

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurez le concentrateur VPN](#)

[Vérifiez](#)

[Vérifiez la configuration de routeur](#)

[Vérifiez la configuration du concentrateur VPN](#)

[Dépannez](#)

[Dépanner le routeur](#)


[Dépannez le concentrateur VPN](#)

[Informations connexes](#)

[Introduction](#)

Ce document affiche comment configurer un tunnel d'IPsec entre un concentrateur de Cisco VPN 3000 et un routeur de Cisco avec la norme de chiffrement anticipée (AES) comme algorithme de chiffrement.

AES est une nouvelle publication de la Norme fédérale pour le traitement de l'information (FIPS) créée par le National Institute of Standards and Technology (NIST) à utiliser comme méthode de cryptage. Cette norme spécifie un algorithme de chiffrement symétrique AES qui remplace le Norme de chiffrement de données (DES) pendant qu'une intimité transforment pour IPsec et Échange de clés Internet (IKE). AES a trois longueurs principales différentes, une clé 128-bit (le par défaut), une clé 192-bit, et une clé 256-bit. La caractéristique AES dans le Cisco IOS® ajoute le soutien de la nouvelle norme de chiffrement AES, avec le bloc de chiffrement enchaînant le mode (CBC), à IPsec.

Référez-vous au [site de centre de ressources de protection de l'ordinateur NIST](#)  pour plus d'informations sur AES.

Référez-vous au [tunnel d'IPsec d'entre réseaux locaux entre l'exemple de configuration de concentrateur de Cisco VPN 3000 et de Pare-feu PIX](#) pour plus d'informations sur la configuration de tunnel entre réseaux locaux entre un concentrateur VPN 3000 et le Pare-feu PIX.

Référez-vous au [tunnel d'IPsec entre PIX 7.x et](#) pour en savoir plus d'[exemple de configuration de concentrateur VPN 3000](#) quand le PIX a la version de logiciel 7.1.

[Conditions préalables](#)

Conditions requises

Ce document exige une compréhension de base de protocole IPsec. Référez-vous à une [introduction au chiffrement IPsec](#) pour se renseigner plus sur IPsec.

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

- **Configurations requises du routeur** - La caractéristique AES a été introduite dans le Logiciel Cisco IOS version 12.2(13)T. Afin d'activer AES, votre routeur doit prendre en charge IPsec et exécuter une image IOS avec de longues clés de "k9" (le sous-système de "k9").**Remarque:** Le support matériel pour AES est également disponible sur des modules VPN d'accélération AES de Cisco 2600XM, 2691, 3725, et 3745. Cette caractéristique n'a aucune implication de configuration et le module de matériel est automatiquement sélectionné si chacun des deux sont disponibles.
- **Conditions requises de concentrateur VPN** - Le support logiciel pour la caractéristique AES a été introduit dans la version 3.6. Le support matériel est fourni par le nouveau processeur amélioré et extensible de cryptage (SEP-E). Cette caractéristique n'a aucune implication de configuration.**Remarque:** Dans la version 3.6.3 de concentrateur de Cisco VPN 3000, les tunnels ne négocient pas à AES dû à l'ID de bogue Cisco [CSCdy88797](#) (clients [enregistrés](#) seulement). Ceci a été résolu de la version 3.6.4.**Remarque:** Le concentrateur de Cisco VPN 3000 utilise l'un ou l'autre des septembre ou septembre - Modules E, pas chacun des deux. N'installez pas chacun des deux sur le même périphérique. Si vous installez un module SEP-E sur un concentrateur VPN qui contient déjà un module de SEPT, le concentrateur VPN désactive le module de SEPT et utilise seulement le module SEP-E.

Composants utilisés

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

- Routeur de gamme Cisco 3600 avec la version du logiciel Cisco IOS 12.3(5)
- Concentrateur Cisco VPN 3060 avec la version de logiciel 4.0.3

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, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

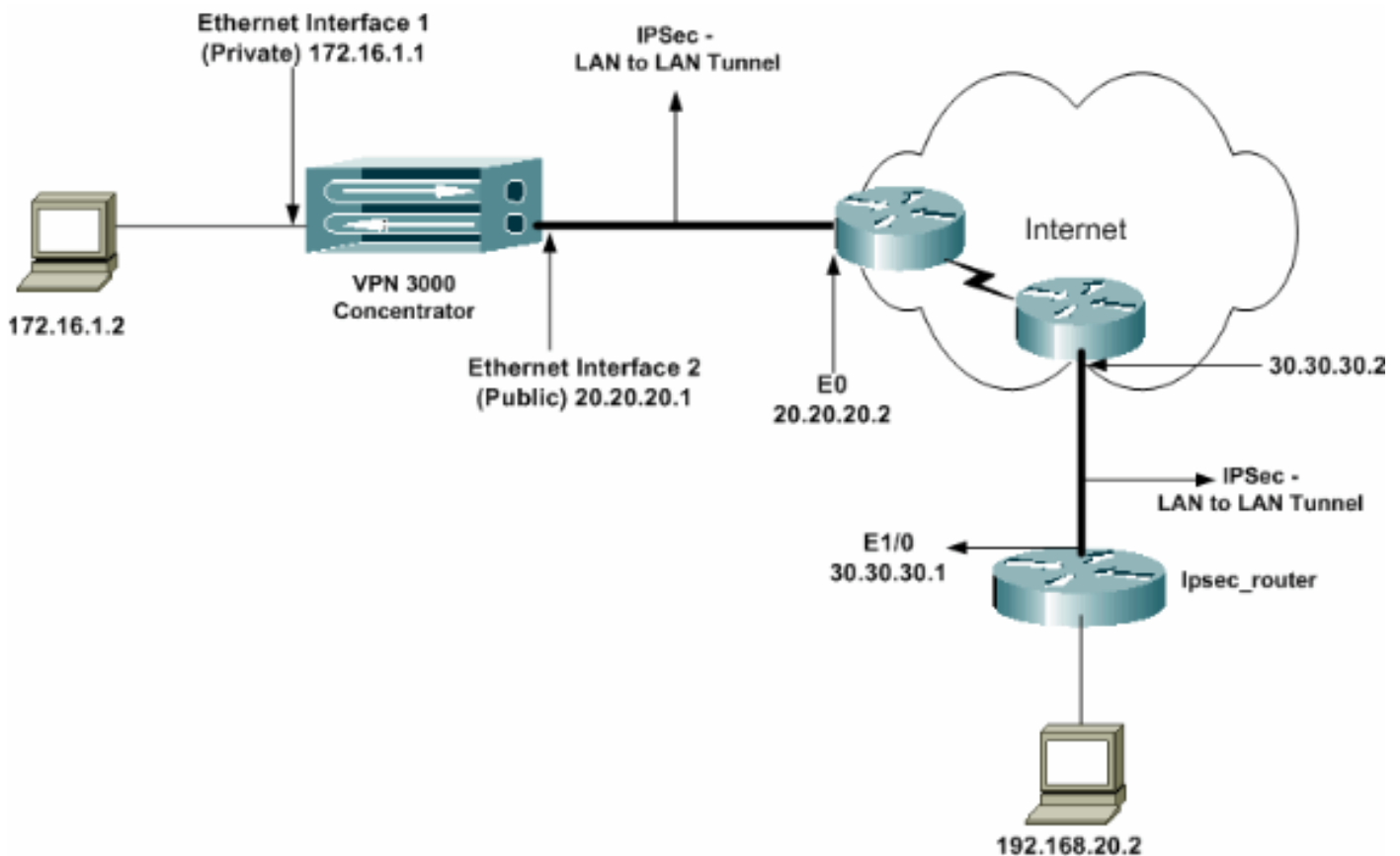
Configurez

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

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) 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 d'IPsec](#)
- [Concentrateur VPN](#)

configuration d'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!interface Ethernet1/0ip
address 30.30.30.1 255.255.255.0ip nat outsidehalf-
duplexcrypto map vpn!--- Configures the interface to use
the crypto map "vpn" for IPsec. !interface
FastEthernet2/0ip address 192.168.20.1 255.255.255.0ip
nat insideduplex autospeed auto!ip nat pool mypool
30.30.30.3 30.30.30.3 netmask 255.255.255.0ip nat inside
source route-map nonat pool mypool overloadip http
serverno ip http secure-serverip classlessip 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 0line aux 0line
vty 0 4login!end

```

Remarque: Bien que la syntaxe d'ACL soit inchangée, les significations sont légèrement différentes pour crypto ACLs. Dans crypto ACLs, l'**autorisation** spécifie cela les paquets assortis devrait être chiffrée, tandis que **refusez** spécifie cela les paquets assortis n'ont pas besoin d'être chiffrés.

[Configurez le concentrateur VPN](#)

Des concentrateurs VPN ne sont pas préprogrammés avec des adresses IP dans leurs configurations d'usine. Vous devez employer le port de console pour configurer les configurations initiales qui sont une interface de ligne de commande pilotée par menu (CLI). Référez-vous à [configurer des concentrateurs VPN par la console](#) pour les informations sur la façon dont configurer par la console.

Après l'adresse IP sur des Ethernet 1 l'interface (privée) est configurée, le repos peut être configuré ou utilisant le CLI ou par l'intermédiaire de l'interface du navigateur. L'interface du navigateur prend en charge le HTTP et le HTTP au-dessus du Protocole SSL (Secure Socket Layer).

Ces paramètres sont configurés par la console :

- **Heure/date** - La date et heure correcte sont très importante. Ils aident à s'assurer que se connecter et entrées de traçabilité sont précis, et que le système peut créer un Security Certificate valide.

- **Interface (privée) d'Ethernet 1** - L'adresse IP et le masque (de notre topologie du réseau 172.16.1.1/24).

En ce moment, le concentrateur VPN est accessible par un navigateur HTML du réseau intérieur. Pour les informations sur configurer le concentrateur VPN dans le mode CLI, référez-vous à la [configuration rapide utilisant le CLI](#).

1. Tapez l'adresse IP de l'interface privée du navigateur Web pour activer l'interface gui. Cliquez sur en fonction l'icône **nécessaire par sauvegarde** pour sauvegarder des modifications à la mémoire. Le nom d'utilisateur et mot de passe de par défaut d'usine sont le « admin » qui distingue les majuscules et minuscules.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Configuration | Administration | Monitoring

Logged in: admin

Main

Welcome to the VPN 3000 Concentrator Manager.

In the left frame of the navigation bar above, click the function you want:

- [Configuration](#) -- to configure all features of this device.
- [Administration](#) -- to control administrative functions on this device.
- [Monitoring](#) -- to view status, statistics, and logs on this device.

The bar at the top right has:

- [Main](#) -- to return to this screen.
- [Help](#) -- to get help for the current screen.
- [Support](#) -- to access VPN 3000 Concentrator support and documentation.
- [Logout](#) -- to log out of this session and return to the Manager login screen.

Under the location bar in the upper right, these icons may appear. Click to:

- [Save](#) -- save the active configuration and make it the boot configuration.
- [Save Needed](#) -- as above, indicating you have changed the active configuration.
- [Reset](#) -- to temporarily reset statistics to zero.
- [Restore](#) -- to restore statistics from their real values.
- [Refresh](#) -- to refresh statistics.

2. Après que vous apportiez le GUI, **Configuration > Interfaces > Ethernets** choisis **2 (public)** pour configurer l'interface des Ethernets

Configuration | Interfaces | Ethernet 2

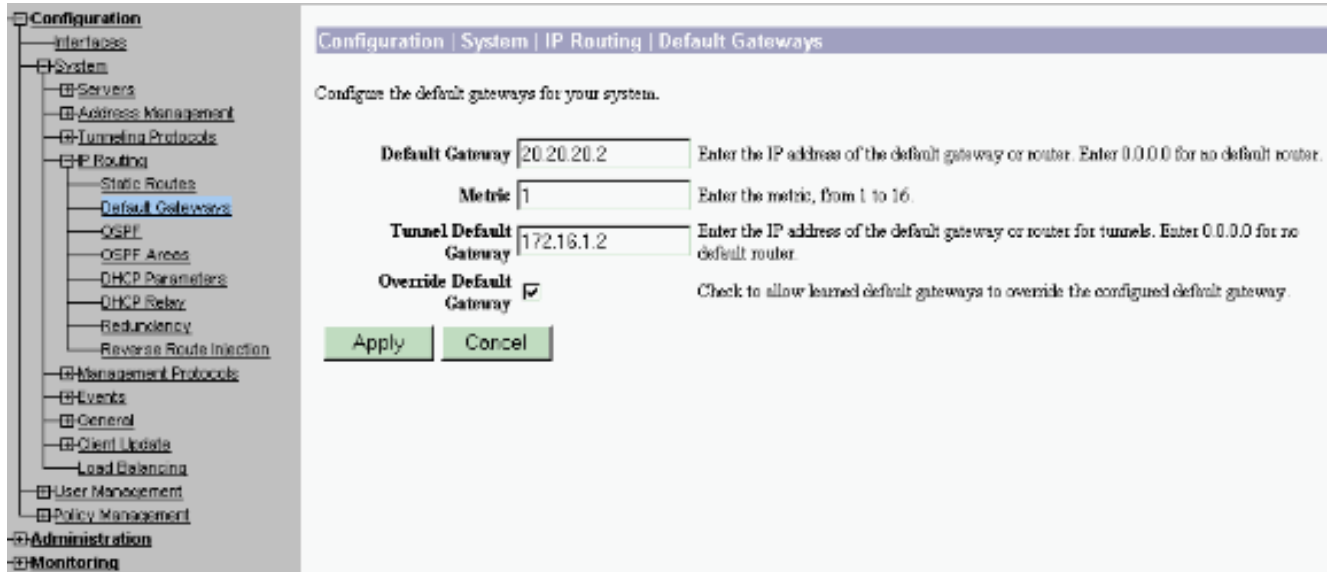
Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | Bandwidth

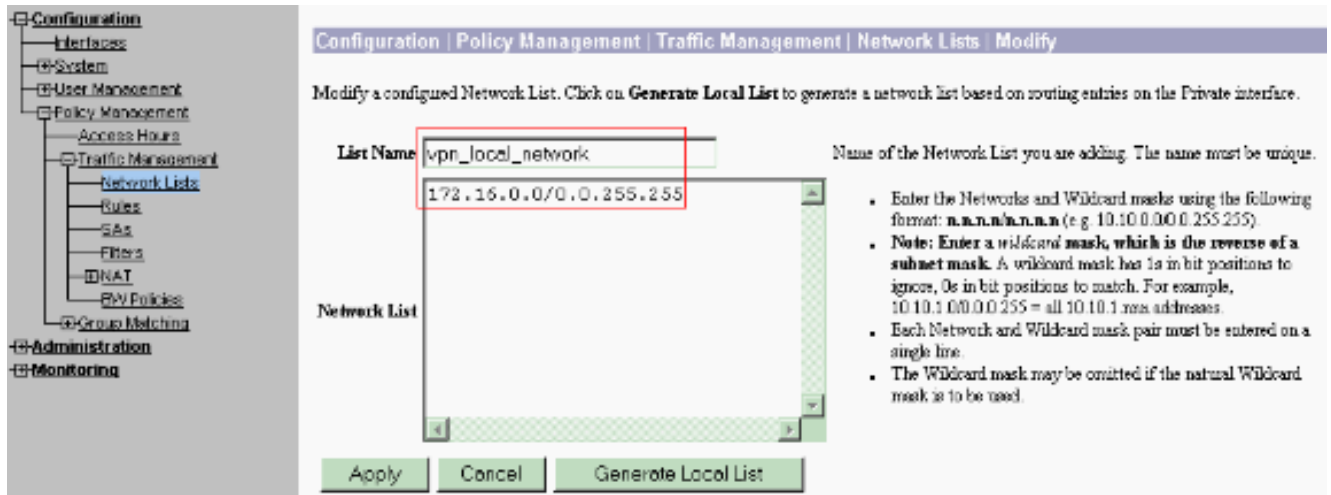
General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	20.20.20.1	
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00:90:A4:00:41:F9	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 (68 - 1500).
	Public Interface IPsec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPsec encapsulation, fragment prior to interface transmission	
		<input type="radio"/> Fragment prior to IPsec encapsulation, with Path MTU Discovery (ICMP)	
		<input type="radio"/> Fragment prior to IPsec encapsulation, without Path MTU Discovery (Clear DF bit)	

Apply Cancel

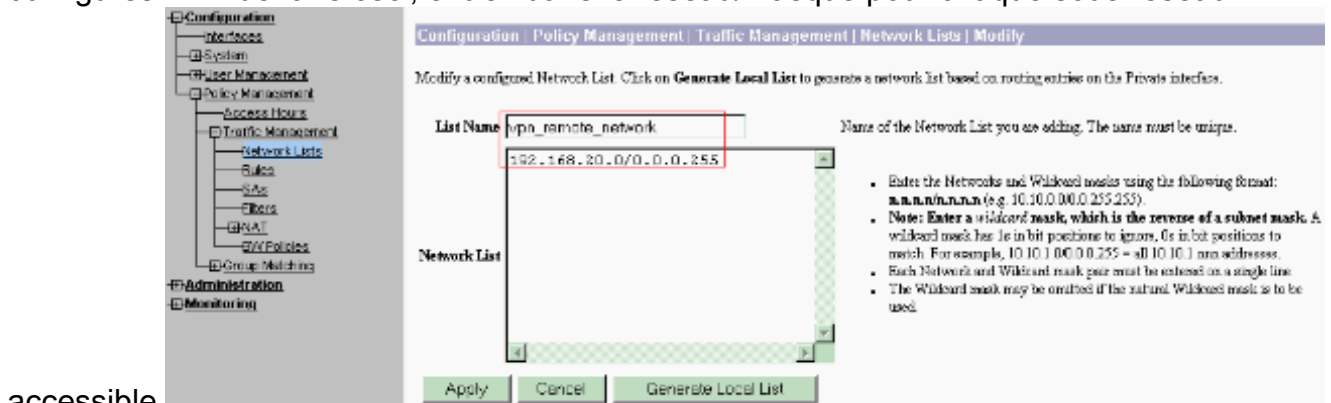
3. La configuration > le système > le Routage IP > les passerelles par défaut choisies configurent la passerelle par défaut (d'Internet) et la passerelle de par défaut de tunnel (à l'intérieur) pour qu'IPsec atteigne les autres sous-réseaux dans le réseau privé. Dans ce scénario, il y a seulement un sous-réseau disponible sur le réseau intérieur.



4. La configuration > la Gestion des stratégies > la gestion de trafic > les listes des réseaux choisies > ajoutent pour créer les listes des réseaux définissant le trafic à chiffrer. Les réseaux mentionnés dans la liste sont accessibles au réseau distant. Les réseaux affichés dans la liste ci-dessous sont des réseaux locaux. Vous pouvez également générer la liste de réseau local automatiquement par l'intermédiaire du RIP quand vous clic **générerez la liste locale**.



5. Les réseaux dans cette liste sont des réseaux distants et doivent être manuellement configurés. Afin de faire ceci, entrez dans le réseau/masque pour chaque sous-réseau



accessible.

Une fois terminés, ce sont les deux listes des réseaux :

6. La configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux choisis d'IPSec > ajoutent et définissent le tunnel entre réseaux locaux. Cette fenêtre a trois sections. La section supérieure est pour l'information réseau et les deux sections inférieures sont pour les listes de gens du pays et de réseau distant. Dans la section d'information réseau, sélectionnez le cryptage AES, type d'authentification, proposition d'IKE, et tapez la clé pré-partagée. Dans les sections inférieures, point aux listes des réseaux que vous avez déjà créées, des listes de gens du pays et de distant respectivement.

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Enable Check to enable this LAN-to-LAN connection.

Name test Enter the name for this LAN-to-LAN connection.

Interface Ethernet2 (Public) (20.20.20.1) Select the interface for this LAN-to-LAN connection.

Connection Type Bidirectional Choose the type of LAN-to-LAN connection. An *Originate Only* connection may have multiple peers specified below.

Peers 30.30.30.1 Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.

Digital Certificate None (Use Preshared Keys) Select the digital certificate to use.

Certificate Transmission Entire certificate chain. Choose how to send the digital certificate to the IKE peer.
 Identity certificate only

Preshared Key cisco123 Enter the preshared key for this LAN-to-LAN connection.

Authentication ESP/MD5/HMAC-128 Specify the packet authentication mechanism to use.

Encryption AES-256 Specify the encryption mechanism to use.

IKE Proposal IKE-AES256-SHA Select the IKE Proposal to use for this LAN-to-LAN connection.

Filter None Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.

IPsec NAT-T Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPsec over NAT-T under NAT Transparency.

Bandwidth Policy None Choose the bandwidth policy to apply to this LAN-to-LAN connection.

Routing None Choose the routing mechanism to use. Parameters below are ignored if **Network AutoDiscovery** is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List vpn_local_network Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

Wildcard Mask

Note: Enter a wildcard mask, which is the reverse of a subnet mask. A 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 xxx addresses.

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List vpn_remote_network Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

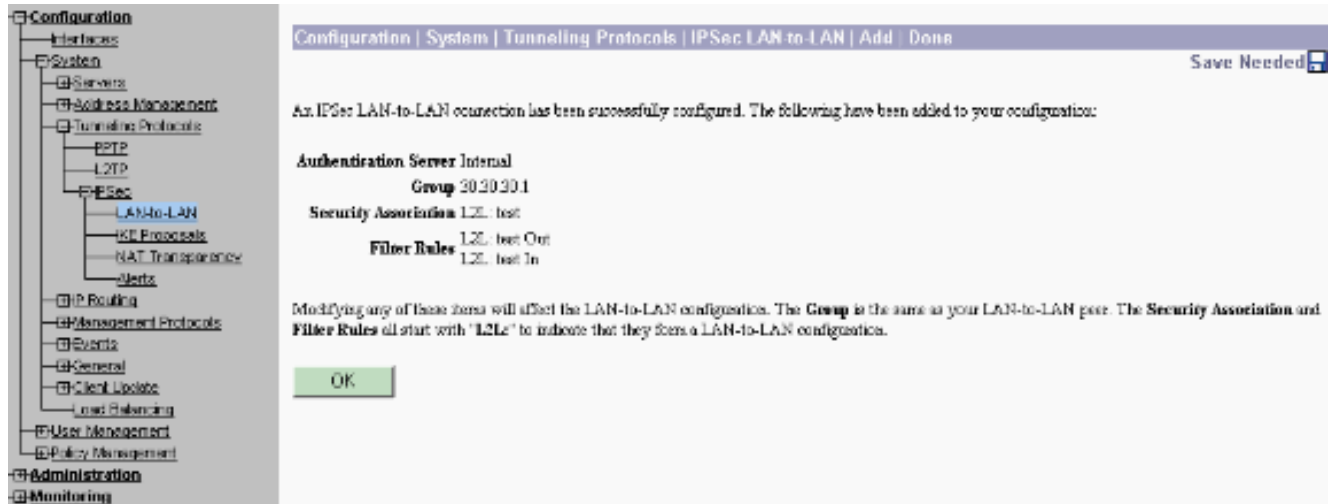
Wildcard Mask

Note: Enter a wildcard mask, which is the reverse of a subnet mask. A 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 xxx addresses.

Add **Cancel**

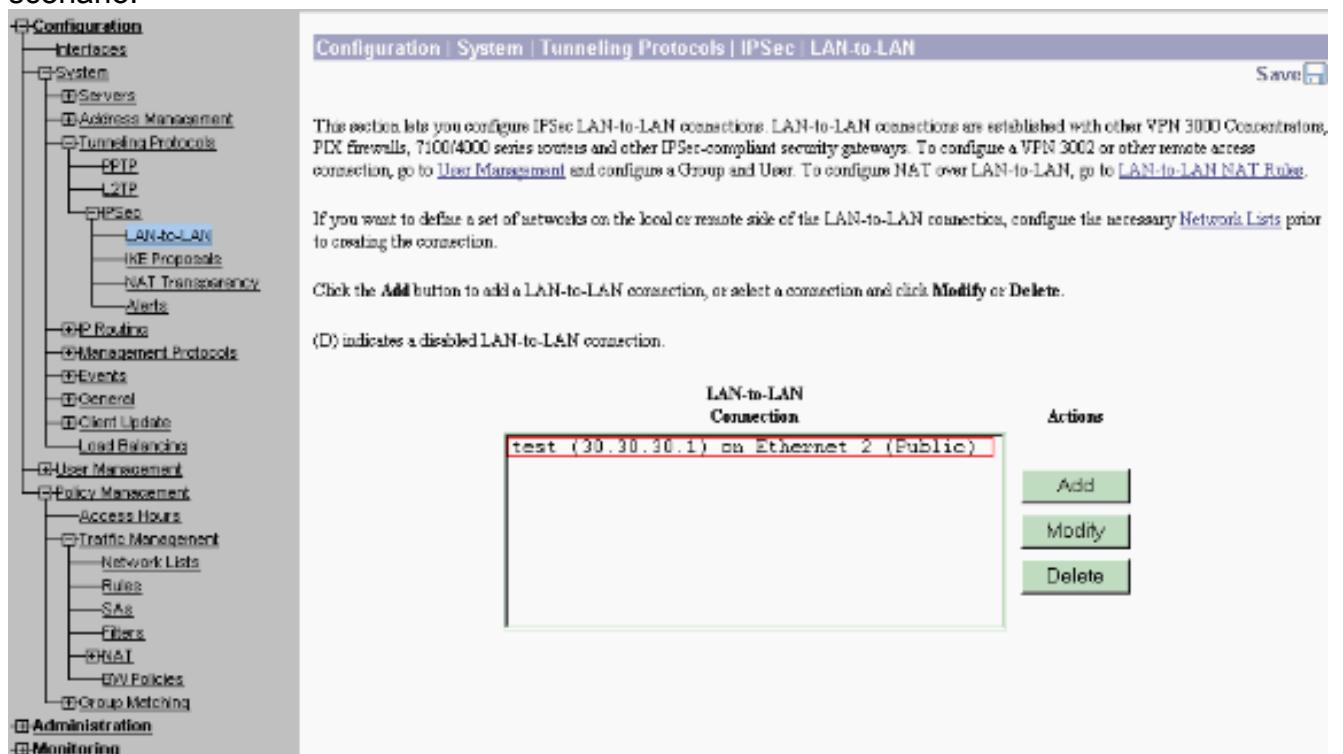
7. Après que vous cliquez sur Add, si votre connexion est correcte, vous êtes présenté avec la fenêtre Réseau local-à-RÉSEAU local-ajouter-faite par IPSec. Cette fenêtre présente une synthèse des informations de configuration de tunnel. Il configure également

automatiquement le nom de groupe, le nom SA, et le nom du filtre. Vous pouvez éditer tous les paramètres dans cette table.



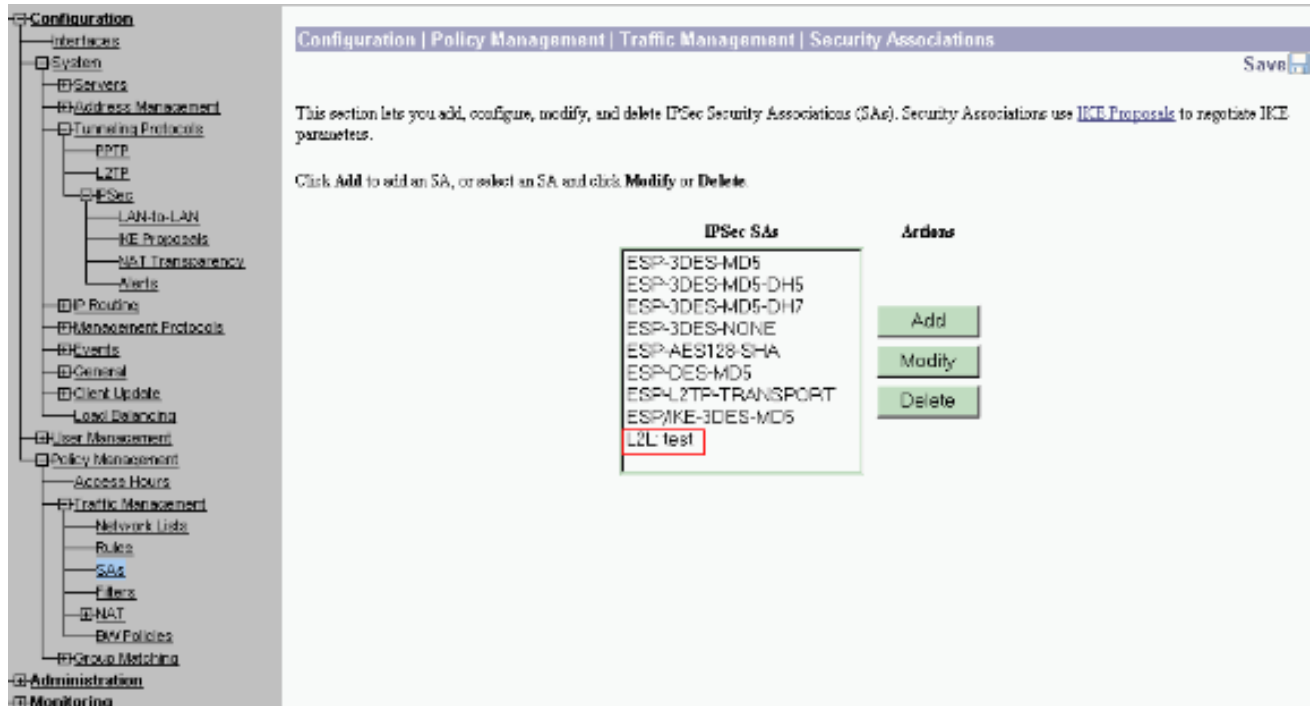
En ce moment le tunnel entre réseaux locaux d'IPsec a été installé et vous pouvez commencer fonctionner. Si, pour quelque raison, le tunnel ne fonctionne pas, vous pouvez vérifier des mauvaises configurations.

- Vous pouvez visualiser ou modifier les paramètres précédemment créés d'IPsec d'entre réseaux locaux quand vous sélectionnez la **configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux d'IPsec**. Ce graphique affiche le « test » car le nom du tunnel et de l'interface publique de l'extrémité distante est 30.30.30.1 selon le scénario.

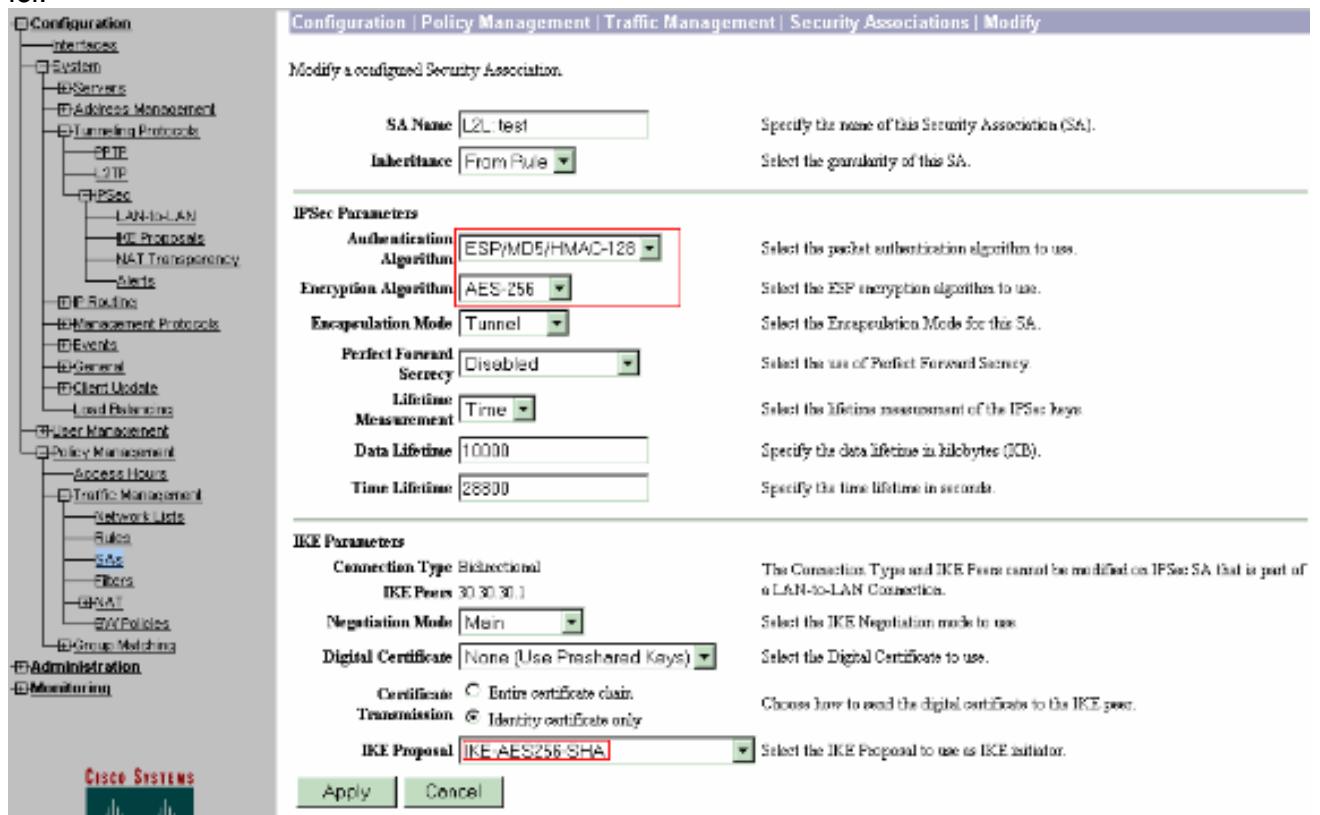


- Parfois, votre tunnel ne pourrait pas monter si votre proposition d'IKE est dans la liste inactive de propositions. **Configuration > protocoles de système > de Tunnellisation > IPsec > propositions** choisis d'IKE pour configurer la proposition active d'IKE. Si votre proposition d'IKE est dans « les propositions inactives » vous répertorient peuvent l'activer quand vous sélectionnez la proposition d'IKE et cliquez sur en fonction le bouton de **lancement**. Dans ce graphique la proposition sélectionnée "IKE-AES256-SHA" est dans la liste active de propositions.

10. Configuration > Gestion des stratégies > gestion de trafic > associations de sécurité choisies à vérifier si les paramètres SA sont corrects.



11. Cliquez sur le nom SA (dans ce cas, L2L : le test), et cliquez sur alors modifiez pour vérifier SAS. Si les paramètres l'un des ne s'assortissent pas avec la configuration de homologue distante, elle peut être changée ici.



[Vérifiez](#)

[Vérifiez la configuration de 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'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa ?** Affiche tout l'IKE en cours SAS à un pair. L'état QM_IDLE dénote que les restes SA authentifiés avec son pair et peut être utilisé pour des échanges rapides ultérieurs de mode. Il est dans un état de 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 configurations utilisées par le courant SAS. 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. Puisqu'OH des jeux de transformations sont utilisés, il est vide.
`ipsec_router#show crypto ipsec sa interface: Ethernet1/0 Crypto map tag: vpn, local addr. 30.30.30.1 protected vrf: local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0) 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:`
- **connexions de show crypto engine actives ?** Affiche les connexions de session chiffrées par active en cours pour tous les moteurs de chiffrement. Chaque ID de connexion est seul. Le nombre de paquets qui sont chiffrés et déchiffrés sont affichés dans les deux dernières colonnes.
`ipsec_router#show crypto engine connections active 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](#)

Terminez-vous ces étapes pour vérifier la configuration du concentrateur VPN.

1. Semblable au **show crypto ipsec sa** et au **show crypto isakmp sa** commande sur des Routeurs, vous pouvez visualiser les statistiques d'IPsec et d'IKE quand vous sélectionnez la **surveillance > les statistiques > l'IPSec** sur les concentrateurs



IKE Phase 1 Statistics		IKE Phase 2 Statistics	
Item	Count	Item	Count
Total Tunnels	2	Total Tunnels	2
Successes	0	Successes	0
Failures	0	Failures	0
Success Rate	0%	Success Rate	0%
Fail Rate	0%	Fail Rate	0%
Successes	0	Successes	0
Failures	0	Failures	0
Success Rate	0%	Success Rate	0%
Fail Rate	0%	Fail Rate	0%
Successes	0	Successes	0
Failures	0	Failures	0
Success Rate	0%	Success Rate	0%
Fail Rate	0%	Fail Rate	0%

2. Semblable à la commande **active de connexions de show crypto engine** sur des Routeurs, vous pouvez employer la fenêtre de Gestion-sessions sur le concentrateur VPN pour visualiser les paramètres et les statistiques pour tous les connexions entre réseaux locaux ou tunnels actifs d'IPsec.

Administration | Administer Sessions Thursday, 01 January 2004 19:30:20
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group:

Logout All: [PPTP User](#) | [L2TP User](#) | [IPSec User](#) | [IPSec LAN-to-LAN](#)

Session Summary

Active LAN-in-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
1	0	1	2	3	400	19

LAN-in-LAN Sessions [[Remote Access Sessions](#)] [[Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions
test	30.30.30.1	IPSec LAN-to-LAN	AES-256	Jan 1 19:57:29	0:02:51	2128	2128	[Logout] [Ping]

Remote Access Sessions [[LAN-to-LAN Sessions](#)] [[Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	Actions
No Remote Access Sessions							

Management Sessions [[LAN-to-LAN Sessions](#)] [[Remote Access Sessions](#)]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions
admin	172.16.1.1	HTTP	None	Jan 01 19:17:42	0:12:38	[Logout] [Ping]

Dépannez

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

Dépanner le routeur

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

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

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

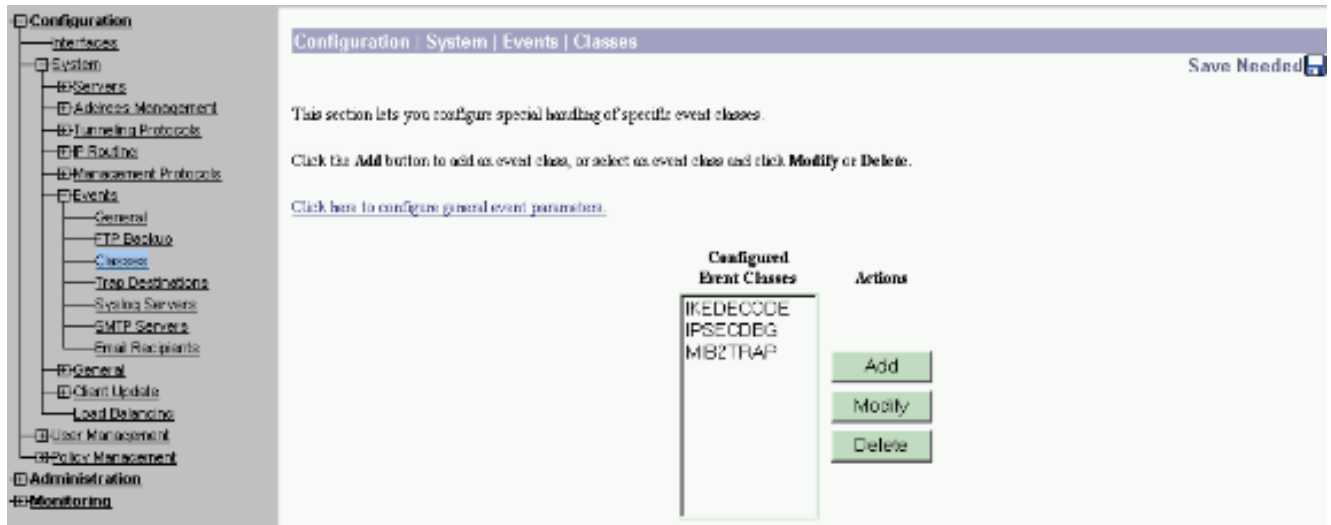
Référez-vous au [dépannage d'IPSec - Comprenant et utilisant des commandes de débogage](#) pour plus d'informations détaillées et de sortie témoin.

Dépannez le concentrateur VPN

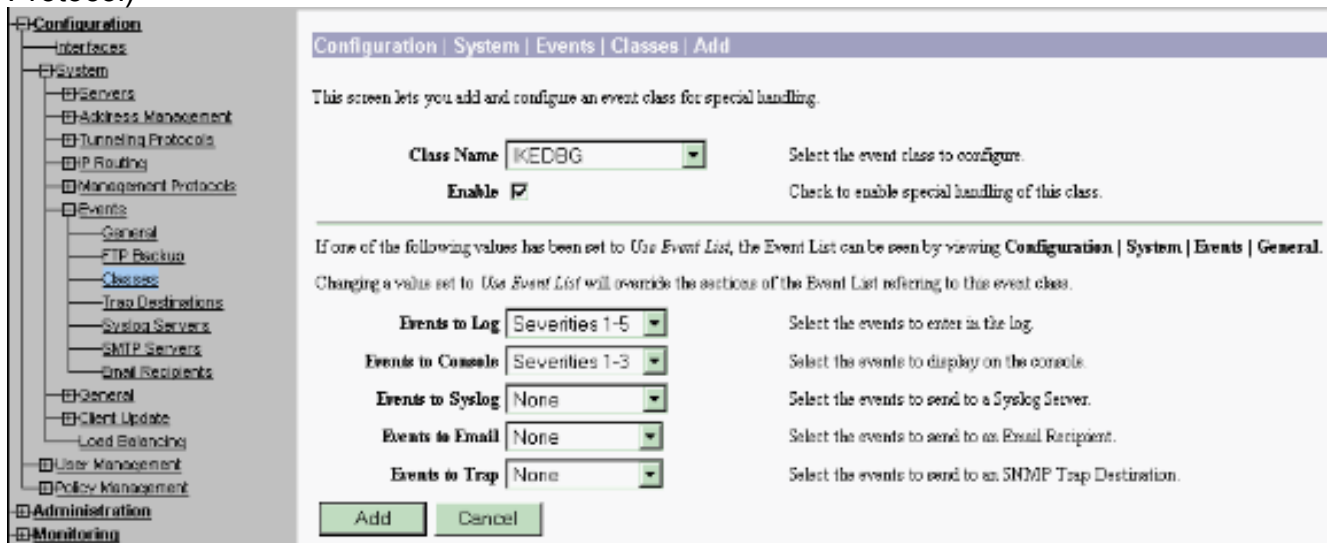
Semblable aux commandes de **débogage** sur les Routeurs de Cisco, vous pouvez configurer des

classes d'événement pour visualiser toutes les alarmes.

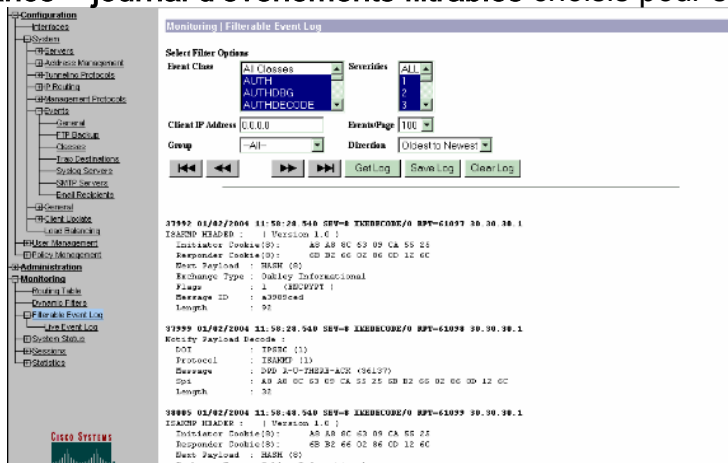
1. La configuration > le système > les événements > les classes choisies > ajoutent pour activer se connecter des classes d'événement. Ces classes sont disponibles pour IPsec : IKEKEDBG, IKEDECODE, IPSECDBG, IPSECDBG, IPSECDBG, IPSECDBG



2. Tout en ajoutant, vous pouvez également sélectionner le niveau d'importance pour chaque classe, basé sur le niveau d'importance que l'alarme est envoyée. Les alarmes peuvent être manipulées par une de ces méthodes : Par le log Affiché sur la console, Envoyé au serveur de Syslog UNIX, Envoyé comme email, Envoyé comme déroutement à un serveur de Protocole SNMP (Simple Network Management Protocol)



3. Surveillance > journal d'événements filtrables choisis pour surveiller les alarmes



activées.

Informations connexes

- [Norme AES \(Advanced Encryption Standard\)](#)
- [Module de chiffrement de VPN DES/3DES/AES](#)
- [Mise à jour de logiciel du concentrateur VPN](#)
- [Concentrateur VPN - Notes de mise à jour](#)
- [Concentrateur VPN configurant des interfaces IP](#)
- [Configurations d'échantillon d'IPSec](#)
- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Page d'assistance du Client VPN 3000 Series Cisco](#)
- [Page de support de la négociation IPSec/des protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)