	Enter the Networks and Wildcard masks using the following
SAS				formet: n.n.n.n/n.n.n.(e.g. 10.10.0.00.0.255.255).
<u>Filters</u>				subnet mask. A wikicard mask, which is the reverse of a
BYV Policies				ignore, 0s in bit positions to match. For example, 10.10.1.000.0.0.255 = all 10.10.1 year addresses
- Group Matching	Network List			<ul> <li>Each Network and Wildcard mask pair must be entered on a</li> </ul>
Administration				single line.
(I Monitoring				The Wildcard mask may be omitted if the natural Wildcard
			*	mask is to be used.
		<b>I</b>	). F	
	Apply	Concel Generate Lo	icol List	

5. Les réseaux mentionnés dans cette liste sont des réseaux distants, qui doivent être configurés manuellement. Pour ce faire, saisissez le réseau ou le caractère générique de chaque sous-réseau accessible.



Ensuite, notez les deux listes de

,	
racaaliy	
ICSCAUX	

Honfauration     Honfauration	Configuration   Policy Managem This esction lets you edd, modify, copy, a Click Add to create a Network List, or eeb	nent   Traffic Management   Netw and delete Network Lists lett a Network List and dick <b>Medify, Cep</b> <u>Network List</u> VPN Client Local LAN (Default) VPN_Client Local LAN (Default) VPN_Client Local LAN (Default) VPN_local_network	y, or Delete. Actiene Add Modity Delete	Save

6. Allez à Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add [configuration > système > protocoles de tunnellisation > IPSec LAN à LAN > ajouter], puis définissez le tunnel LAN à LAN.Cette fenêtre comporte trois sections. La section supérieure concerne les informations réseau, tandis que les deux sections inférieures sont réservées aux listes de réseaux locaux et distants. Dans la section des informations réseau, sélectionnez le chiffrement AES, le type d'authentification et la proposition IKE, puis indiquez la clé partagée. Dans les sections inférieures, pointez sur les listes de réseaux locaux et distants que vous avez créées.

T Configuration		
-S- <u>Computation</u> 	Configuration   System   Tunneling Protocols   IPSec	LAN-to-LAN   Add
	Add a new IPSec LAN-to-LAN connection	
-C+Tunneino Protocols	Enable 🖂	Check to easible this LAN-to-LAN connection.
	Name test	Enter the same for this LAN-to-LAN connection.
	Interface Ethernet 2 (Public) (20 20 20 1)	Salari the interface for this [ A.N. to [ A.N. concention
KE Proposela		Choose the increase of LAN-in-LAN connection. An Originala Gale connection may
<u>NAT Transparency</u>	Connection Type Bi-directional	have multiple peers specified below.
	30.30.30.1	
- (3) Management Protocols (3) Superio	8	
- CB-General	8	Enter the princip over IP addresses for this LAN to LAN connection. Originate,
Client Update	Peen	$\Omega_{\rm N}$ connection may specify up to ten peet P addresses. Enter one IP address per
User Management	18	100
DEPolicy Management	8	
Group Matching	Digini None (Use Preshared Kevs)	Select the digital certificate to use.
-3: Monitoring	Certificate	
	Transmission @ Idantity cartificate only	Choose how to send the digital cartificate to the IXE peer.
	Preshared Key cisco123	Enter the possbared key for this LAN-to-LAN connection.
	Authentication ESP/MD5/HMAC-128	Specify the packet authentication mechanism to use.
Cisco Systems	Enroyption AES-256	Specify the energyption mechanism to use.
ումՈնուսմՈնութ	IKE Porposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.
- Configuration		
- Develores		
- E-Servers 17-Address Messmered		
Tunneling Protocols		
	Filter -Nons-	Choose the filter to apply to the traffic that is transled through this LAN-to-LAN
EPPSsc	-	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN
HE Processis	IPSer NAT-T	rearrention through a NAT device. You ratest also enable IFSee over NAT-T under NAT Transmuser.
NAT Transporency Alerts	Bandwidth Policy -None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
- E-P Routing	Routing None	Choose the routing mechanism to use Parameters below are ignored if Network Initializes were in above.
-E-Events		aubusteety b canes.
- El <u>General</u>	Loral Network: If a LAN-to-LAN NAT rule is used, this is the Transb	ated Network address.
Load Balancing	Network List Vpn_locol_network	Specify the local network ofderess list or the IP address and wildcard music for this LAN-to-LAN connection.
The low Management	IP Address	Note: Enter a wildcard mark, which is the ownerse of a volumet mark. A
- Traffic Management	Wildeard Mask	wikinani assis kas 1s in bit positions to ignore, 0s in bit positions to match. For scample, 10.10.1.00.0.0.255 = all 10.10.1 mm addresses.
	Barasta Nationale Mall & Marall & MART will be used this is the Bas	neta Naturek addinace
- Monitoring	Network List vpn_remote_network	<ul> <li>Specify the senter network address list or the IP address and wildcard mask for</li> <li>Which is 1.50 memory in the intervention.</li> </ul>
	IP Address	- Ing LAN-ID-LAN CONSCIEN.
		Note: Enter a widdowd mask, which is the reverse of a subnet mask. A wildrard mask has is in bit positions to ignore, 0s in bit positions to match. For
Corres Barrows	Willocatti Mask	ranaple, 10.10 1 0.0 0.0 255 = all 10.10 1 ann adéresses.
attliture thing.	Add Concel	

7. Après avoir cliqué sur Add [ajouter], vous verrez apparaître, si votre connexion est bonne, la fenêtre « IPSec LAN-to-LAN-Add-Done » [IPSec LAN à LAN–ajouté].Cette fenêtre montre un résumé des informations sur la configuration du tunnel. De plus, la configuration du nom de groupe, du nom du SA et du nom du filtre se fait automatiquement. Vous pouvez modifier tout paramètre dans ce tableau.



Àce stade, le tunnel IPSec LAN à LAN a été configuré, et vous pouvez commencer à travailler. Si, pour une raison ou une autre, le tunnel ne fonctionne pas, vous pouvez vérifier si la configuration contient des erreurs.

8. Vous pouvez afficher ou modifier les paramètres IPSec LAN à LAN créés précédemment lorsque vous sélectionnez Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN [configuration > système > protocoles de tunnellisation > IPSec LAN à LAN ].L'illustration indique « test » comme nom de tunnel, et l'interface publique de l'extrémité distante est 30.30.30.1 conformément au

scenano.		
- Configuration		
	Configuration   System   Tunneling Protocols   IPSec   LAN-to-LAN	
- <del>G Systen</del>		Save
- @Servers		
- EAddress Management	This section late you configure IPSec 1.4 N.to.1.6 N connections 1.4 N.to.1.6 N connections are set	whished with other VPN 3000 Concentratore
	PIX frequels, 2100/4000 series contents and other IPSec-convoluent security rates wars. To configure	a VPN 3002 or other remote access
<u>OPTP</u>	connection, go to User Management and configure a Group and User. To configure NAT over LAN	-to-LAN, go to LAN-to-LAN NAT Bules.
L2TP		
EHPSeo	If non-work to define a set of networks on the local or remote side of the LAN-to-LAN connection	configure the necessary Network Lists prior.
LAN-to-LAN	in creating the connection	compact in accounty <u>increases</u> pain
IKE Proposals	to occurring the contract.	
	(Tak the Addition to add a 1 kM to 1.6 M accuration, or select a connection and click Madifu or	Dalata
-Nerts	CALK THE MAN CARAN TO THE A LIFE OF CALLED CONTRACTION, OF SELECT A CONTRACTION AND CALLED HAMBING OF	Den II.
- CHP Routing	(TV indicates a dischard 1 kM to 1.6 M association)	
Management Protocols	(D) Inficates a disabled LAN-10-LAN configuration.	
- @Events		
- Deneral	LAN-to-LAN	
- I Client Update	Connection	Actions
Load Balancing	test (30.30.30.1) on Ethernet 2 (Public)	
		A HAR
- G-Policy Management		A00
Access Hours		Modify
- Tratfic Management		mouny
Network Lists		Delete
Hules		201010
<u>SA8</u>		
CIDECS CONTRACT		
THEAL TRANSPORT		
TO Cargon Matching		
- Monitoring		
LT MANAGEMENT		

9. Il peut arriver que votre tunnel ne soit pas activé si votre proposition IKE figure dans la liste des propositions inactives. Sélectionnez Configuration > System > Tunneling Protocols> IPSec > IKE Proposals [configuration > système > protocoles de tunnellisation > IPSec > propositions IKE] pour configurer la proposition IKE active.Si votre proposition IKE figure dans la liste des propositions inactives, vous pouvez l'activer en sélectionnant la proposition IKE en question, puis en cliquant sur le bouton Activate [activer]. Ce schéma illustre la proposition « IKE-AES256-SHA » dans la liste des propositions actives.

-P <u>Configuration</u>						
	Configuration   System   Tunneling Protoco	ls   IPSec   IKE Propos	als			
- <del>P</del> System				Save		
- I Servers						
- (-)-Address Management	Add, delete, prioritize, and configure IKE Proposals.					
-G-Turneling Protocols						
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Select an Inactive Proposal and click Artivate to make i	elect as Inactive Promosal and chick Artivate to make it Artive, or click Modify. Conv or Delete as anyoportate,				
	Select as Active Proposal and click Deactivate to make	it Inactive, or click Move Up	or Move Down to change its priority.			
	Click Add or Copy to add a new Inactive Proposal. IKE	Proposals are used by Secur	ity Associations to specify IKE parameters.			
LAN-10-LAN						
KE Projections	Active		Inactive			
Alerte	Proposals	Actions	Proposals			
- Realize	CiscoVPNCtient-3DES-MD5	1	IKE-1DES-SHA-DSA			
- City House of Protocols	IKE-3DES-MD5	<< Activate	IKE-1DES-MD5-BSA-DH1			
- CE Events	IKE-3DES-MD5-DH1	Description for the second	IKE-DES-MD5-DH7			
-(T)-General	IKE-DES-MD5	Descivale>>	CiscoVPNClient-3DES-MD5-RSA			
- (*) Client Update	IKE-3DES-MD5-DH7	Moue Un	CiscoVPNClient-3DES-SHA-DSA			
Load Balancing	CiscoVPNClient-3DES-MD5-DH5	mare op	CiscoVPNClient-3DES-MD5-RSA-DH5			
	Cisco//PNClient-AES128-SHA	Move Down	CiscoVPNClient-3DES-SHA-DSA-DH5			
- E-Policy Management	IKE-AES128-SHA		CiscoVPNClient-AES256-SHA			
- <u> Administration</u>	IKE-3DES-MD5-RSA	Add				
• Monitoring	IKE-AES256-SHA	Madifiz				
		Moully				
		Сору				
		Delete				
			1			

10. Allez à **Configuration > Policy Management > Traffic Management > Security Associations** [configuration > gestion des politiques > gestion du trafic > associations de sécurité] pour vérifier si les paramètres du SA sont

corrects.	
Genflouration	Configuration   Policy Management   Traffic Management   Security Associations Save This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use <u>IKEProposals</u> to regotiate IKE parameters. Click Add to add an SA, or select an SA and click Modify or Delete.
LAN-to-LAN     HE Processis     HE	IDSec SAs     Ardens       ESP-3DES-MD5     ESP-3DES-MD5       ESP-3DES-MD5-DH7     ESP-3DES-NONE       ESP-3DES-NONE     Add       ESP-3DES-MD5     Modity       ESP-218-SHA     Modity       ESP-218-SHD5     ESP-218-SHD5       ESP-218-SHD5     ESP-218-SHD5

11. Cliquez sur le nom du SA (ici, L2L : test), puis cliquez sur Modify [modifier] aux fins de vérification.Si un des paramètres ne correspond pas à la configuration de l'homologue distant, celui-ci peut être modifié ici.

Configuration	Configuration   Policy Management   Traffic Managem	ent   Security Associations   Modify
	Modify a configured Security Association.	
Address Management     Durneling Protocols	SA Name L2L: test	Specify the name of this Security Association (SA).
	Inheritance From Bule 💌	Select the granukarity of this SA.
LAN-ID-LAN	IPSec Parameters	
NAT Transparency	Authentication Algorithm ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
<u>Alerts</u> D@.Boxting	Encryption Algorithm AES-256	Select the ESP encryption algorithm to use.
-ED-Management Protocols	Encapsulation Mode Tunnel 🖃	Select the Encapsulation Mode for this SA.
- Events - El-General	Perfect Format Disabled	Select the use of Perfect Forward Secrecy.
End Balancing	Lifetime Measurement	Select the lifetime measurement of the IPSe: heye
Policy Management	Data Lifetime 10000	Specify the data lifetime in kilobytes (ICB).
Access Hours	Time Lifetime 28800	Specify the time lifetime in seconds.
	IKE Parameters	
	Connection Type Bickreetional IKE Press 30 30 30 J	The Consection Type and IKE Ferrs cannot be modified on IFSec SA that is part of a LAN-to-LAN Connection.
EX/Policies	Negatiation Mode Main 💌	Select the IKE Negotiation mode to use
Group Matching     Group Matching     Group Matching	Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
-E <u>Monitoring</u>	Certificate C Entire certificate clain. Transmission © Identity certificate only	Chooses how to send the digital certificate to the IKE power.
	IKE Proposal IKE AES256 SHA	Select the IKE Proposal to use as IKE initiator.
CISCO SYSTEMS	Apply Concel	

## **Vérification**

#### Vérifiez la configuration du routeur

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'<u>Output Interpreter Tool</u> (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

 show crypto isakmp sa—Affiche toutes les IKE SA actuelles chez un homologue. L'état QM\_IDLE indique que le SA demeure authentifié avec son homologue et peut être utilisé pour un prochain échange de mode rapide. Il se trouve alors au repos.
 ipsec\_router#show crypto isakmp sa

dst	src	state	conn-id	slot
20.20.20.1	30.30.30.1	QM_IDLE	1	0

 show crypto ipsec sa — Affiche les paramètres utilisés par les SA. Recherchez les adresses IP de l'homologue, les réseaux accessibles aux niveaux local et distant et le jeu de transformations utilisé. Il y a deux SAS ESP, une dans chaque direction. Ici, il est vide étant donné que les ensembles de transformation AH sont utilisés.
 ipsec\_router#show crypto ipsec sa

local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

```
interface: Ethernet1/0
Crypto map tag: vpn, local addr. 30.30.30.1
protected vrf:
```

```
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
```

#### current\_peer: 20.20.20.1:500

PERMIT, flags={origin\_is\_acl,} #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145 #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 6, #recv errors 0 local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1 path mtu 1500, media mtu 1500 current outbound spi: 54FA9805 inbound esp sas: spi: 0x4091292(67703442) transform: esp-256-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow\_id: 1, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4471883/28110) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x54FA9805(1425709061) transform: esp-256-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow\_id: 2, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4471883/28110) IV size: 16 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

 show crypto engine connections active : Cette commande affiche les connexions de session chiffrées qui sont actuellement actives pour tous les moteurs de chiffrement. Chaque ID de connexion est unique. Le nombre de paquets chiffrés et déchiffrés est affiché dans les deux dernières colonnes.

ipsec_router# <b>show crypto engine connections active</b>								
ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt		
1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	0	0		
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	0	19		
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0		

#### Vérifiez la configuration du concentrateur VPN

Voici la marche à suivre pour vérifier la configuration du concentrateur VPN.

 Tout comme les commandes show crypto ipsec sa et show crypto isakmp sa sur les routeurs, vous pouvez consulter les statistiques IPSec et IKE lorsque vous sélectionnez Monitoring > Statistics > IPSec [surveillance > statistiques > IPSec] sur les concentrateurs VPN.

-3-Configuration	Monitoring   Statistics   IPSec		Thursday,	U1 Jan	wary 2004 19:32:36
- ElSystem				F	leset 🥔 Refresh 🔞
FiUser Management	IKE (Phase 1) Statistics	IPSec (Phase 2) Statistics			
Policy Management	Active Tunnels	L	Active Tunnels	l	
Access Hours	Total Tunnels	2	Total Tunnels	2	
Network Lists	Received Bytes	3545268	Received Bytes	3602	
Rules	Sent Bytes	5553204	Sent Bytes	5376	
<u>SAs</u>	Received Packets	60187	Received Packets	145	
Eller2	Sent Parkets	60299	Sent Packets	51	
BAY Policies	Received Parkets Dropped.	0	Received Parkets Dropped	0	
	Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	U	
- Administration	Received Notifies	60084	Sent Packets Dropped	0	
ESoftware Undete	Sent Notifies	120172	Inhound Authentirations	145	
Concentrator	Received Phase-2 Eachanges	2	Failed Inbound Authentications	0	
<u>Clients</u>	ents Sent Phase-2 Exchanges		Outbound Authentirations	51	
Rebot Status	Invalid Phase-2 Exchanges Received	D	Failed Outboard Authentications	U	
Eins	Invalid Phase 2 Eachanges Sent	0	Decryptions	145	
Monitoring Refresh	Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0	
- Ele Management	Rejected Sent Phase-2 Exchanges	0	Encryptions	51	
Swap Conflo File	Phase-2 SA Delete Requests Received	0	Failed Encryptions	0	
	Phase-2 SA Delete Requests Sent	50	System Capability Failures	ū	
XML Export	Initiated Tunnels	0	No-SA Failures	0	
EP-Certificate Management	Failed Initiated Tunnels	0	Protocol Use Failures	0	
Enrollment	Failed Remote Tunnels	0			
	Authentication Failures	0			
Routing Table	Decryption Failures	D			
Dynamic Filtere	Hash Validation Failures	0			
Cisco Systems	System Capability Failures	0			
thuthu	No-SA Failures	0			

 Àl'instar de la commande show crypto engine connections active sur les routeurs, vous pouvez utiliser la fenêtre Administration-Sessions sur le concentrateur VPN pour afficher les paramètres et les statistiques des connexions actives IPSec LAN à LAN ou des tunnels.

Configuration	Administration   Ad	iminister Ses	slons					Thursday	, 01 Janu	ary 2004-19:30:20
	This screen shows statist on that session's name. T	tios for sessions. 'o log out a sessio	To refiech i m, chick <b>Leg</b>	he statistic: gent in the t	s, click <b>Refresh</b> able below. To b	Selant a Gro est the patwo	up to filter the so atk connection to	estions. For n a sension, ch	uore informe ck Ping.	tion on a session, click
- Brook Lide - Bros - SA2 - Citers - EthAI	Group —All- Logout All: <u>PPTP User</u> Session Summary	127P User   125	lec User   II	Sec LAN-b	<u>o-LAN</u>					
Group Matching	Active LAN-to- LAN Sessions	Active Remot Access Session	e Activ 15	e Manager Sessions	nent Total A Sessi	ctive Pe ous	ik Concurrent Sessions	Conrus	vent 1 Limit	fotal Cumulative Sessions
Administer Sessions	1	0		1	2		3	400		19
Concentrator Concentrator Concentrator Concentrator Connection Name IP Address Produced Encryption Legis Time Duration					ete Access S Byoss Tx	estions   Ma Bytes Ra	Actions			
-the	test	30.30.30.1	IPSecLAX	l-to-LAN	AES-256	Jan 1 19:57	29 0:02:51	2128	2128	[Logent   Ping]
Horitoria Seriesi Horitoria Seriesi Horitoria Management Contribute Management Contribute Management Chical Type Chical Type					sations   Ma Bytes	nogement Sessions ]				
		Public IP A66	THEF		Encryption	Services	ration	Version	Bytes	HX
	140 demoit Actess desseds									
Management Sessions [LAN-to-LAN Sessions   Barnate Access Sessi							la Accesa Sessiona ]			
	Administrator	IP Addre	ss Pi	retecol	Encryption	L	gin Time	Duratie	h	Artiens
	admin.	172.161.2	нт	P	None	Jan OI 1	91742	0:12:38	[1.000	ot [ Ping ]

## **Dépannage**

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

#### Dépanner le routeur

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

**Remarque :** Consulter les <u>renseignements importants sur les commandes de débogage</u> avant d'utiliser les commandes de **débogage**.

- debug crypto engine : Cette commande affiche le trafic chiffré. Le moteur de chiffrement est le mécanisme qui procède au chiffrement et au déchiffrement. Un moteur de chiffrement peut être un accélérateur logiciel ou matériel.
- debug crypto isakmp : Cette commande affiche les négociations ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1 d'IKE.
- debug crypto ipsec Affiche les négociations IPsec de la phase IKE 2.

Consultez la section sur le <u>dépannage d'IPSec portant sur les connaissances et l'utilisation des</u> <u>commandes de débogage pour obtenir des informations détaillées sur le sujet et des exemples de</u> <u>résultats.</u>

#### Dépannage du concentrateur VPN

Àl'instar des commandes de **débogage des routeurs Cisco, vous pouvez configurer des classes** d'événements pour afficher les alarmes.

1. Sélectionnez Configuration > System > Events > Classes > Add [configuration > système > événements > classes > ajouter] pour activer la journalisation des classes d'événements.Ces

#### classes sont possibles pour IPsec :IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE

interfaces     Configuration   System   Events   Classes     Save Nor	ede d 📻
- Paysian Save Net	eded 🗖
- Ex <u>Servers</u>	
Enderess Monogement     This section lets you configure special handling of specific event classes.	
- 40 Tunneling Protocols	
EVER Souther Click the Add button to odd on event class, or select on event class and thick Modify or Delete.	
42-Minimizationent Producedis	
Cick here to configure superal event parameters.	
Central Central	
Castronad	
Category Constants	
Symul Servers IKEDECCCE	
IPSECOEG	
MB2TEAP Add	
Ender Levels	
Local Palentini Modily	
- Calleer a longer at the second	
Litter Mensoerent	
m Administration	
+ Montoring	

2. Pendant l'ajout, vous pouvez également sélectionner le niveau de gravité de chaque classe, en fonction de celui que transmet l'alarme.Les alarmes peuvent être gérées par l'une ou l'autre des méthodes suivantes :par le journalpar l'affichage sur la consolepar l'envoi au serveur Syslog UNIXpar l'envoi d'un courrielpar l'envoi d'une pièce à un serveur de protocole SNMP (Simple Network Management

Protocol)						
-E+Configuration						
	Configuration   System   Events   Classes   Add					
DEvision     Devision     Devision     Devision	This screen lets you add and configure an event class for spe	cial handling.				
Tunneling Protocols     EP Routing	Class Name KEDBG	Select the event class to configure.				
Bytensigement Protocols     Bytensis	Enable 🖂	Check to enable special handling of this class.				
General FTP Backup	Hone of the following values has been set to Use Event List, the Event List can be seen by viewing Configuration   System   Events   General.					
	ranging a value set to Use Svere List will override the sections of the Event List referring to this event class.					
	Events to Log Severities 1-5	Select the events to enter in the log.				
Enail Recipients	Events to Console Severities 1-3 💌	Select the events to display on the consols.				
- El General	Events to Syslog None	Select the events to send to a Syslog Server.				
Eclent Update	Events to Email None	Select the events to send to an Read Recipient.				
Der Management     Delicy Management	Events to Trap None 💌	Select the events to send to an SNMP Trap Destination.				
	Add Cancel					

 Sélectionnez Monitoring > Filterable Event Log [surveillance > journal des événements avec filtres] pour surveiller les alarmes activées.



## Informations connexes

- <u>Standard de cryptage avancé (AES)</u>
- Module de chiffrement VPN DES/3DES/AES
- Exemples de configuration IPSec
- Page d'assistance du Client VPN 3000 Series Cisco
- Page de support de la négociation IPSec/des protocoles IKE

#### 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.

#### 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.

#### 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.