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

Contenu

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 Computer Security Resource Center du NIST 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 configuration du tunnel IPSec entre le pare-feu PIX 7.x et le concentrateur 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 CSCdy88797 (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 Conventions relatives aux conseils techniques Cisco.

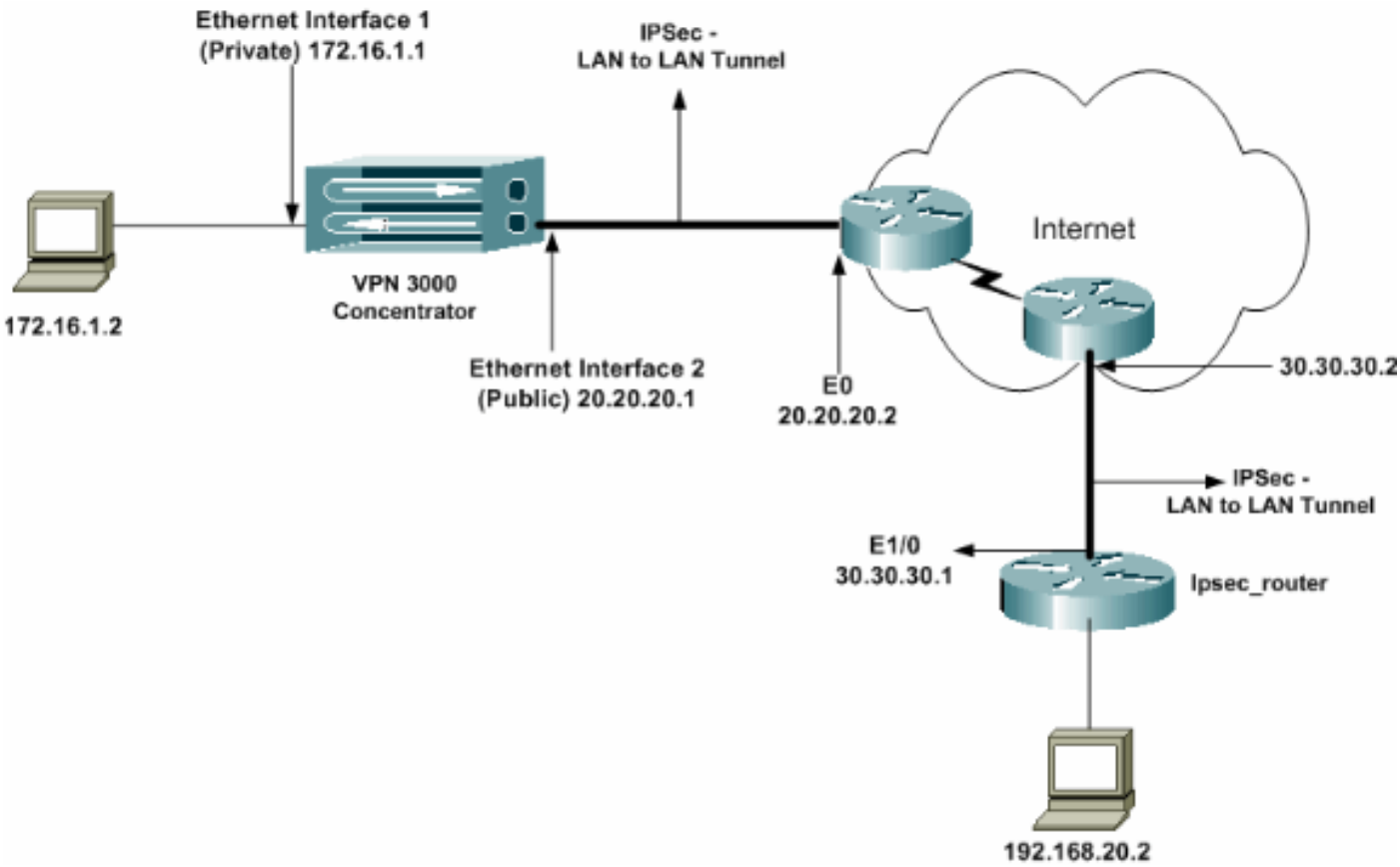
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés 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
- Concentrateur VPN

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
!
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.

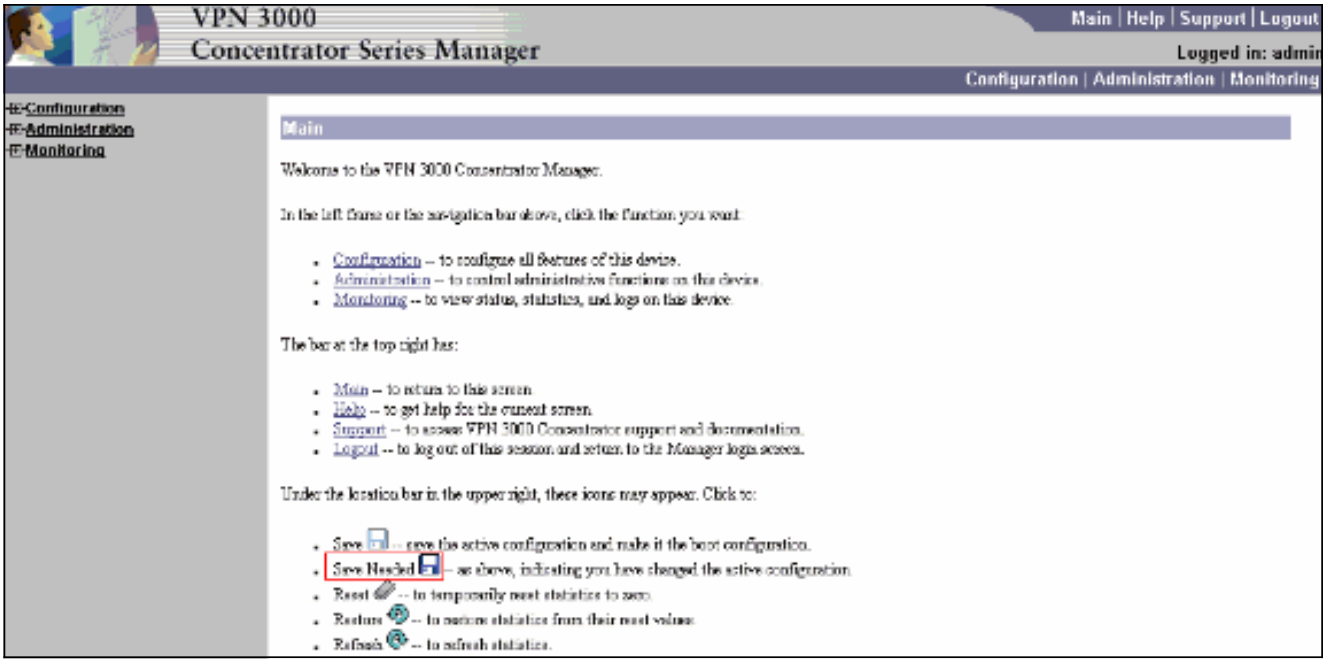
Une fois que l'adresse IP de l'interface Ethernet 1 (privée) est configurée, le reste peut être configuré à son tour au moyen de l'interface de ligne de commande ou de celle du navigateur. L'interface du navigateur prend en charge les protocoles HTTP et HTTP sur SSL (Secure Socket Layer).

Les paramètres suivants sont configurés par la console :

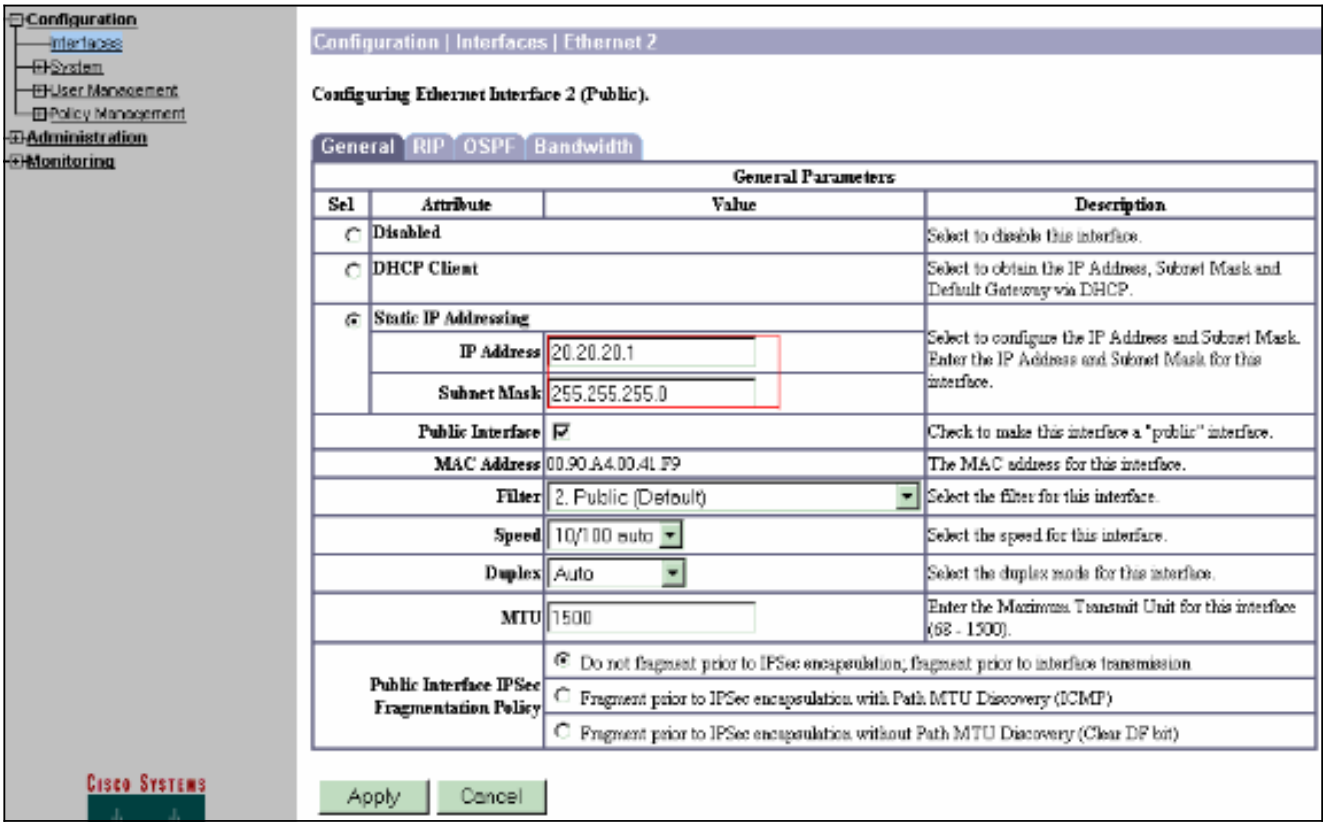
- **Date/heure – Il est très important que la bonne date et la bonne heure soient programmées.** Elles permettent l'exactitude des entrées de journalisation et de gestion des comptes et la création par le système d'un certificat de sécurité valide.
- **Interface Ethernet 1 (privée) : L'adresse IP et 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 configuration rapide au moyen de l'interface CLI.

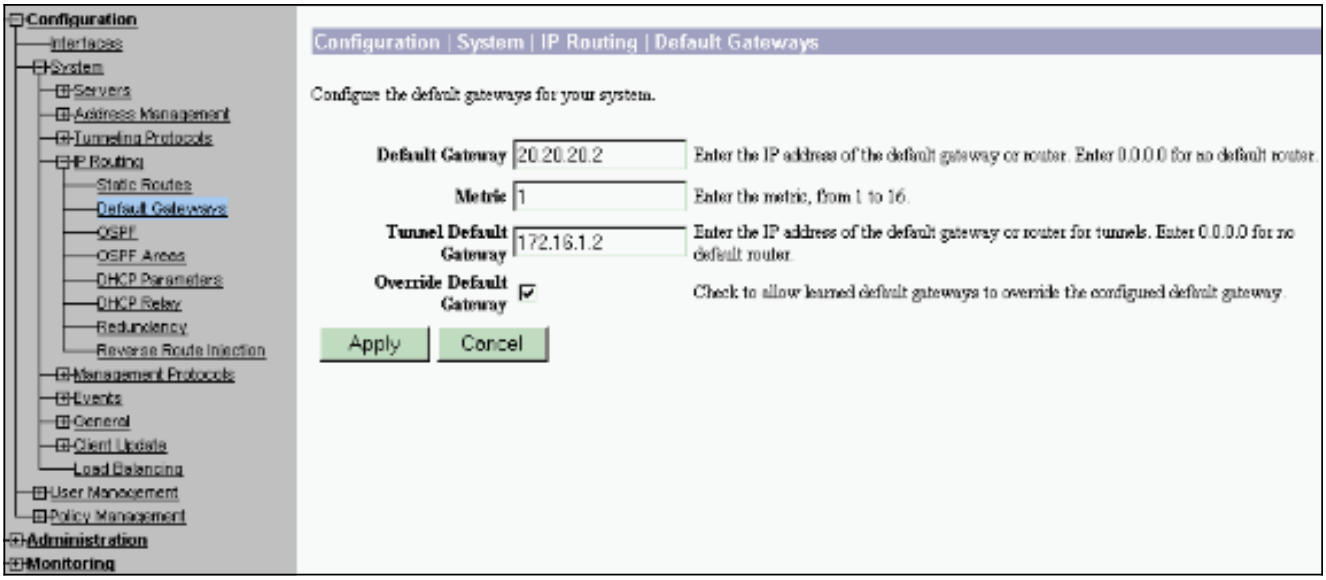
1. Entrez l'adresse IP de l'interface privée à partir du navigateur Web pour activer l'interface GUI.Cliquez sur l'icône **save needed [enregistrement nécessaire] pour enregistrer les modifications apportées à la mémoire.** La valeur d'usine par défaut attribuée au nom d'utilisateur et au mot de passe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



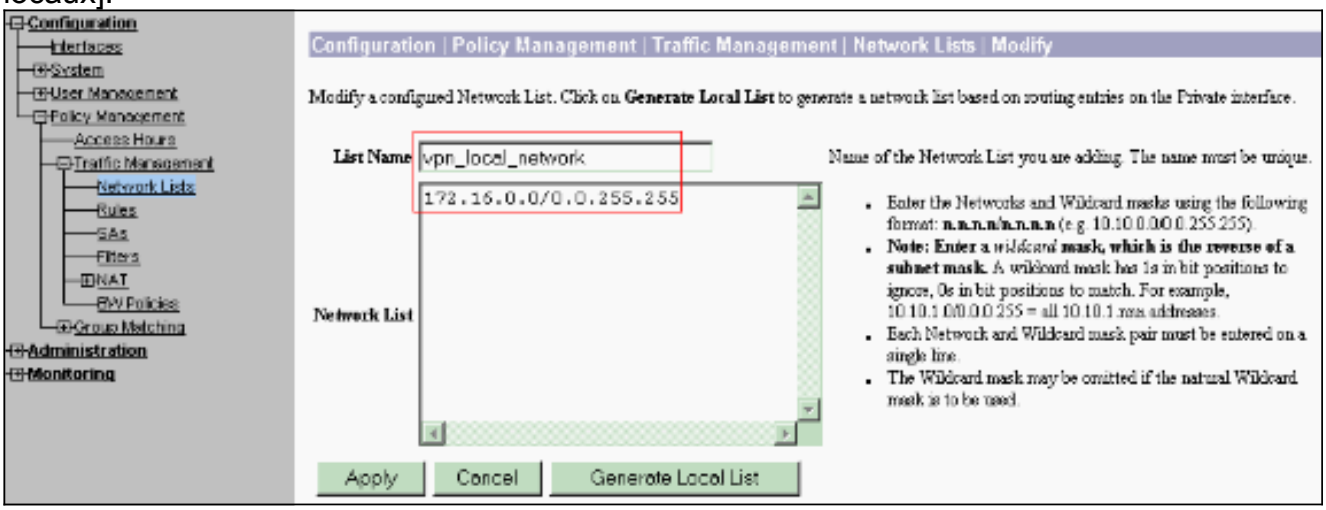
2. Lorsque l'interface GUI est activée, sélectionnez **Configuration > Interfaces > Ethernet 2 (Public) [configuration > interfaces > Ethernet 2 (public)] pour configurer l'interface Ethernet 2.**



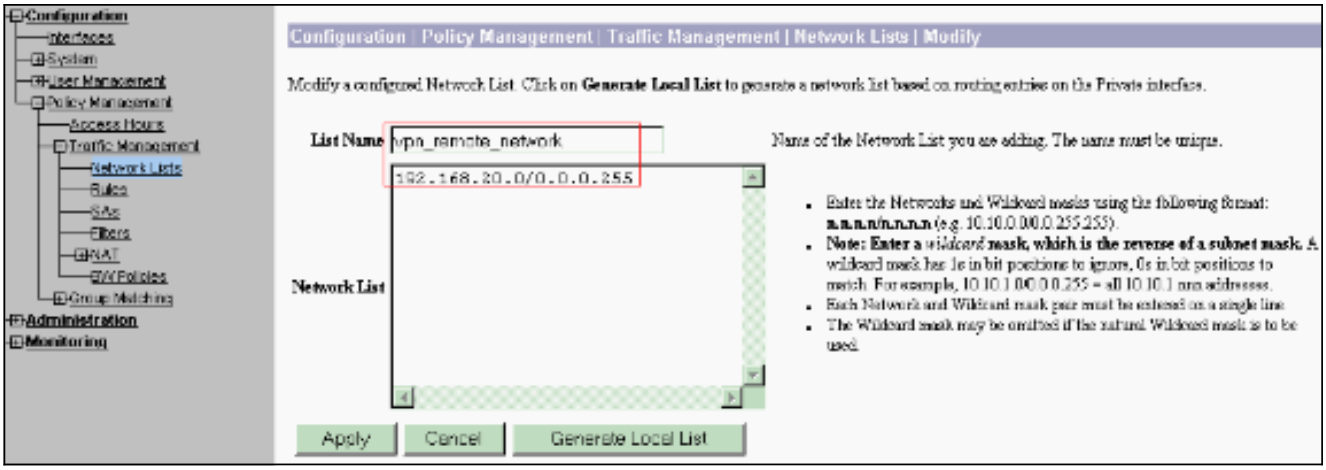
3. Allez à **Configuration > System > IP Routing > Default Gateways [configuration > système > routage IP > passerelles par défaut] pour configurer la passerelle par défaut (Internet) ainsi que la passerelle par défaut du tunnel (interne) pour qu'IPSec atteigne les autres sous-réseaux du réseau privé.**Dans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



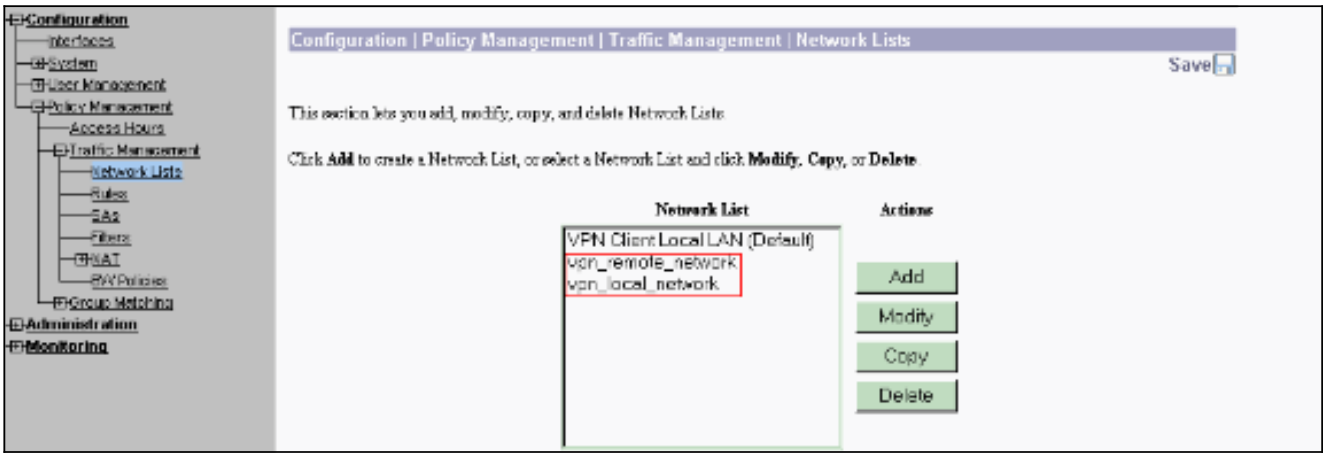
4. Allez à **Configuration > Policy Management > Traffic Management > Network Lists > Add [configuration > gestion des politiques > gestion du trafic > listes des réseaux > ajouter] pour créer les listes des réseaux précisant le trafic à chiffrer.**Les réseaux figurant dans la liste sont accessibles 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].



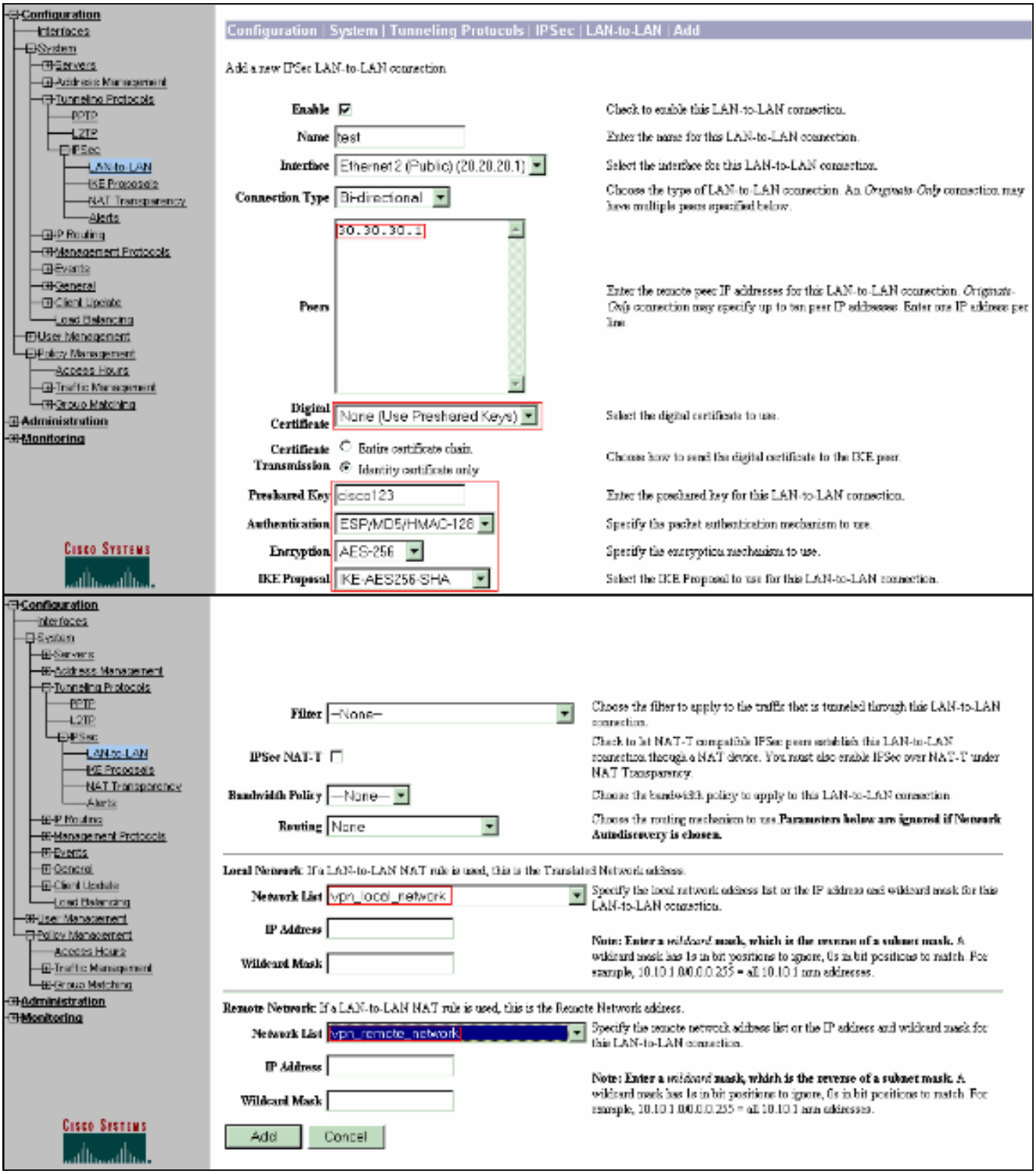
5. Les réseaux mentionnés dans cette liste sont des réseaux distants, qui doivent être configurés manuellement. Pour ce faire, saisissez le réseau ou le caractère générique de chaque sous-réseau
accessible.



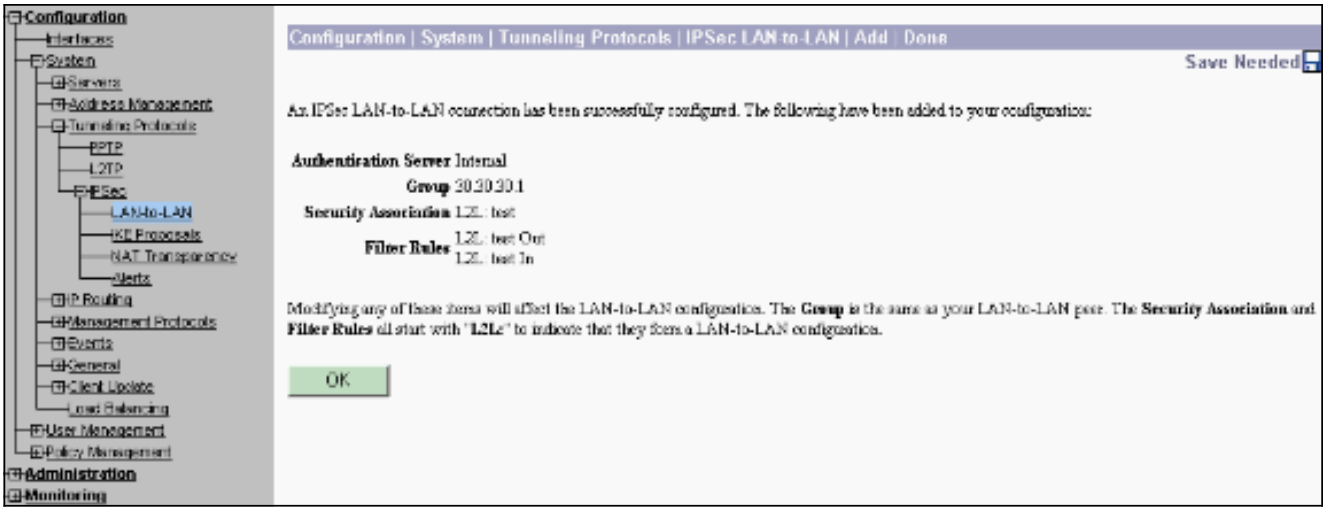
Ensuite, notez les deux listes de réseaux :



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.

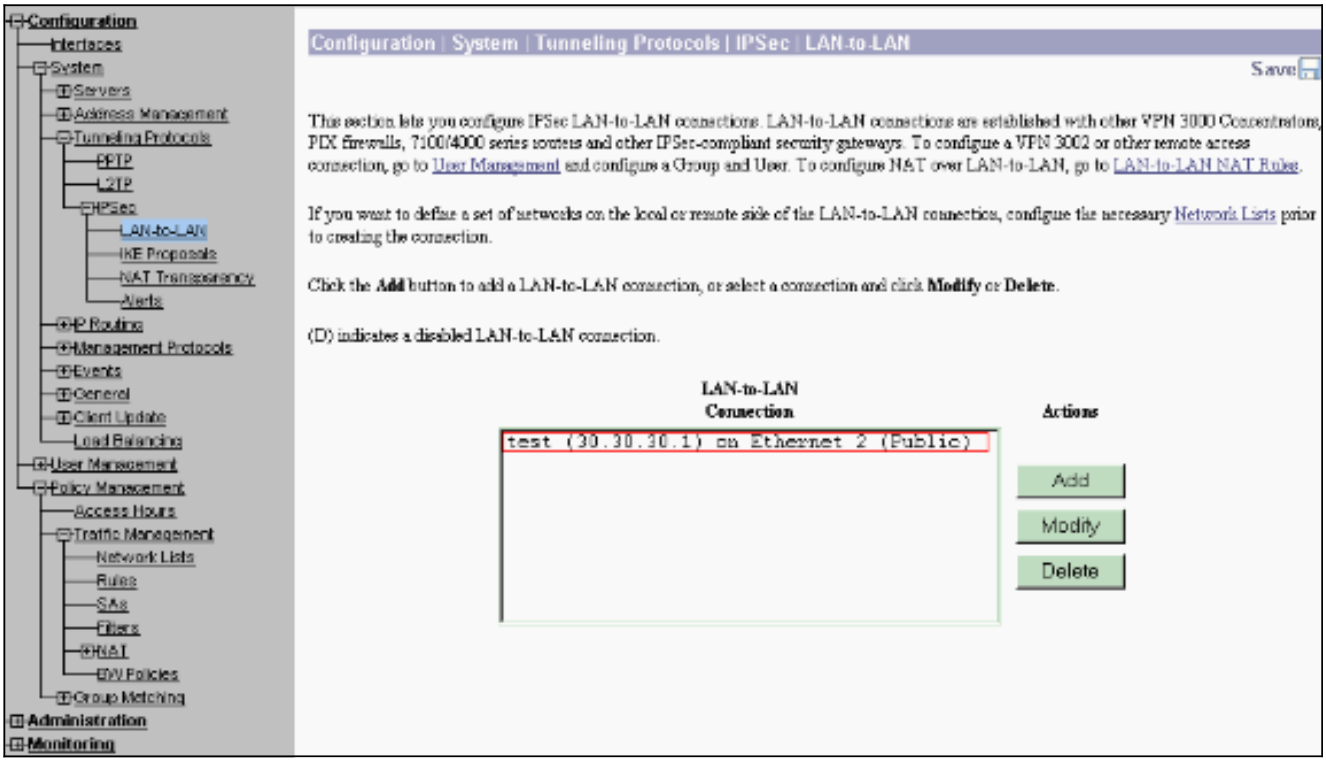


7. Après avoir cliqué sur Add [ajouter], vous verrez apparaître, si votre connexion est bonne, la fenêtre « IPSec LAN-to-LAN-Add-Done » [IPSec LAN à LAN–ajouté].Cette fenêtre montre un résumé des informations sur la configuration du tunnel. De plus, la configuration du nom de groupe, du nom du SA et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

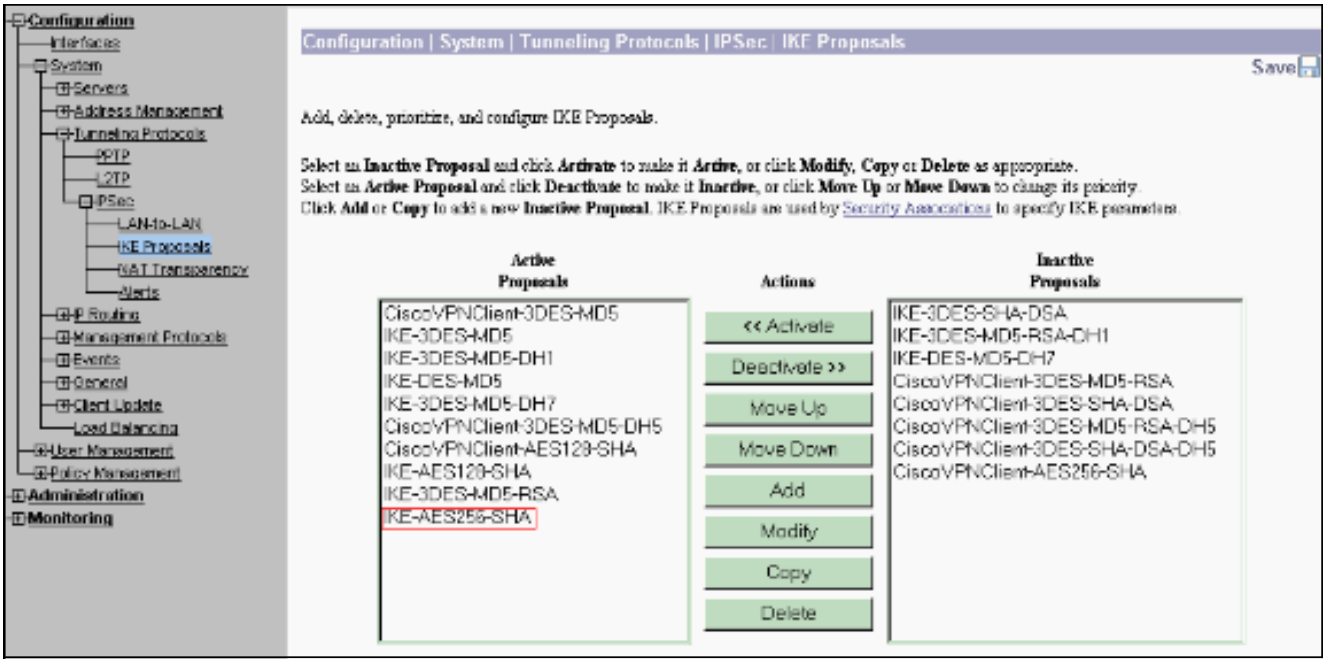


Àce stade, le tunnel IPSec LAN à LAN a été configuré, et vous pouvez commencer à travailler. Si, pour une raison ou une autre, le tunnel ne fonctionne pas, vous pouvez vérifier si la configuration contient des erreurs.

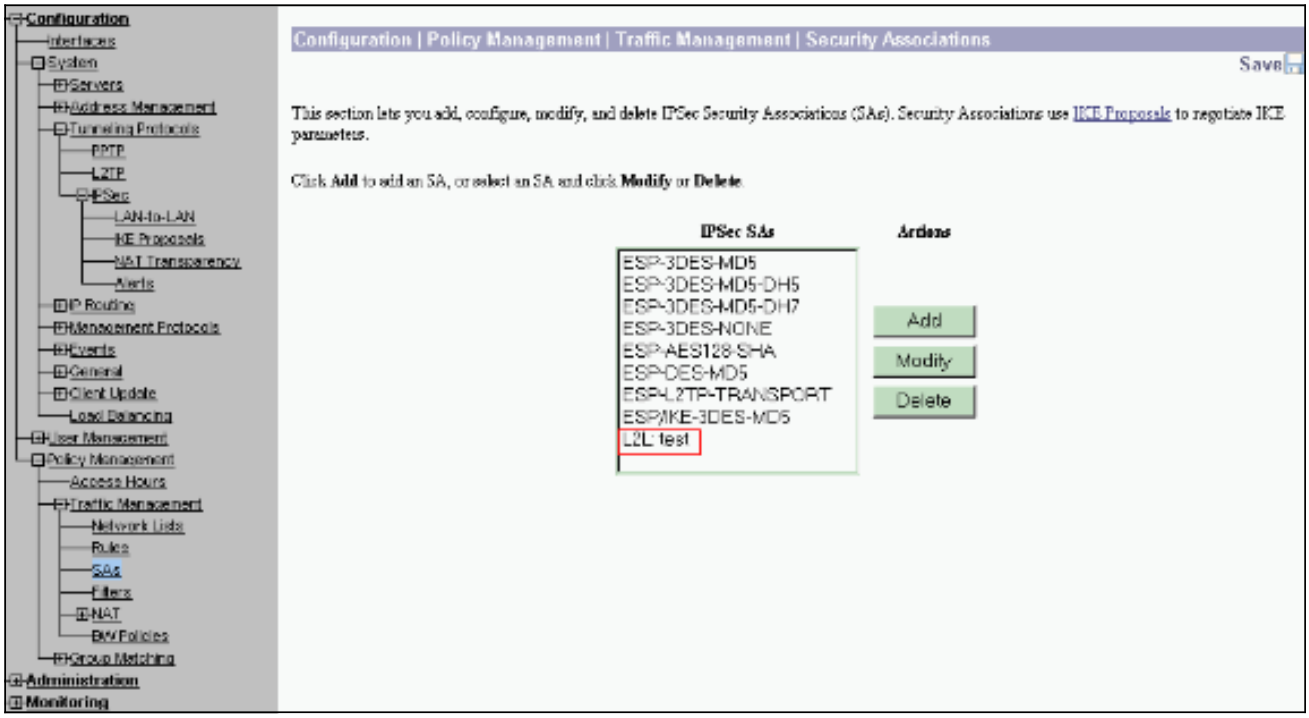
8. Vous pouvez afficher ou modifier les paramètres IPSec LAN à LAN créés précédemment lorsque vous sélectionnez **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** [configuration > système > protocoles de tunnellisation > IPSec LAN à LAN].L'illustration indique « test » comme nom de tunnel,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



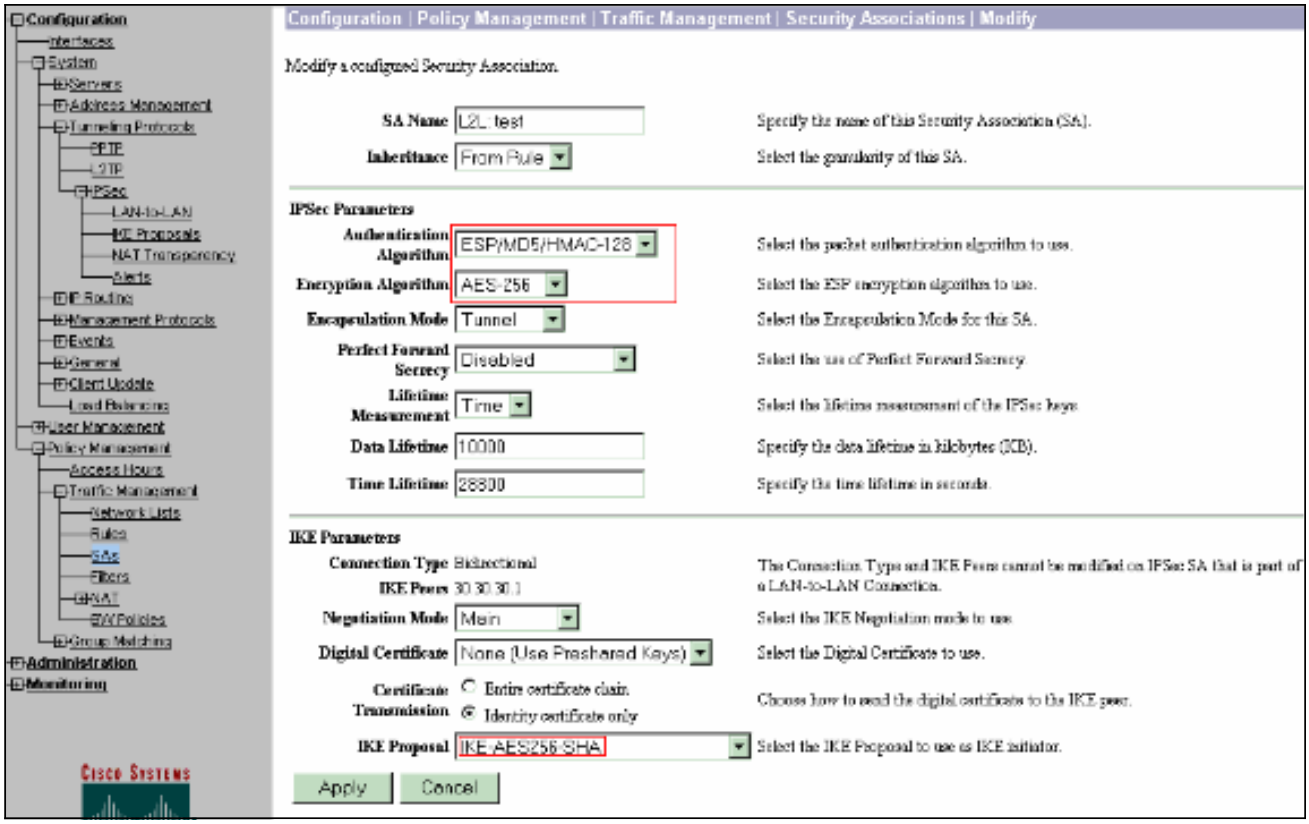
9. Il peut arriver que votre tunnel ne soit pas activé si votre proposition IKE figure dans la liste des propositions inactives. Sélectionnez **Configuration > System > Tunneling Protocols> IPSec > IKE Proposals [configuration > système > protocoles de tunnellisation > IPSec > propositions IKE] pour 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.



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.



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.



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'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 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

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:

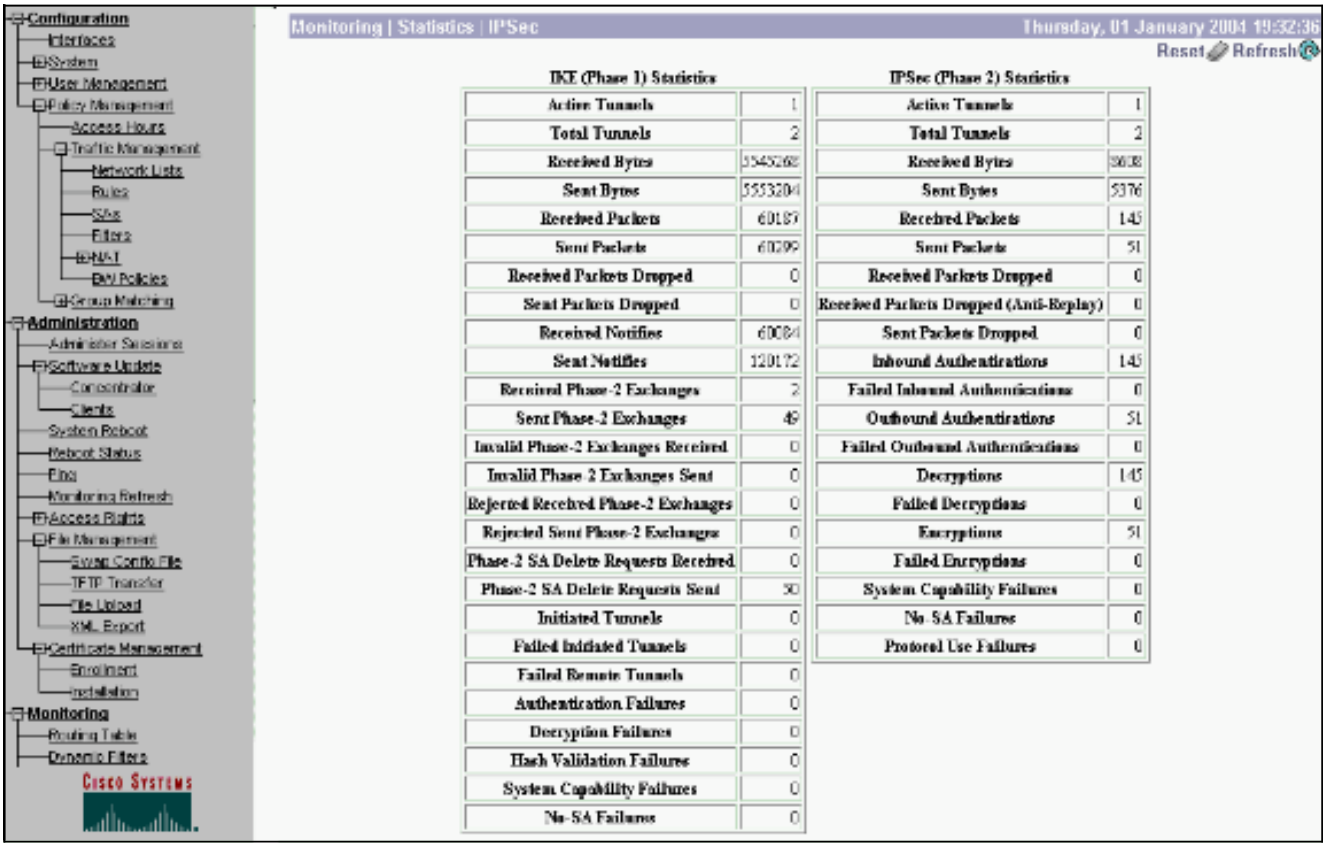
- **show crypto engine connections active : Cette commande affiche les connexions de session chiffrées qui sont actuellement actives pour tous les moteurs de chiffrement.** Chaque ID de connexion est unique. Le nombre de paquets chiffrés et déchiffrés est affiché dans les deux dernières colonnes.

```
ipsec_router#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
```

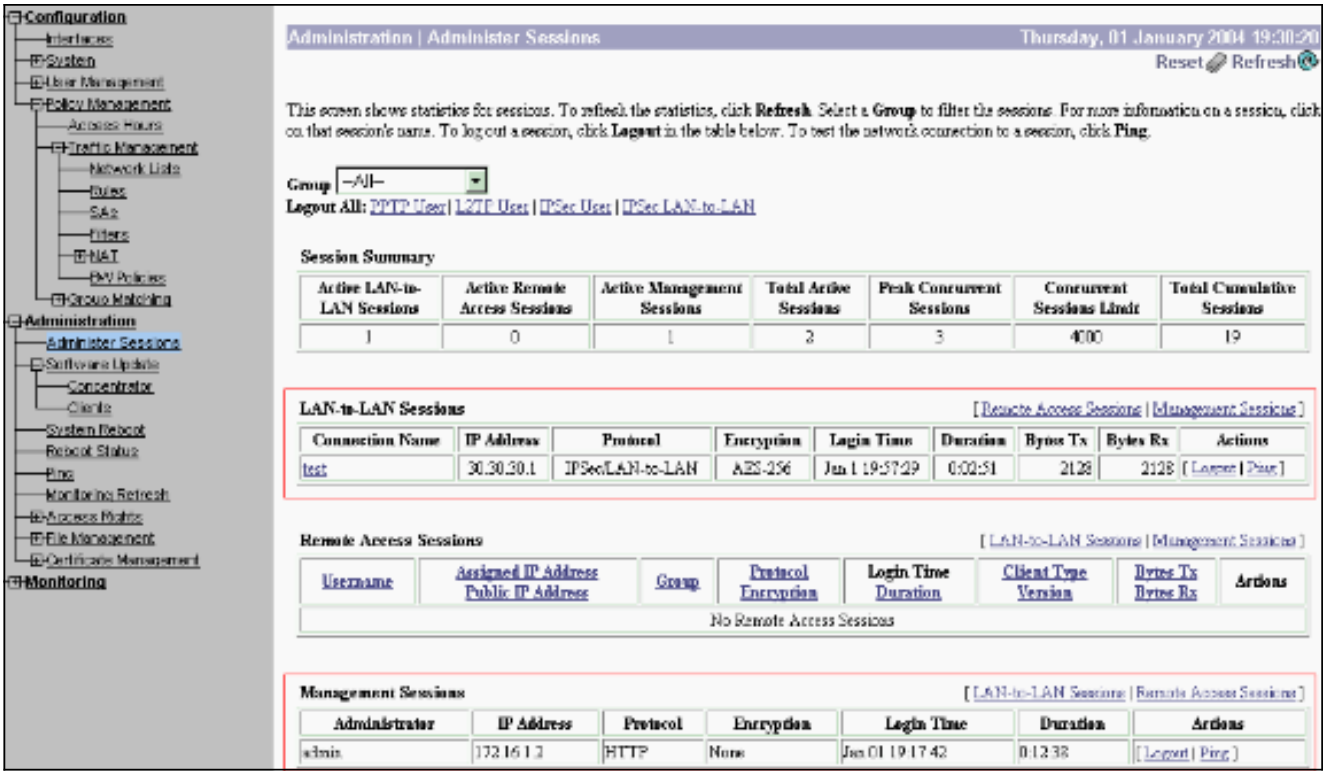
Vérifiez la configuration du concentrateur VPN

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

1. 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.**



2. 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.**



Dépannage

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 : Consulter les renseignements importants sur les commandes de débogage 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.**

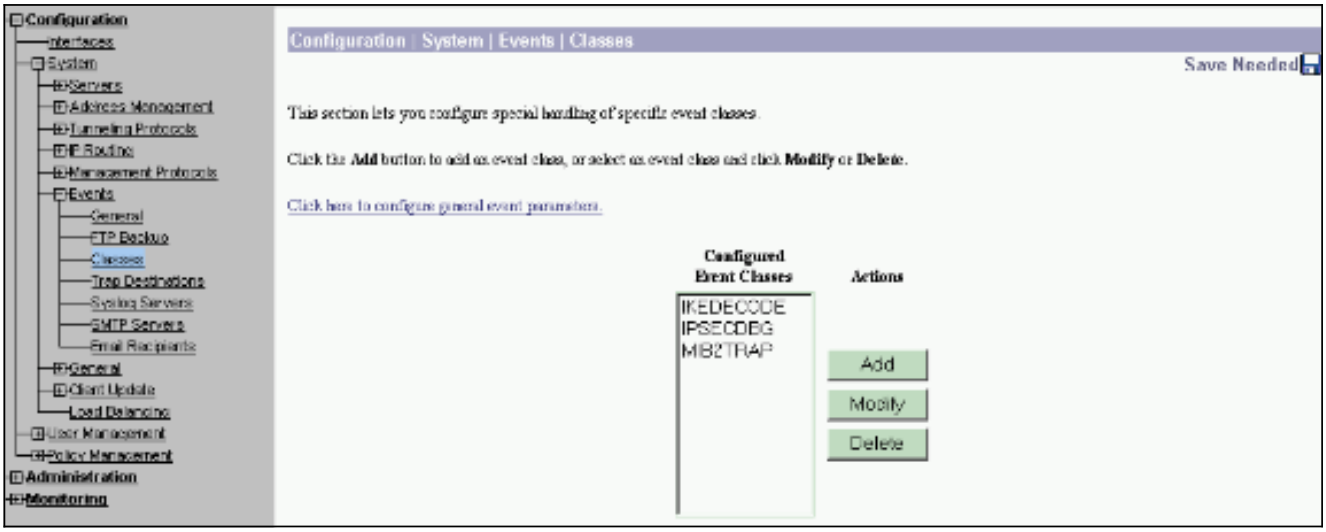
Consultez la section sur le dépannage d'IPSec portant sur les connaissances et l'utilisation **des commandes de débogage pour obtenir des informations détaillées sur le sujet et des exemples de résultats.**

Dépannage du concentrateur VPN

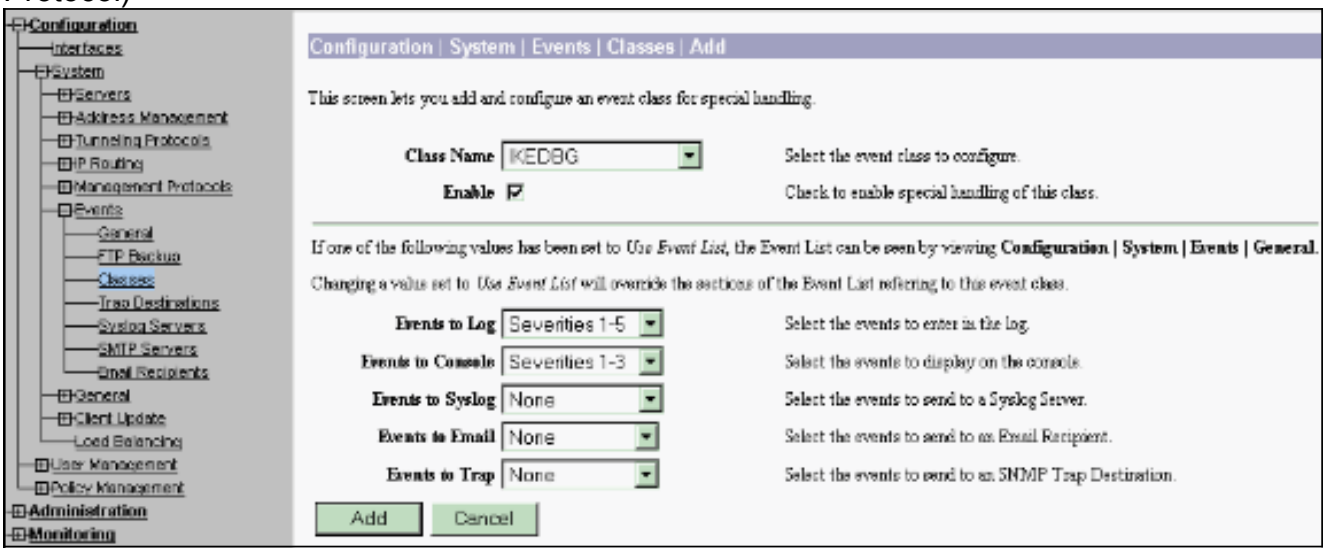
Àl'instar des commandes de **débogage des routeurs Cisco, vous pouvez configurer des classes d'événements pour afficher les alarmes.**

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

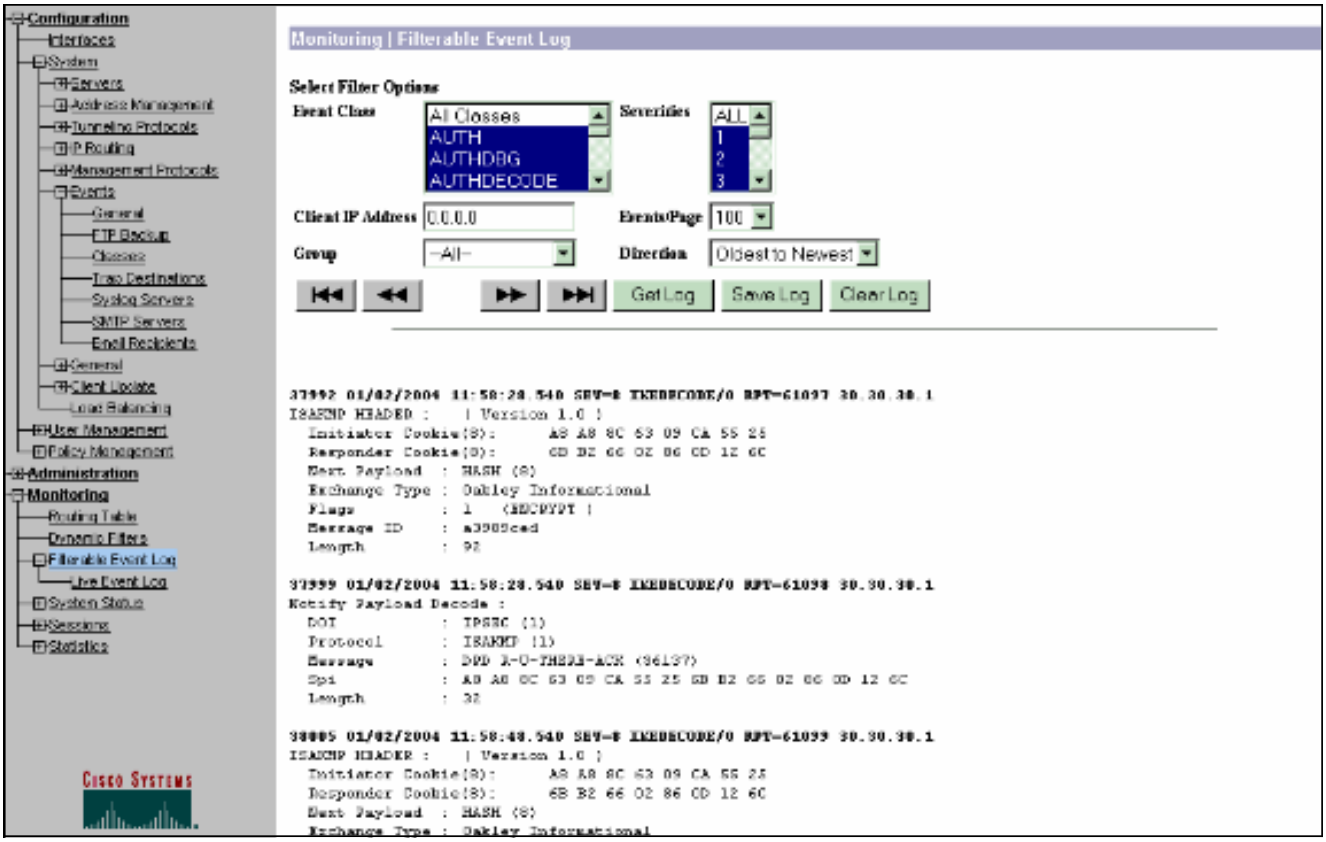
classes sont possibles pour
IPsec :IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



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)



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



Informations connexes

- Standard de cryptage avancé (AES)
- 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.