PIX/ASA 7.x et versions ultérieures : Exemple de configuration d'un tunnel VPN PIX à PIX

Contenu

Introduction

Ce document décrit la procédure pour configurer des tunnels VPN entre deux pare-feux PIX utilisant Cisco Adaptive Security Device Manager (ASDM). ASDM est un outil de configuration basé sur l'application conçu pour vous aider à installer, configurer et contrôler votre pare-feu PIX avec une interface graphique. Les pare-feux PIX sont placés à deux endroits différents.

Un tunnel est formé utilisant IPsec. IPSec est une combinaison de normes ouvertes qui fournissent la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données entre des homologues IPSec.

Remarque: Dans PIX version 7,1 et ultérieures, la commande **sysopt connection permit-ipsec** est modifiée en **sysopt connection permit-vpn**. Cette commande autorise le trafic de routage qui entre dans l'appliance de sécurité par un tunnel VPN et est ensuite déchiffré, pour contourner les listes d'accès de l'interface. Les statégies de groupe et les listes d'accès d'autorisation par utilisateur s'appliquent toujours au trafic. Pour désactiver cette fonctionnalité, n'utilisez la forme **no** de cette commande. Cette commande n'est pas visible dans la configuration CLI.

Consultez PIX 6.x : Exemple de configuration simple de tunnel VPN PIX- -PIX pour en savoir plus

sur le même scénario lorsque l'appliance de sécurité Cisco PIX exécute la version 6.x du logiciel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document spécifient que cet homologue lance le premier échange de propriété afin de déterminer l'homologue approprié auquel se connecter.

- Appliance de sécurité de la gamme Cisco PIX 500 avec version 7.x et ultérieures
- ASDM version 5.x et ultérieures

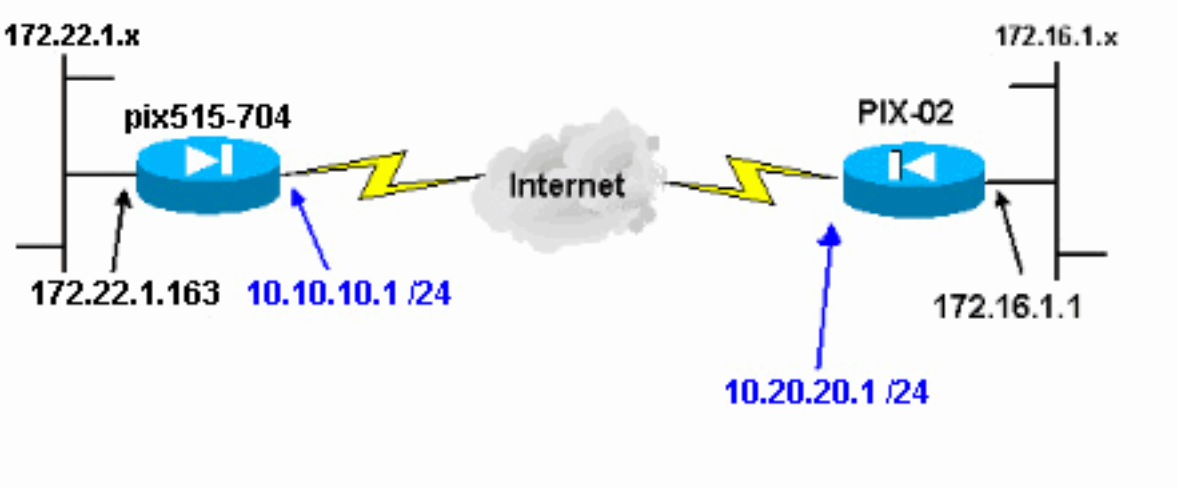
Remarque: Référez-vous à Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré par l'ASDM.

Remarque: La version 7.x/8.x de la gamme ASA 5500 exécute le même logiciel que dans la version PIX 7.x/8.x. Les configurations présentées dans ce document s'appliquent aux deux gammes de produits.

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

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

Informations générales

La négociation IPSec peut être décomposée en cinq étapes et inclut deux phases d'échange de clés Internet (IKE).

1. Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré intéressant quand il voyage entre les pairs d'IPsec.
2. Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois que les homologues sont authentifiés, un tunnel sécurisé est créé en utilisant Internet Security Association and Key Management Protocol (ISAKMP).
3. Dans la phase 2 d'IKE, les homologues IPSec utilisent le tunnel authentifié et sécurisé pour négocier des transformations d'association de sécurité IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.
4. Le tunnel d'IPsec est créé et des données sont transférées entre les pairs d'IPsec basés sur les paramètres d'IPsec configurés dans les jeux de transformations d'IPsec.
5. Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.**Remarque:** La négociation IPSec entre les deux PIX échoue si les associations de sécurité sur les deux phases d'IKE ne correspondent pas sur les homologues.

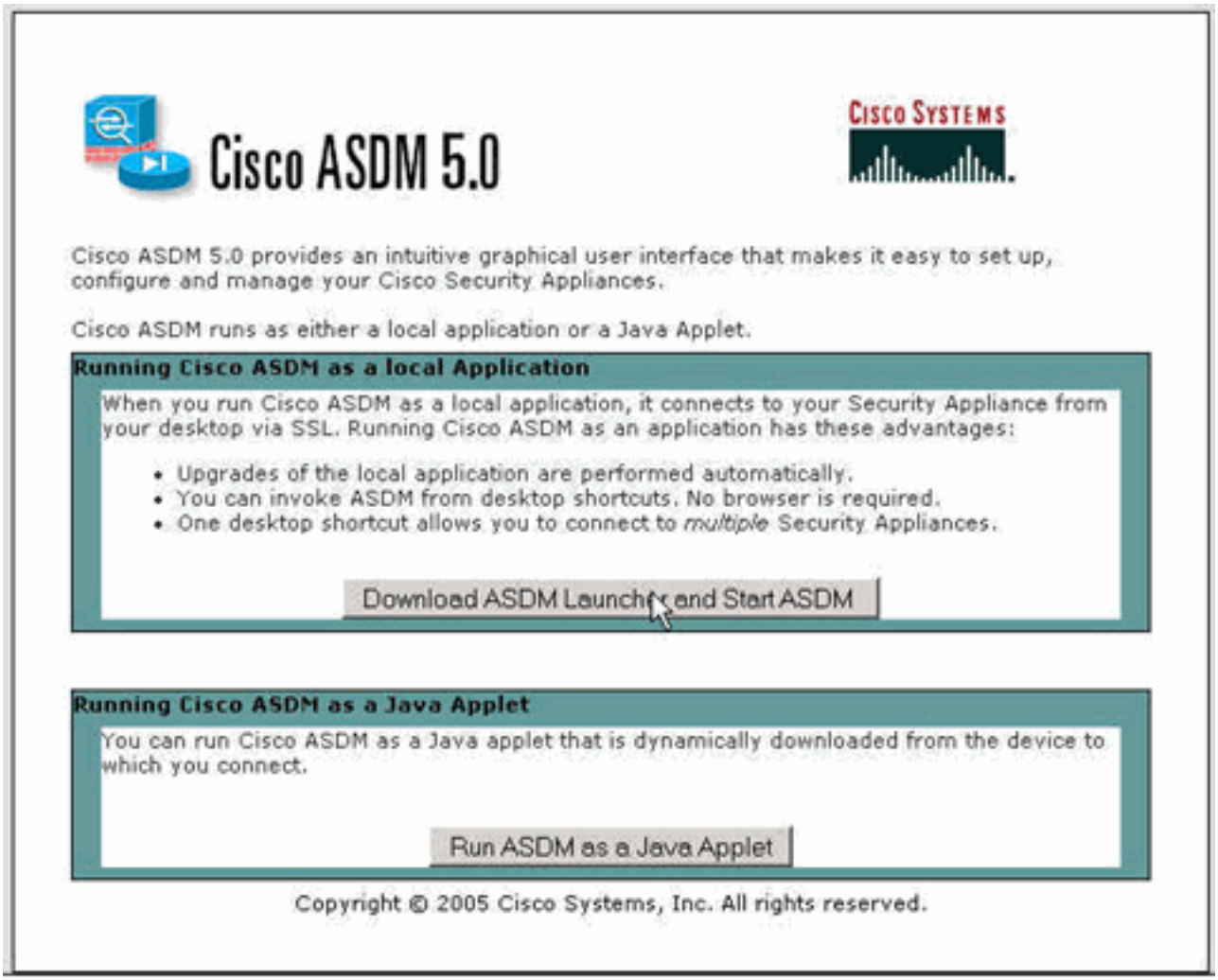
Configuration

- Configuration ASDM
- Configurations CLI PIX

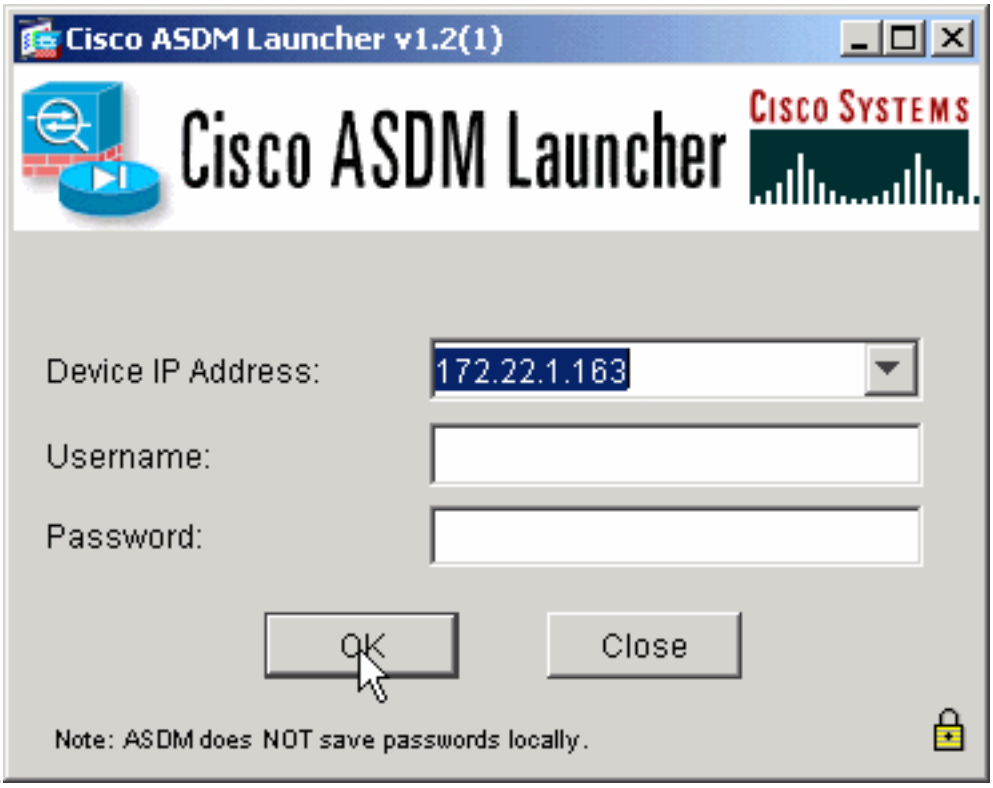
Configuration ASDM

Procédez comme suit :

1. Ouvrez votre navigateur et saisissez **https://<Inside_IP_Address_of_PIX>** pour accéder à l'ASDM sur le PIX.Assurez-vous d'autoriser tous les avertissements que votre navigateur vous donne en ce qui concerne l'authenticité de certificat SSL. Le nom d'utilisateur par défaut et le mot de passe sont tous deux vides.Le PIX présente cette fenêtre pour permettre le téléchargement de l'application ASDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet
   Java.

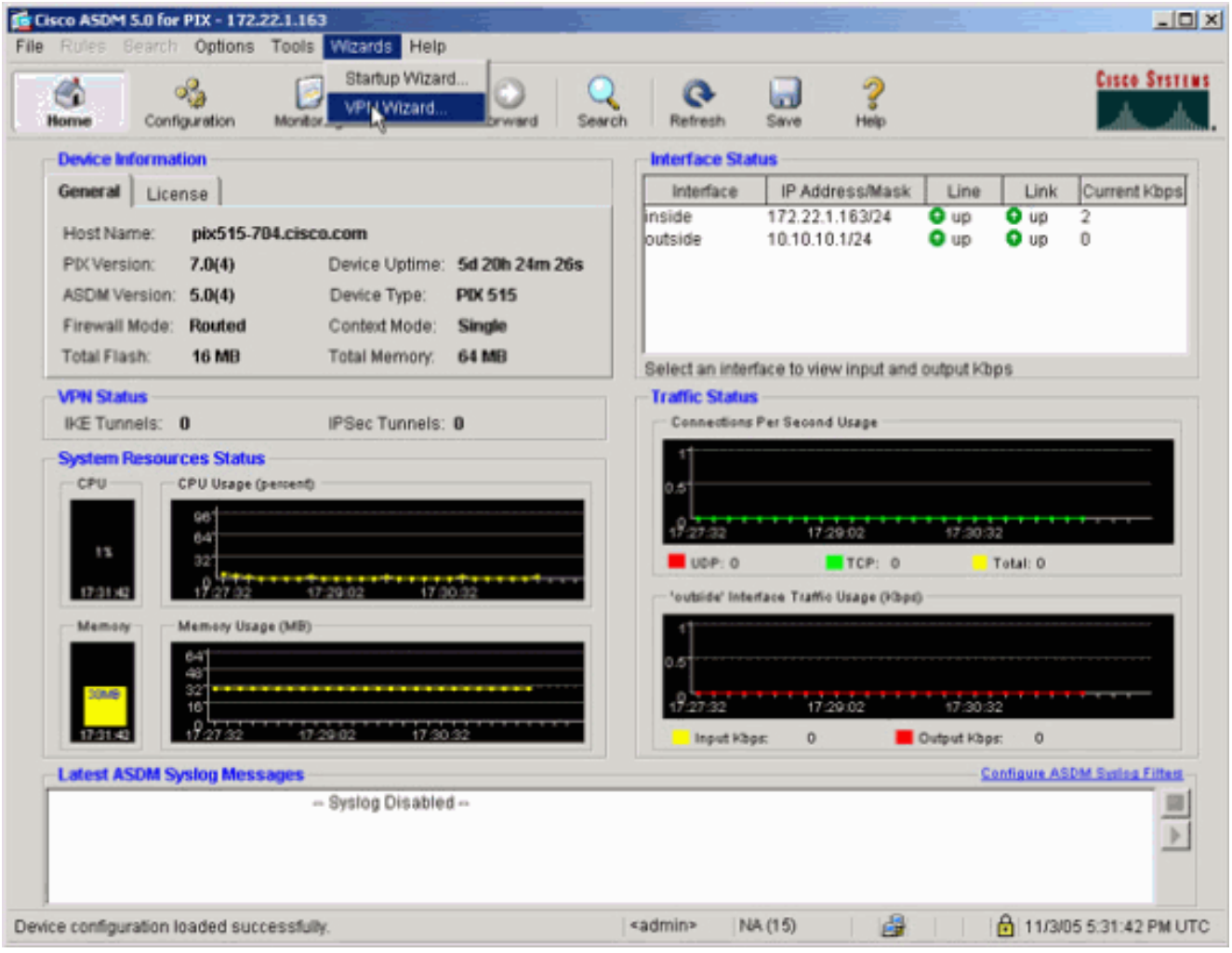


2. Cliquez sur le **Download ASDM Launcher and Start ASDM** pour télécharger l'installateur pour l'application ASDM.
3. Une fois que l'installateur ASDM est téléchargé, suivez les invites afin d'installer le logiciel et exécuter l'installateur Cisco ASDM.
4. Entrez l'adresse IP pour l'interface que vous avez configurée avec la commande **http -** et un nom d'utilisateur et mot de passe, le cas échéant.Cet exemple n'utilise pas de nom d'utilisateur ni de mot de passe (configuration par

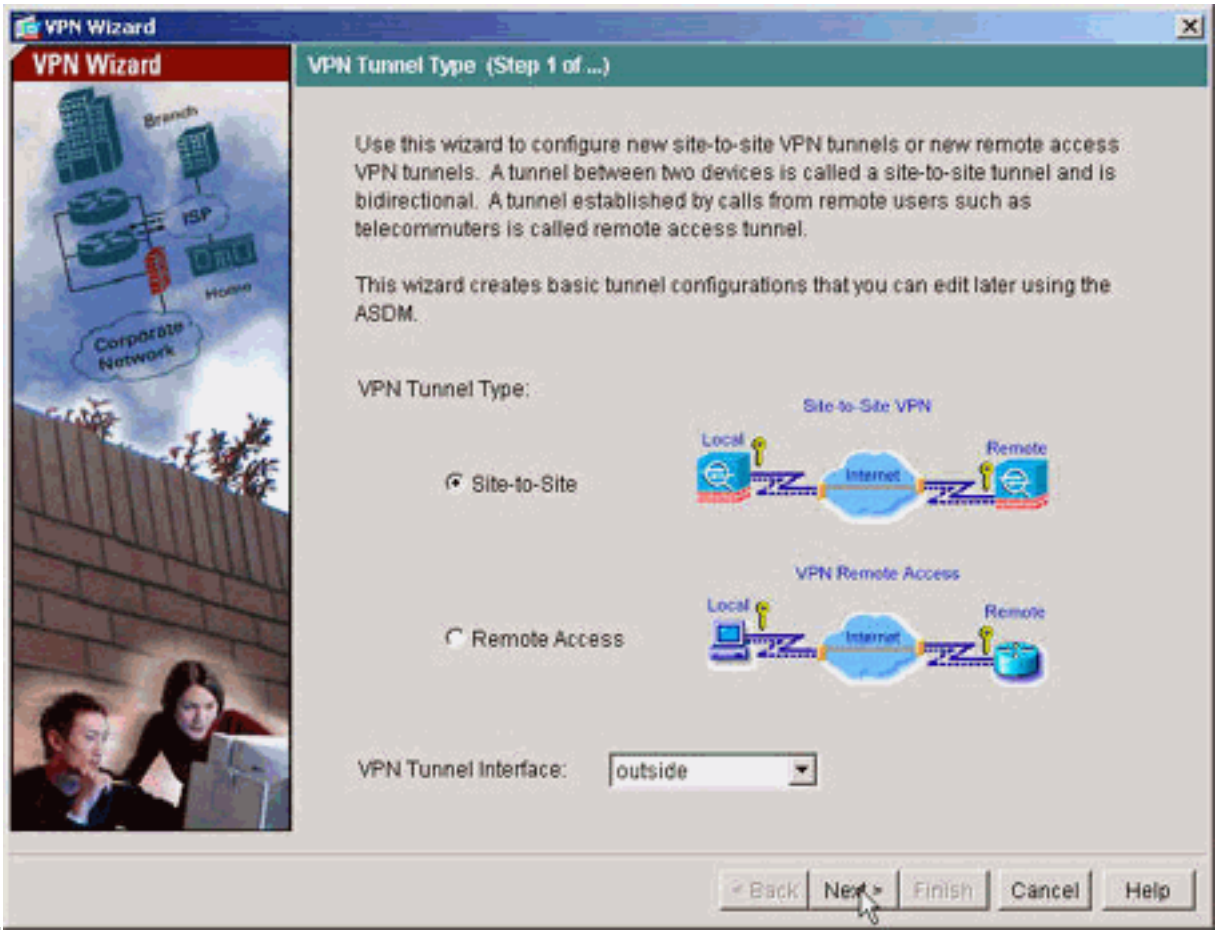


défaut).

5. Exécutez l'assistant VPN une fois que l'application ASDM se connecte au PIX.

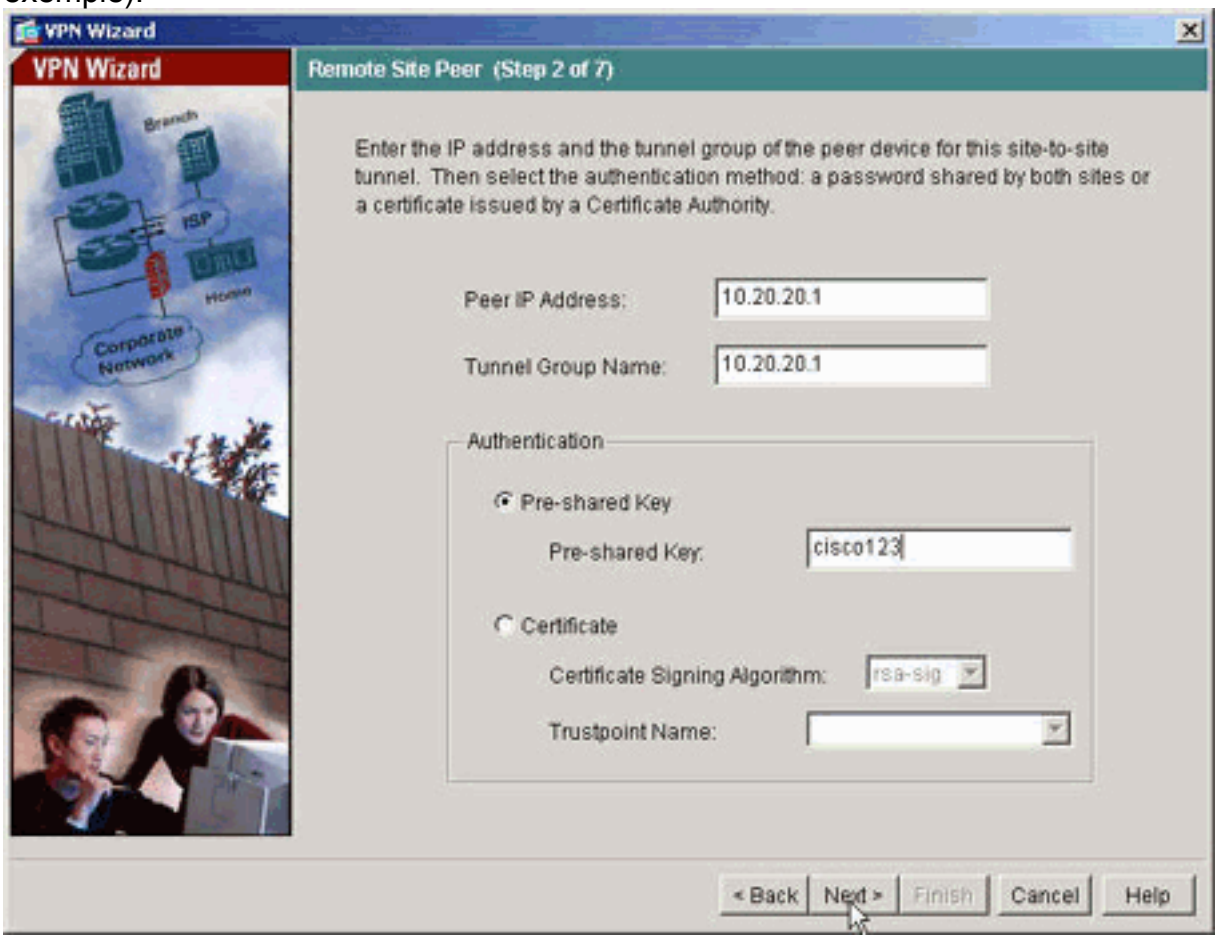


6. Choisissez le type de tunnel VPN **site à**



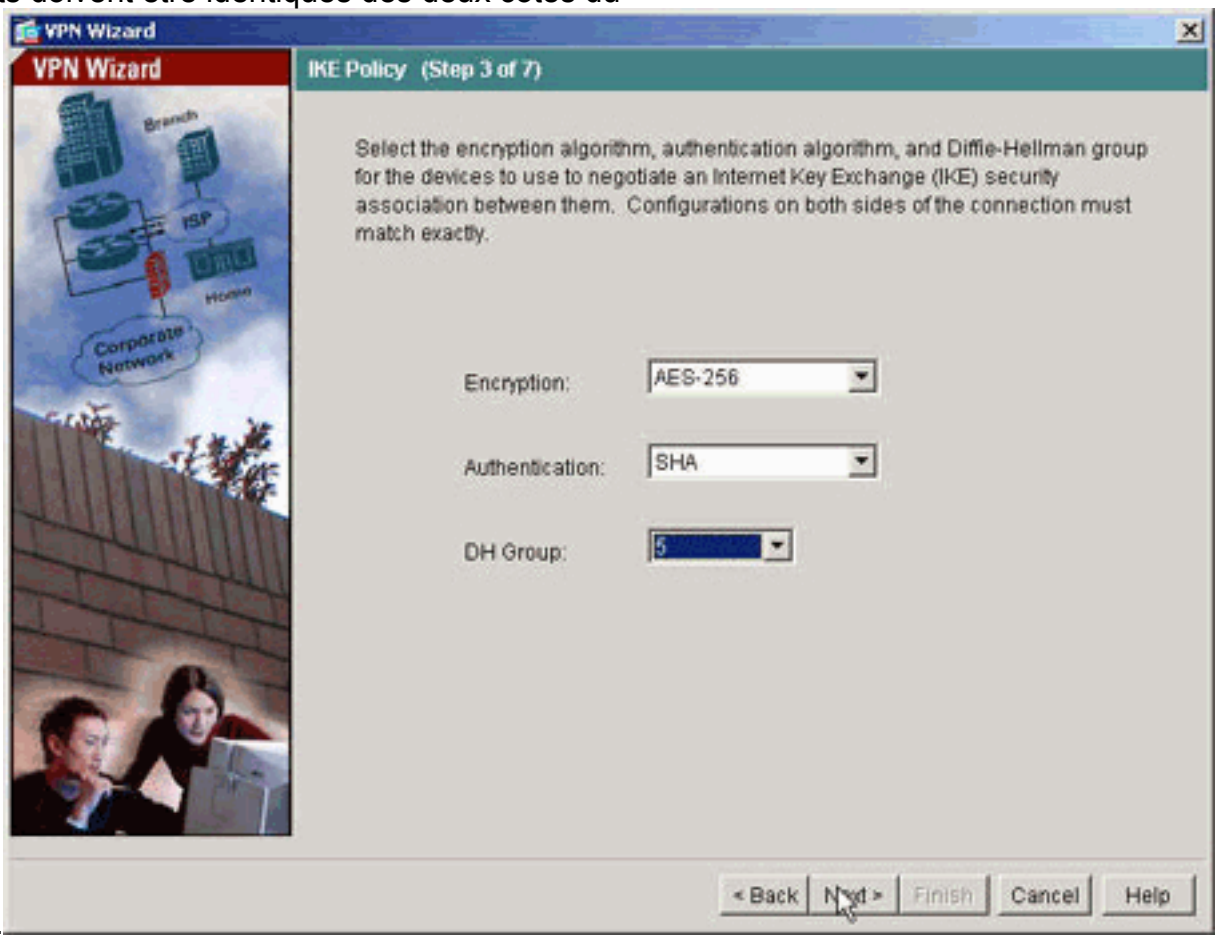
site.

7. Spécifiez l'adresse IP externe du partenaire distant. Entrez les informations d'authentification à utiliser (clé pré-partagée dans cet exemple).

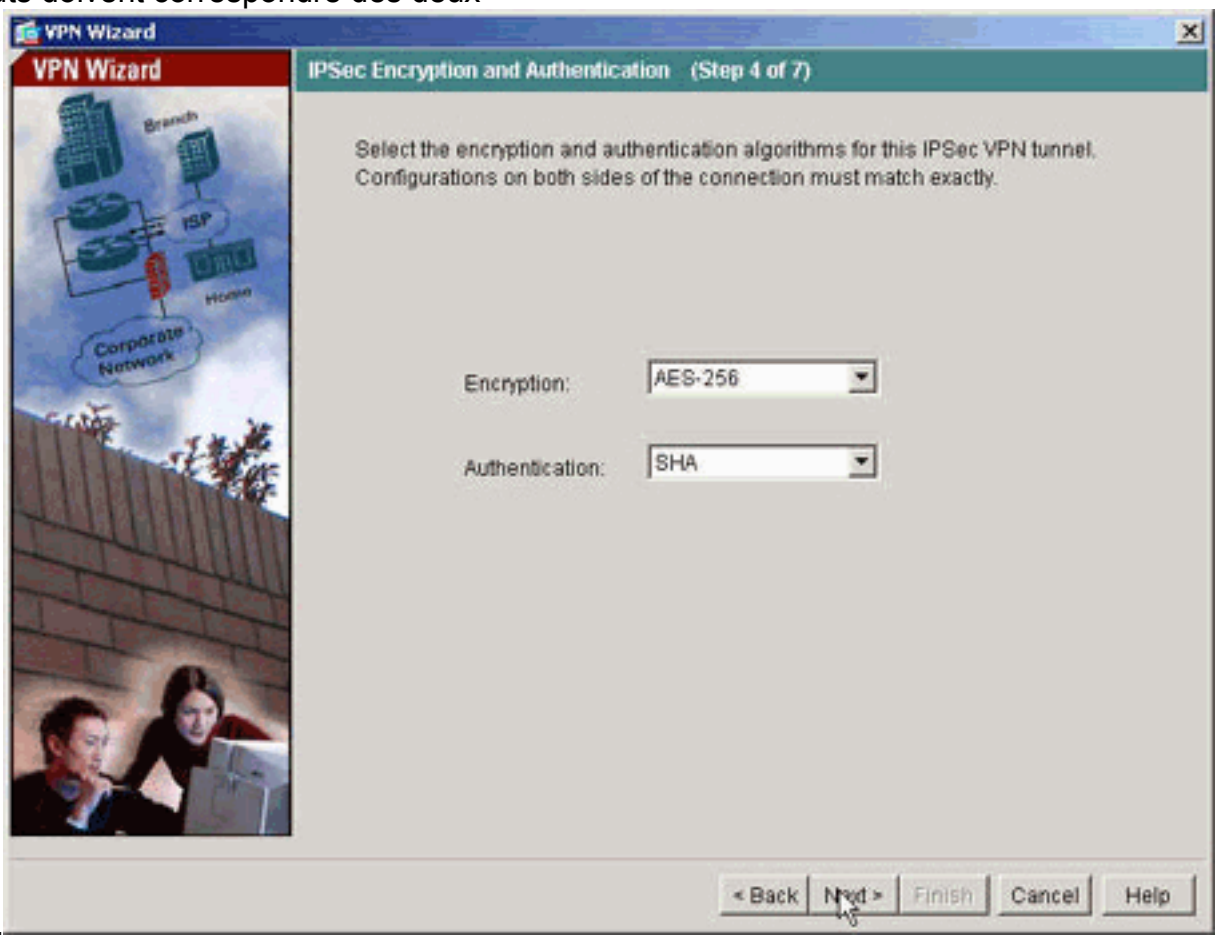


8. Spécifiez les attributs à utiliser pour l'IKE, également connus en tant que « Phase 1 ». Ces

attributs doivent être identiques des deux côtés du tunnel.

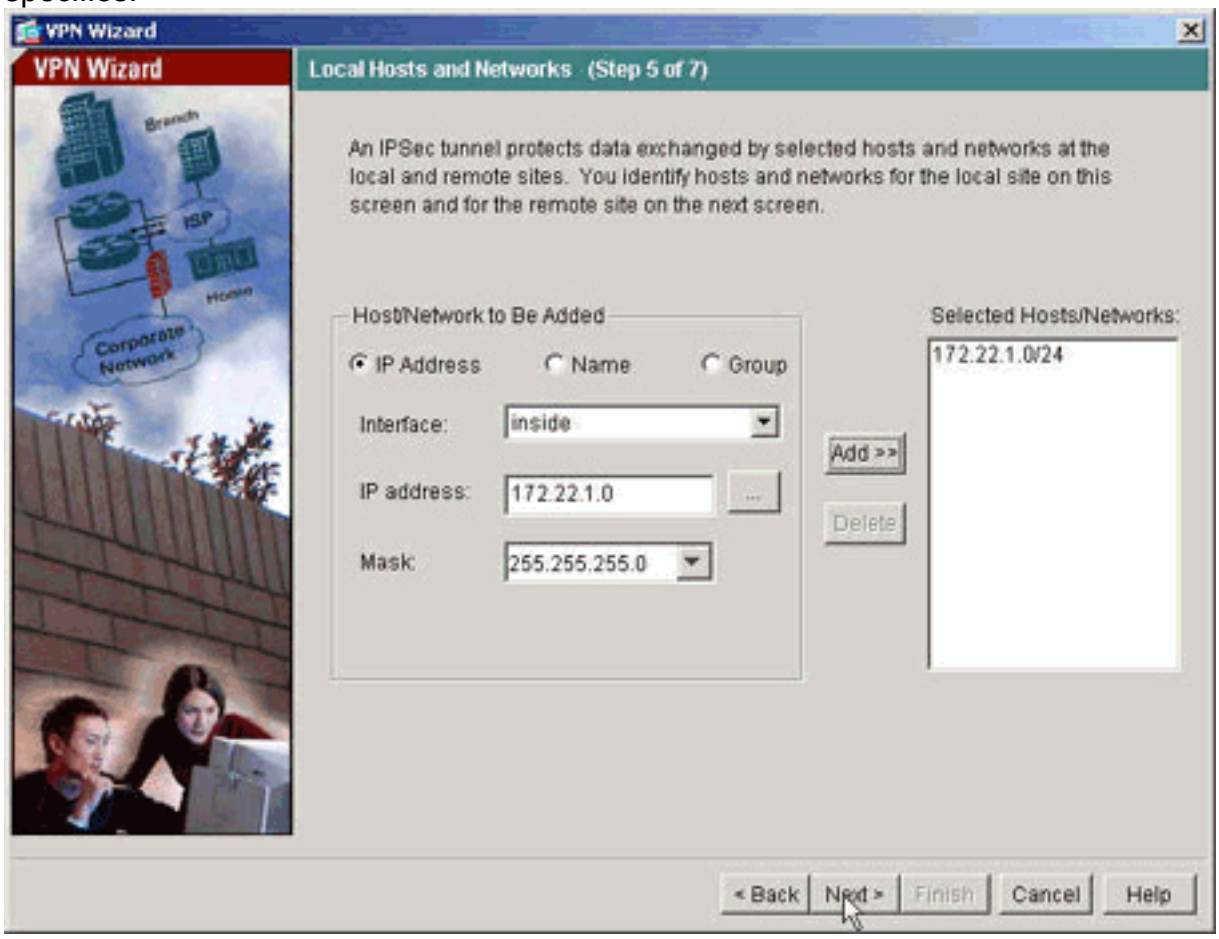


9. Spécifiez les attributs à utiliser pour IPsec, également connus en tant que « Phase 2 ». Ces attributs doivent correspondre des deux côtés.

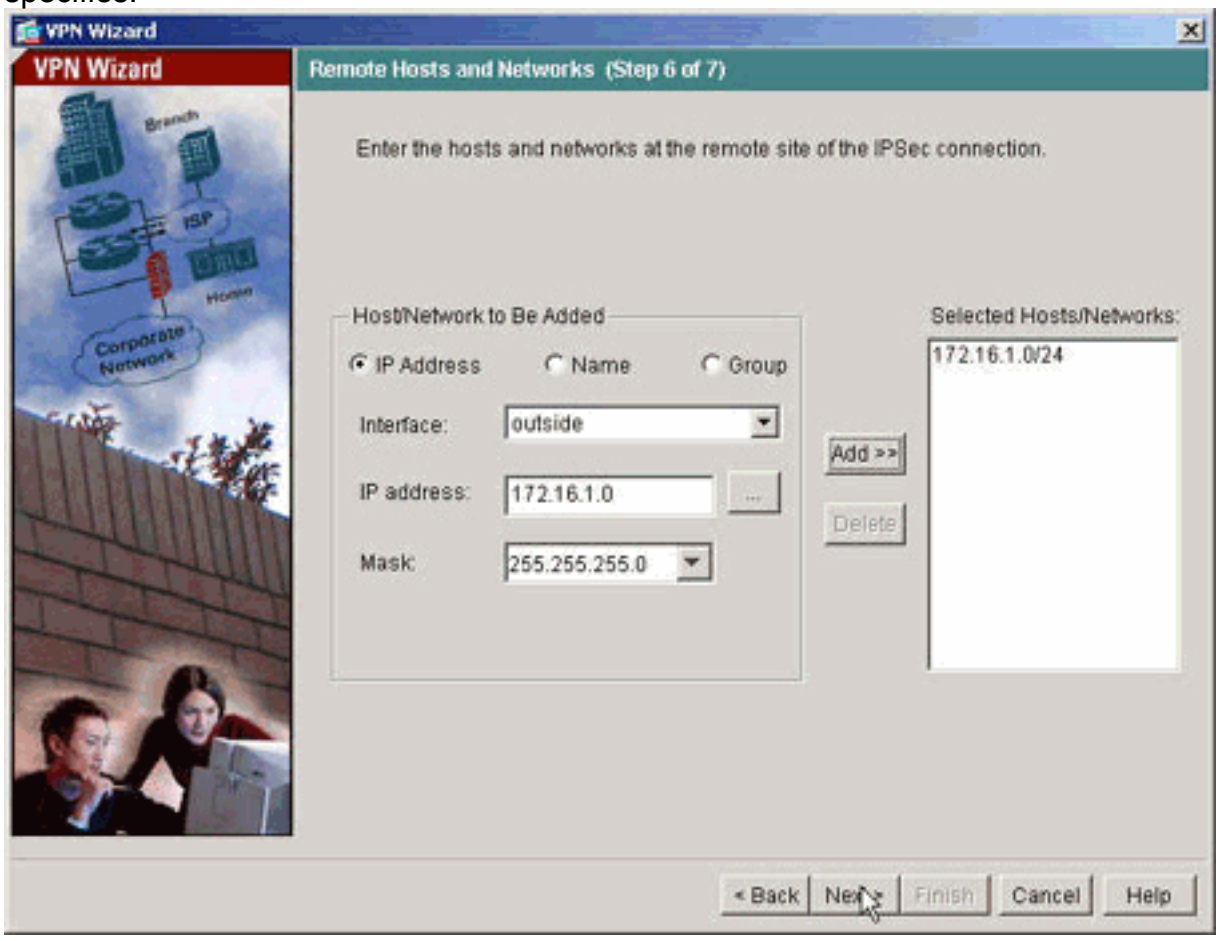


10. Spécifiez les hôtes dont le trafic devrait être autorisé à passer par le tunnel VPN. Dans

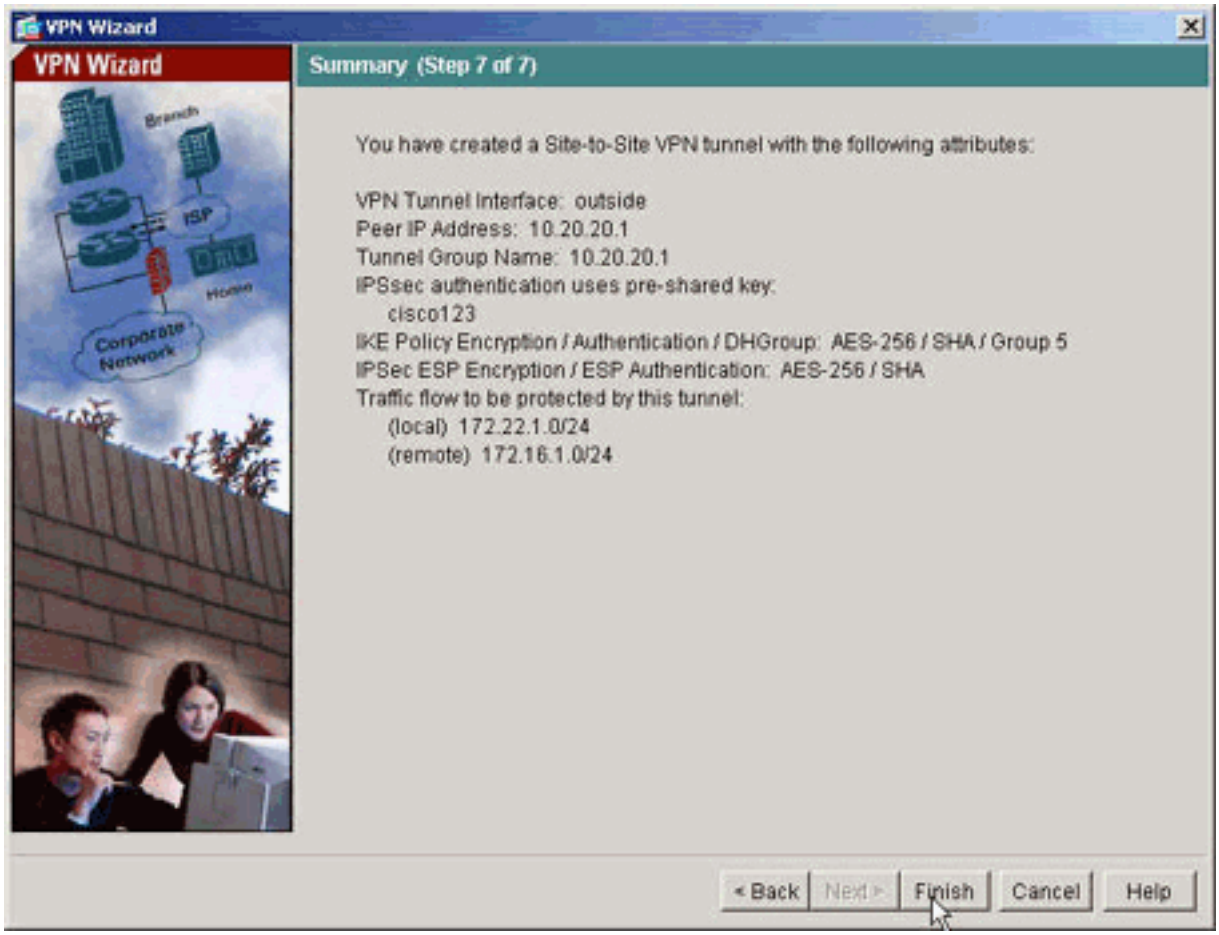
cette étape, les hôtes locaux à pix515-704 sont spécifiés.



11. Les hôtes et les réseaux du côté distant du tunnel sont spécifiés.



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



Configuration CLI PIX

pix515-704

```
pixfirewall#show run : Saved PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 ip
address 10.10.10.1 255.255.255.0 !--- Configure the
outside interface. ! interface Ethernet1 nameif inside
security-level 100 ip address 172.22.1.163 255.255.255.0
!--- Configure the inside interface. ! !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list inside_nat0_outbound
extended permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration. access-list outside_cryptomap_20 extended
permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
```

```
(outside_cryptomap_20) is used with the crypto map !--- outside_map to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside_nat0_outbound). !--- Two separate access lists should always be used in this configuration. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image flash:/asdm-511.bin !--- Enter this command to specify the location of the ASDM image. asdm history enable arp timeout 14400 nat (inside) 0 access-list inside_nat0_outbound !--- NAT 0 prevents NAT for networks specified in the ACL inside_nat0_outbound. route outside 0.0.0.0 0.0.0.0 10.10.10.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable !--- Enter this command in order to enable the HTTPS server for ASDM. http 172.22.1.1 255.255.255.255 inside !--- Identify the IP addresses from which the security appliance !--- accepts HTTPS connections. no snmp-server location no snmp-server contact !--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 20 match address outside_cryptomap_20 !--- Define which traffic should be sent to the IPsec peer. crypto map outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec peer crypto map outside_map 20 set transform-set ESP-AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-256-SHA" !--- to be used with the crypto map entry "outside_map". crypto map outside_map interface outside !--- Specifies the interface to be used with !--- the settings defined in this configuration. !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- Policy 65535 is included in the config by default. !--- The configuration commands here define the Phase !--- 1 policy parameters that are used. isakmp enable outside isakmp policy 10 authentication pre-share isakmp policy 10 encryption aes-256 isakmp policy 10 hash sha isakmp policy 10 group 5 isakmp policy 10 lifetime 86400 isakmp policy 65535 authentication pre-share isakmp policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp policy 65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-l2l !--- In order to create and manage the database of connection-specific records !--- for ipsec-l2l–IPsec (LAN-to-LAN) tunnels, use the tunnel-group !--- command in global configuration mode. !--- For L2L connections the name of the tunnel group MUST be the IP !--- address of the IPsec peer. tunnel-group 10.20.20.1 ipsec-attributes pre-shared-key * !--- Enter the pre-shared-key in order to configure the authentication method. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

PIX-02

```
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.20.20.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704. access-list
outside_cryptomap_20 extended permit ip 172.16.1.0
255.255.255.0 172 .22.1.0 255.255.255.0 !--- Note that
this ACL is a mirror of the outside_cryptomap_20 !---
ACL on pix515-704. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image flash:/asdm-511.bin
no asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
http server enable http 0.0.0.0 0.0.0.0 inside no snmp-
server location no snmp-server contact crypto ipsec
transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20 crypto map outside_map 20 set peer
10.10.10.1 crypto map outside_map 20 set transform-set
ESP-AES-256-SHA crypto map outside_map interface outside
isakmp enable outside isakmp policy 10 authentication
pre-share isakmp policy 10 encryption aes-256 isakmp
policy 10 hash sha isakmp policy 10 group 5 isakmp
policy 10 lifetime 86400 tunnel-group 10.10.10.1 type
ipsec-l2l tunnel-group 10.10.10.1 ipsec-attributes pre-
shared-key * telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874 : end
pixfirewall#
```

Configuration d'un tunnel de sauvegarde de site à site

Afin de spécifier le type de connexion pour la fonctionnalité de sauvegarde de site à site pour cette entrée de carte de chiffrement, utilisez la commande **crypto map set connection-type** en mode de configuration globale. Utilisez la forme no de cette commande pour rétablir la configuration par défaut.

Syntaxe :

```
crypto map map-name seq-num set connection-type {answer-only | originate-only | bidirectional}
```

- **answer-only** - Spécifie que cet homologue réagit d'abord seulement aux connexions IKE entrantes pendant l'échange de propriété initial afin de déterminer l'homologue approprié auquel se connecter.
- **bidirectional** - Spécifie que cet homologue peut accepter et lancer des connexions basées sur cette entrée de carte de chiffrement. C'est le type de connexion par défaut pour toutes les connexions de site à site.
- **originate-only** - Spécifie que cet homologue lance le premier échange de propriété afin de déterminer l'homologue approprié auquel se connecter.

La commande **crypto map set connection-type** spécifie les types de connexion pour la fonctionnalité de sauvegarde de LAN à LAN. Elle permet de spécifier plusieurs homologues de sauvegarde à une extrémité de la connexion. Cette fonctionnalité fonctionne seulement entre ces plates-formes de routage :

- Deux appliances de sécurité de la gamme Cisco ASA 5500
- Une appliance de sécurité de la gamme Cisco ASA 5500 et un concentrateur Cisco VPN 3000
- Une appliance de sécurité de la gamme Cisco ASA 5500 et une appliance de sécurité qui exécute le logiciel Cisco PIX Security Appliance version 7.0 ou ultérieures

Afin de configurer une connexion entre réseaux locaux de sauvegarde, Cisco recommande que vous configuriez une extrémité de la connexion avec le mot clé originate-only, et l'extrémité avec plusieurs homologues de sauvegarde avec le mot clé answer-only. Sur l'extrémité « originate-only », utilisez la commande **crypto map set peer** afin d'ordonner la priorité des homologues. L'appliance de sécurité « originate-only » tente de négocier avec le premier homologue de la liste. Si cet homologue ne répond pas, le dispositif de sécurité descend dans la liste jusqu'à ce qu'un homologue réponde ou qu'il n'y ait plus d'homologues dans la liste.

Une fois configuré de cette façon, l'homologue « originate-only » tente d'abord d'établir un tunnel propriétaire et de négocier avec un homologue. Ensuite, l'un des homologues peut établir une connexion entre réseaux locaux normale et les données de l'une ou l'autre des extrémités peuvent lancer la connexion en tunnel.

Remarque: Si vous configurez le VPN avec plusieurs adresses IP d'homologue pour une entrée de chiffrement, le VPN est établi avec l'IP de l'homologue de sauvegarde une fois que l'homologue primaire s'arrête. Cependant, lorsque l'homologue primaire reprend, le VPN ne préempte pas l'adresse IP primaire. Vous devez manuellement supprimer la SA existante afin de réinitialiser la négociation VPN pour la basculer sur l'adresse IP primaire. Comme l'indique la conclusion, la préemption VPN n'est pas prise en charge dans le tunnel de site à site.

Types de connexion entre réseaux locaux de sauvegarde pris en charge

Côté distant	Côté central

Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Exemple

Cet exemple, écrit en mode de configuration globale, configure la **carte de chiffrement mymap** et définit le type de connexion sur *originate-only*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

Suppression des associations de sécurité (SA)

En mode privilège du PIX, utilisez les commandes suivantes :

- **clear [crypto] ipsec sa** - Supprime les SA IPSec actives. Le mot clé **crypto** est facultatif.
- **clear [crypto] isakmp sa** — supprime les SA IKE actives. Le mot clé **crypto** est facultatif.

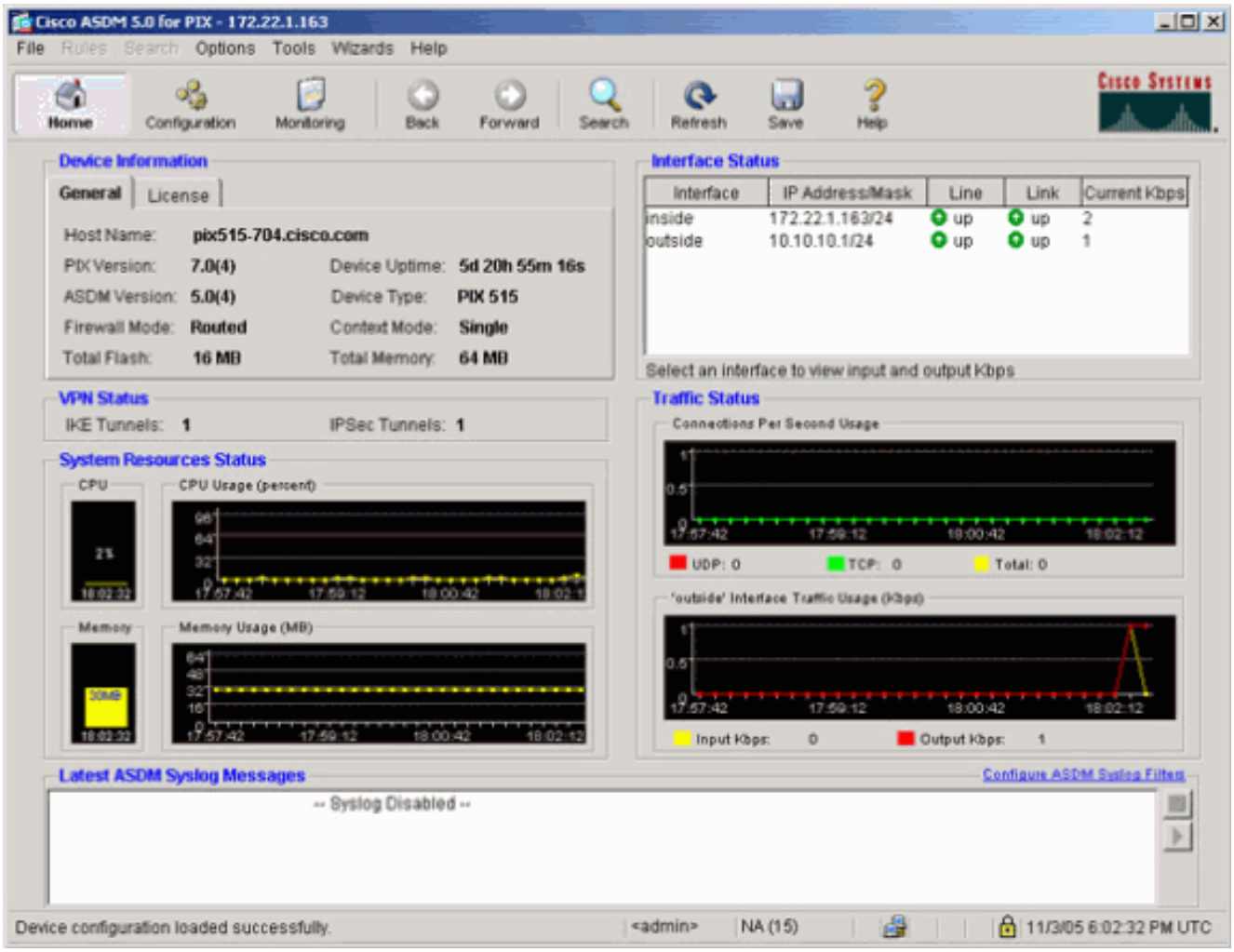
Vérifiez

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

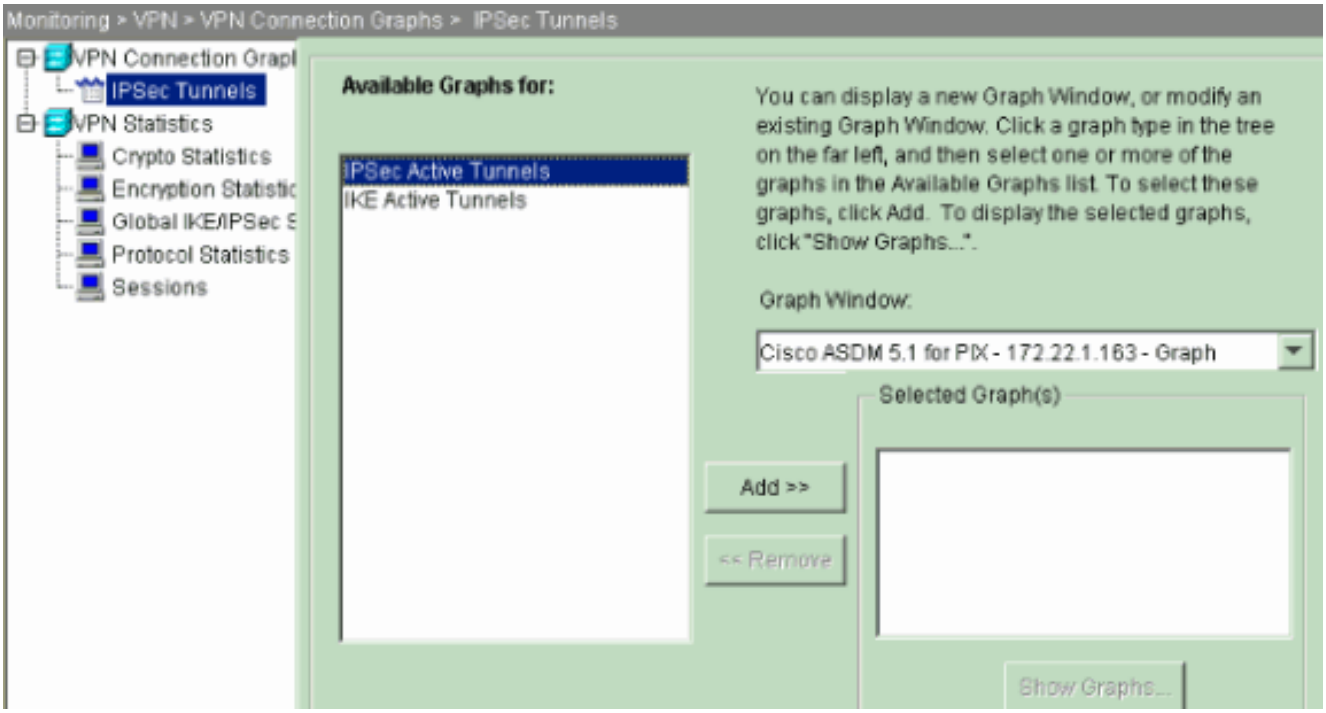
L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

S'il y a du trafic intéressant à l'homologue, le tunnel est établi entre pix515-704 et PIX-02.

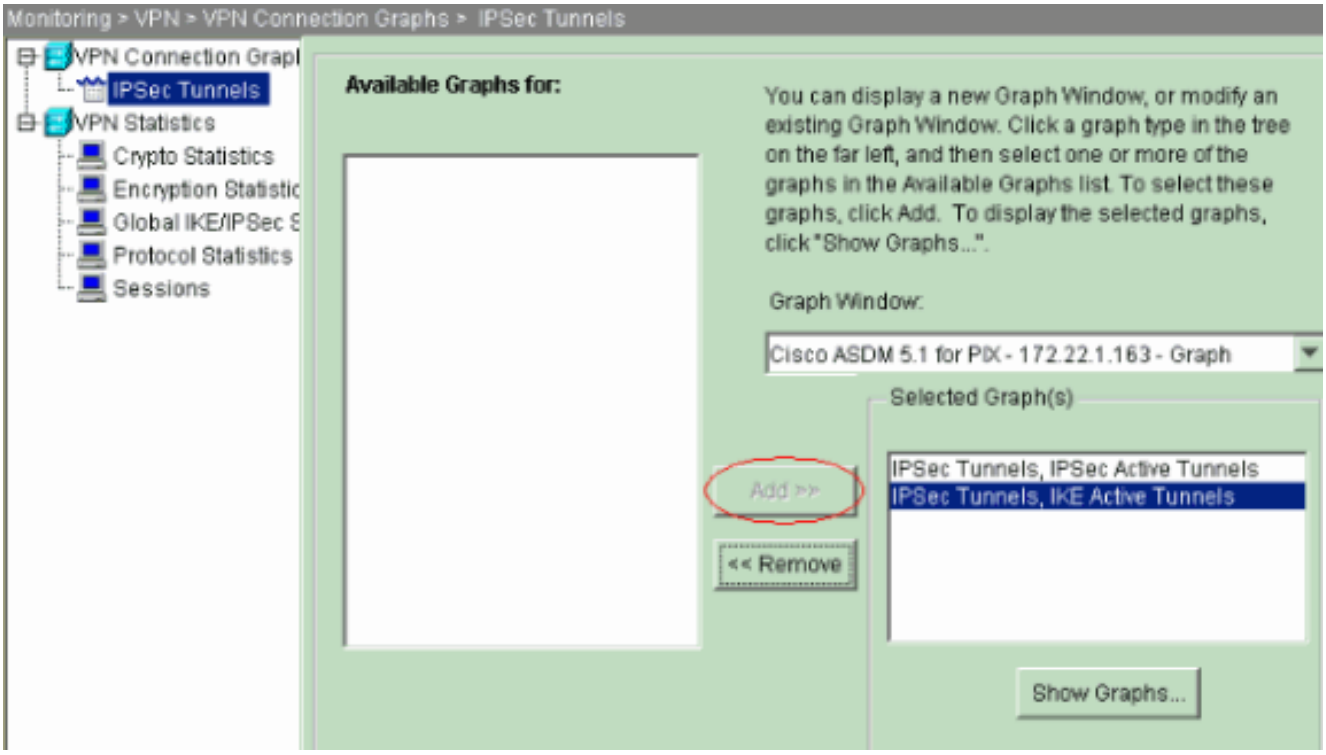
1. Affichez l'état de VPN sous **Home** dans l'ASDM afin de vérifier la formation du tunnel.



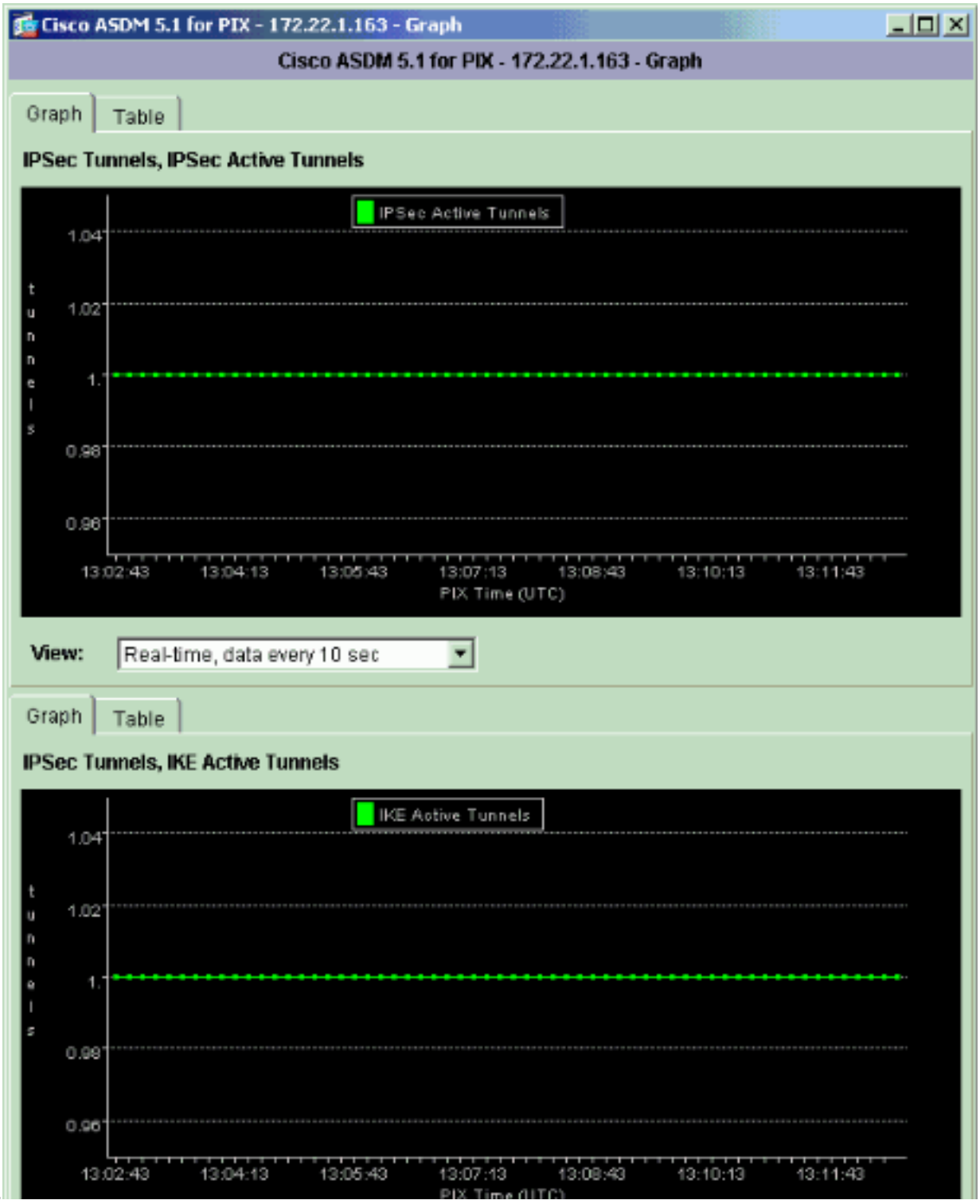
2. Sélectionnez **Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels** afin de vérifier les détails de l'établissement du tunnel.



3. Cliquez sur **Add** pour sélectionner les graphiques disponibles afin de les afficher dans la fenêtre de graphique.

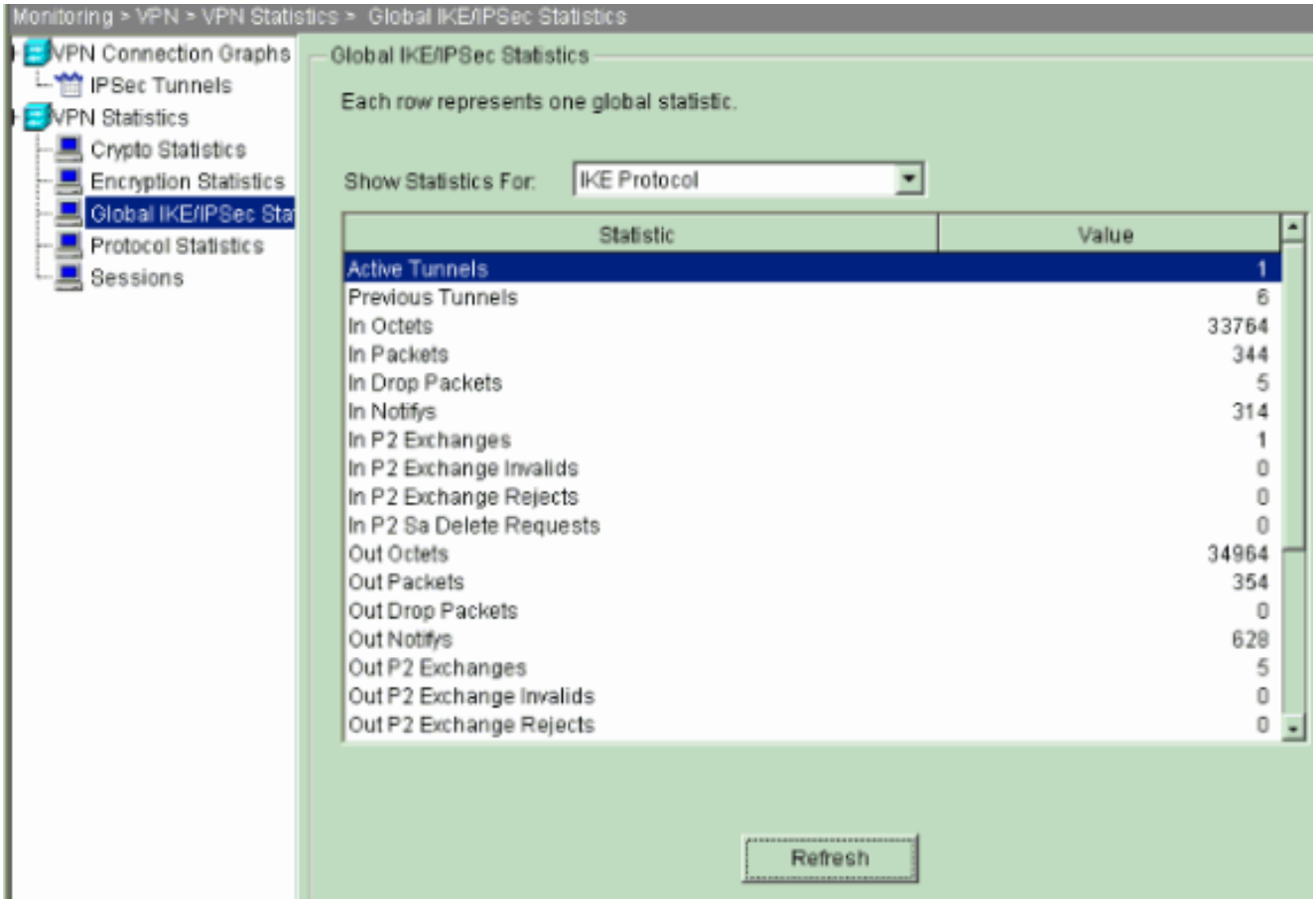


4. Cliquez sur **Show Graphs** afin d'afficher les graphiques des tunnels IKE et IPSec



actifs.

5. Sélectionnez **Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics** afin de consulter les statistiques du tunnel VPN.



Vous pouvez également vérifier la formation des tunnels utilisant la CLI. Exécutez la commande **show crypto isakmp sa** pour vérifier la formation des tunnels et exécutez la commande **show crypto ipsec sa** pour observer le nombre de paquets encapsulés, chiffrés, etc.

pix515-704

```
pixfirewall(config)#show crypto isakmp sa Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey
SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.20.20.1
Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
```

pix515-704

```
pixfirewall(config)#show crypto ipsec sa interface:
outside Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1 access-list outside_cryptomap_20 permit
ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1 #pkts encaps: 20, #pkts
encrypt: 20, #pkts digest: 20 #pkts decaps: 20, #pkts
decrypt: 20, #pkts verify: 20 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 20, #pkts comp
failed: 0, #pkts decomp failed: 0 #send errors: 0, #recv
errors: 0 local crypto endpt.: 10.10.10.1, remote crypto
endpt.: 10.20.20.1 path mtu 1500, ipsec overhead 76,
media mtu 1500 current outbound spi: 44532974 inbound
esp sas: spi: 0xA87AD6FA (2826622714) transform: esp-
aes-256 esp-sha-hmac in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (3824998/28246) IV
size: 16 bytes replay detection support: Y outbound esp
sas: spi: 0x44532974 (1146300788) transform: esp-aes-256
esp-sha-hmac in use settings ={L2L, Tunnel, } slot: 0,
conn_id: 1, crypto-map: outside_map sa timing: remaining
```

```
key lifetime (kB/sec): (3824998/28245) IV size: 16 bytes
replay detection support: Y
```

Dépannez

PFS

Dans des négociations IPsec, le Perfect Forward Secrecy (PFS) assure que chacune nouvelle clé cryptographique est indépendante de toute clé précédente. Activez ou désactivez PFS sur les deux homologues de tunnel, autrement le tunnel IPSec L2L n'est pas établi dans PIX/ASA.

PFS est désactivé par défaut. Afin d'activer PFS, utilisez la commande **pfs** avec le mot clé **enable** en mode de configuration de stratégie de groupe. Afin de désactiver PFS, saisissez le mot clé **disable**.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Afin de retirer l'attribut PFS de la configuration en cours, saisissez la forme **no** de cette commande. Une stratégie de groupe peut hériter d'une valeur pour PFS d'une autre stratégie de groupe. Saisissez la forme **no** de cette commande afin d'éviter d'hériter d'une valeur.

```
hostname(config-group-policy)#no pfs
```

Management-Access

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

Une requête ping ne peut pas être soumise à l'interface interne du PIX depuis l'autre extrémité du tunnel à moins que la commande management-access soit configurée dans le mode de configuration globale.

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access
inside
```

Commandes de débogage

Remarque: Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **debug**.

debug crypto isakmp - Affiche les informations de débogage sur les connexions IPSec et le premier ensemble d'attributs refusés en raison d'incompatibilités sur les deux extrémités.

debug crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7 Nov 27
12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire
message, spi 0x0 Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE Initiator: New Phase 1, Intf 2, IKE Peer
10.20.20.1 local Proxy Address 172.22.1.0, remote Proxy
Address 172.16.1.0, Crypto map (outside map) Nov 27
12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing
ISAKMP SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP =
10.20.20.1, constructing Fragmentation VID + extended
capabilities payload Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total
length : 148 Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1,
```

IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112 Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included IKE fragmentation capability flags : **Main Mode**: True Aggressive Mode: True Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/ Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA_KE payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys for Initiator... Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing dpd vid payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 119 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE RECEIVED

Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 96 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Received DPD VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Oakley begin quick mode Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, **PHASE 1 COMPLETED** Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Starting phase 1 rekey timer: 73440000 (ms) Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got SPI from key engine: SPI = 0x44ae0956 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, oakley constucting quick mode Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing blank hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPSec SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPSec nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing proxy ID Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Transmitting Proxy Id: Local subnet: 172.22.1.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 172.16.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing qm hash payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE RECEIVED Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, loading all IPSEC SAs Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiation complete for LAN-to-LAN Group (10.20.20.1) Initiator, Inbound SPI = 0x44ae0956, Outbound SPI = 0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =

```
10.20.20.1, IP = 10.20.20.1, oakley constructing final
quick mode Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1,
IKE_DECODE SENDING Message (msgid=d723766b) with
payloads : HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, IKE got a KEY_ADD msg for SA: SPI =
0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =
10.20.20.1, IP = 10.20.20.1, Pitcher: received
KEY_UPDATE, spi 0x44ae0956 Nov 27 12:02:00 [IKEv1]:
Group = 10.20.20.1, IP = 10.20.20.1, Starting P2 Rekey
timer to expire in 24480 seconds Nov 27 12:02:00
[IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2
COMPLETED (msgid=d723766b)
```

debug crypto ipsec — Affiche des informations de débogage sur les connexions IPSec.

debug crypto ipsec

```
pix1(config)#debug crypto ipsec 7 exec mode
commands/options: <1-255> Specify an optional debug
level (default is 1) <cr> pix1(config)# debug crypto
ipsec 7 pix1(config)# IPSEC: New embryonic SA created @
0x024211B0, SCB: 0x0240AEB0, Direction: inbound SPI :
0x2A3E12BE Session ID: 0x00000001 VPIF num : 0x00000001
Tunnel type: l2l Protocol : esp Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0, SCB:
0x0240B710, Direction: outbound SPI : 0xB283D32F Session
ID: 0x00000001 VPIF num : 0x00000001 Tunnel type: l2l
Protocol : esp Lifetime : 240 seconds IPSEC: Completed
host OBSA update, SPI 0xB283D32F IPSEC: Updating
outbound VPN context 0x02422618, SPI 0xB283D32F Flags:
0x00000005 SA : 0x0240B7A0 SPI : 0xB283D32F MTU : 1500
bytes VCID : 0x00000000 Peer : 0x00000000 SCB :
0x0240B710 Channel: 0x014A45B0 IPSEC: Completed outbound
VPN context, SPI 0xB283D32F VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
Rule ID: 0x01FA0290 IPSEC: New outbound permit rule, SPI
0xB283D32F Src addr: 10.10.10.1 Src mask:
255.255.255.255 Dst addr: 10.20.20.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0xB283D32F Use SPI: true IPSEC:
Completed outbound permit rule, SPI 0xB283D32F Rule ID:
0x0240AF40 IPSEC: Completed host IBSA update, SPI
0x2A3E12BE IPSEC: Creating inbound VPN context, SPI
0x2A3E12BE Flags: 0x00000006 SA : 0x024211B0 SPI :
0x2A3E12BE MTU : 0 bytes VCID : 0x00000000 Peer :
0x02422618 SCB : 0x0240AEB0 Channel: 0x014A45B0 IPSEC:
Completed inbound VPN context, SPI 0x2A3E12BE VPN
handle: 0x0240BF80 IPSEC: Updating outbound VPN context
0x02422618, SPI 0xB283D32F Flags: 0x00000005 SA :
0x0240B7A0 SPI : 0xB283D32F MTU : 1500 bytes VCID :
0x00000000 Peer : 0x0240BF80 SCB : 0x0240B710 Channel:
0x014A45B0 IPSEC: Completed outbound VPN context, SPI
0xB283D32F VPN handle: 0x02422618 IPSEC: Completed
outbound inner rule, SPI 0xB283D32F Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
Rule ID: 0x0240AF40 IPSEC: New inbound tunnel flow rule,
SPI 0x2A3E12BE Src addr: 172.16.1.0 Src mask:
255.255.255.0 Dst addr: 172.22.1.0 Dst mask:
255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use
protocol: false SPI: 0x00000000 Use SPI: false IPSEC:
```

```
Completed inbound tunnel flow rule, SPI 0x2A3E12BE Rule
ID: 0x0240B108 IPSEC: New inbound decrypt rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound decrypt rule, SPI 0x2A3E12BE Rule ID:
0x02406E98 IPSEC: New inbound permit rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound permit rule, SPI 0x2A3E12BE Rule ID:
0x02422C78
```

Informations connexes

- Création de tunnels redondants entre pare-feu à l'aide de PDM
- Logiciels pare-feu Cisco PIX
- Cisco Adaptive Security Device Manager
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems