ASA/PIX : Exemple de configuration NTP avec et sans tunnel IPSec

Contenu

Introduction

Ce document fournit à une configuration d'échantillon pour synchroniser l'horloge de dispositifs de sécurité PIX/ASA un Serveur de synchronisation de réseau utilisant le Protocole NTP (Network Time Protocol). ASA1 communique directement avec le trafic de NTP de passages du temps server.ASA2 de réseau par un tunnel d'IPsec à ASA1, qui consécutivement en avant les paquets au Serveur de synchronisation de réseau.

Référez-vous à ASA 8.3 et plus tard : NTP avec et sans un exemple de configuration de tunnel d'IPsec pour plus d'informations sur la configuration identique sur Cisco ASA avec des versions 8.3 et ultérieures.

Remarque: Un routeur peut également être utilisé en tant que serveur de NTP pour synchroniser l'horloge de dispositifs de sécurité PIX/ASA.

Conditions préalables

Conditions requises

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

- La Connectivité de bout en bout d'IPsec doit être établie avant de commencer cette configuration de NTP.
- La licence du dispositif de sécurité doit être activée pour le chiffrement Data Encryption Standard (DES) (à un niveau de chiffrement minimal).

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Sécurité adaptative Appliance(ASA) de Cisco avec la 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.

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.

Produits connexes

Cette configuration peut également être utilisée avec le dispositif de sécurité de la gamme Cisco PIX 500, qui exécute la versions 7.x et les versions ultérieures.

Remarque: Le support de NTP a été ajouté dans la version de PIX 6.2. Référez-vous à PIX 6.2 : NTP avec et sans un exemple de configuration de tunnel d'IPsec afin de configurer le NTP sur le Pare-feu de Cisco PIX.

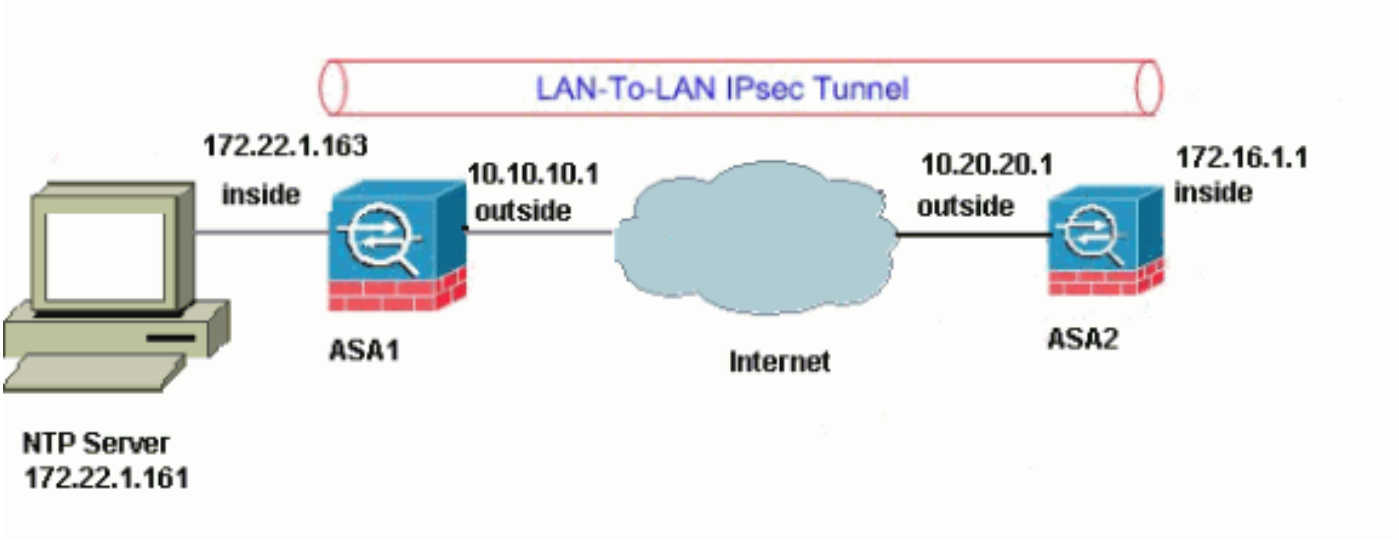
Conventions

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

Configuration

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



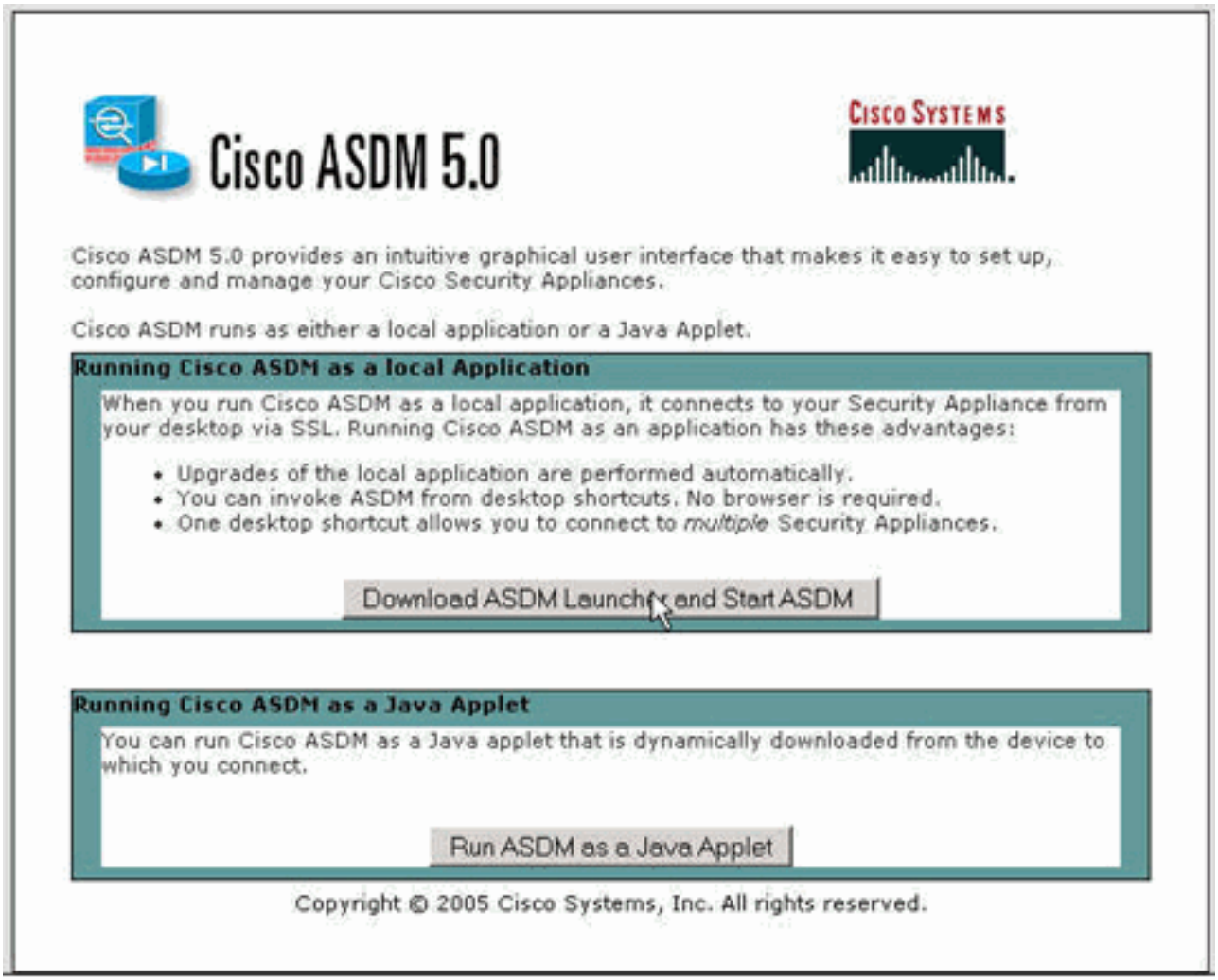
Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

- Configuration ASDM du tunnel VPN
- Configuration du NTP ASDM
- Configuration ASA1 CLI
- Configuration ASA2 CLI

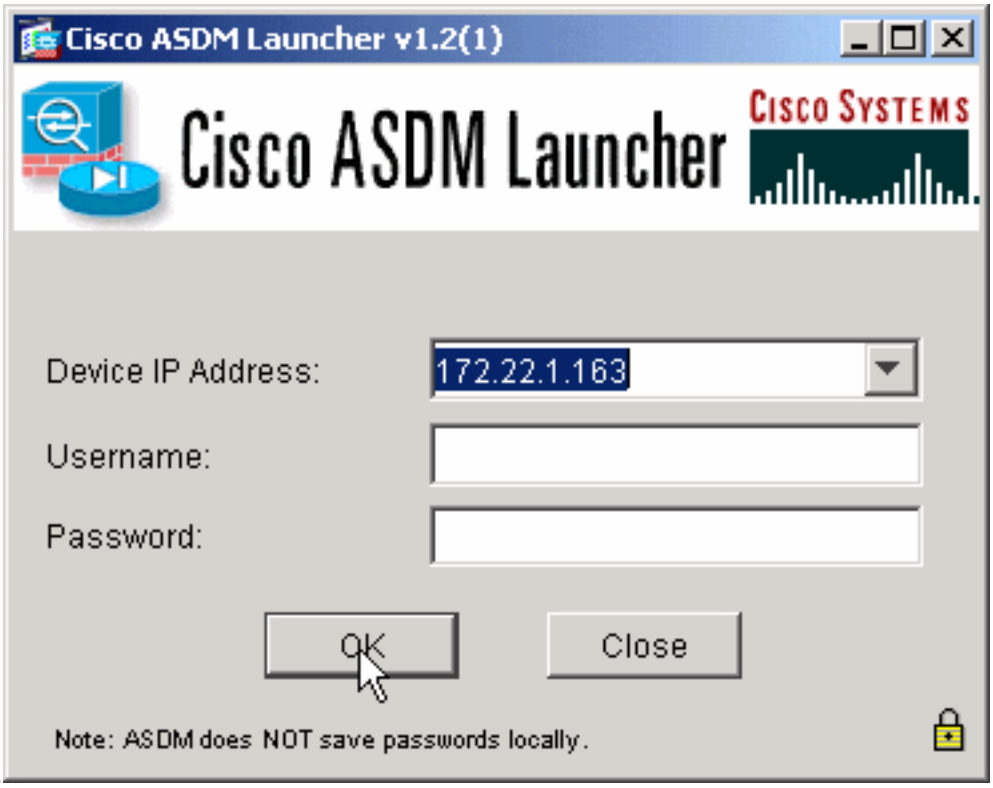
Configuration ASDM du tunnel VPN

Terminez-vous ces étapes pour créer le tunnel VPN :

1. Ouvrez votre navigateur et tapez le **<Inside_IP_Address_of_ASA> de https://** pour accéder à l'ASDM sur l'ASA.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.L'ASA 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.

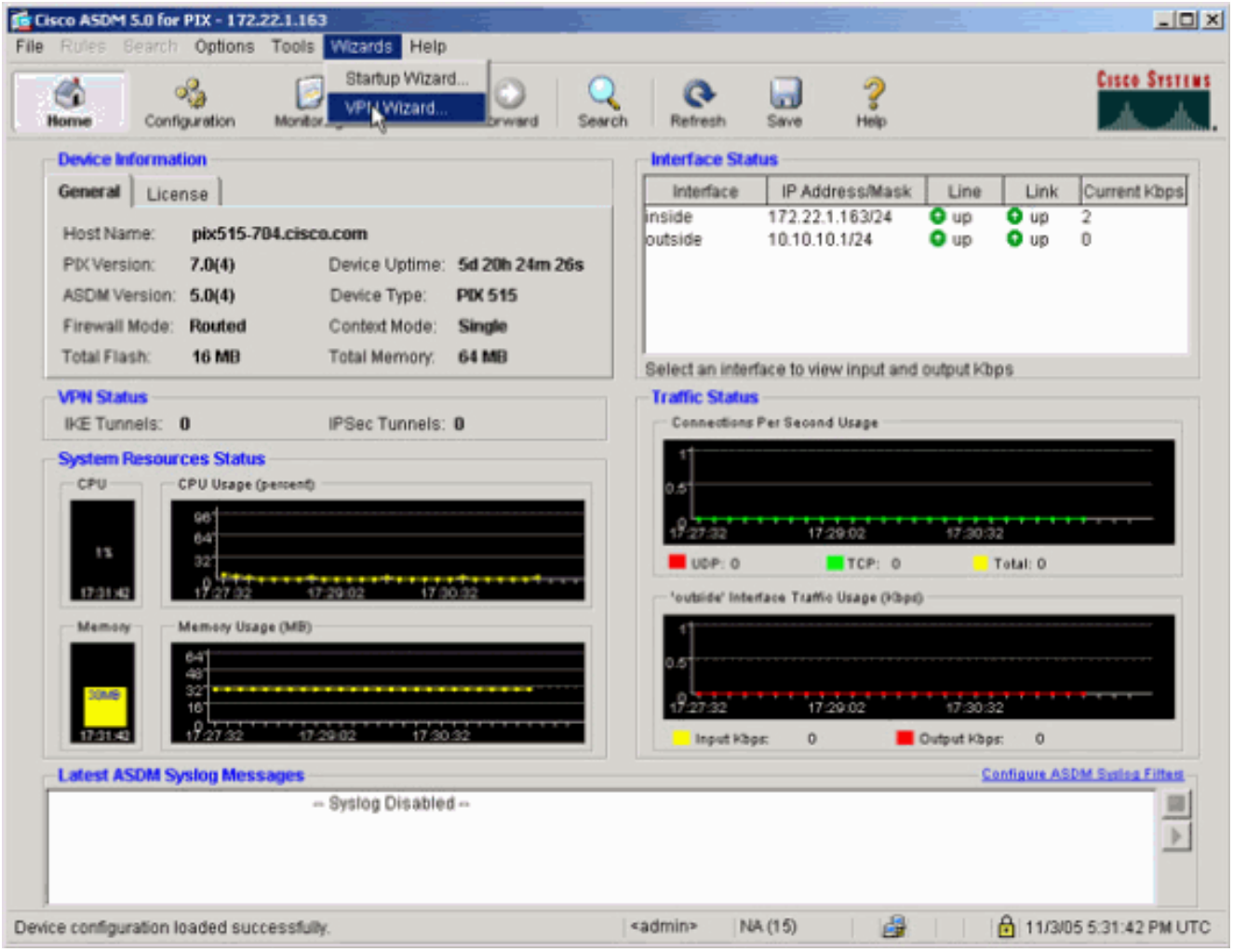


2. Cliquez sur **Download ASDM Launcher and Start ASDM** pour télécharger le programme d'installation de l'application ASDM.
3. Une fois le lanceur d'ASDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco ASDM.
4. Entrez l'adresse 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

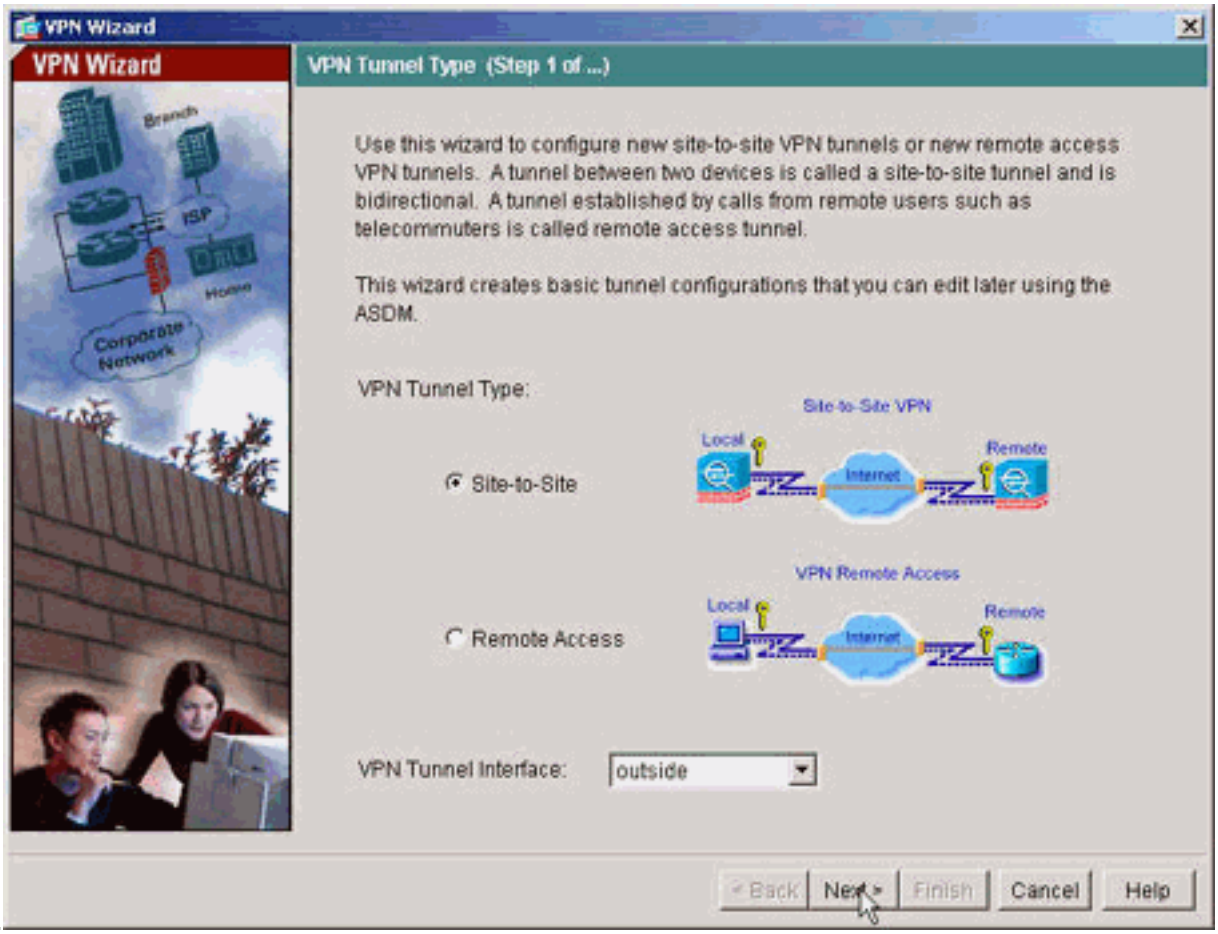


défaut).

5. Exécutez l'assistant VPN une fois que l'application ASDM se connecte à l'ASA.

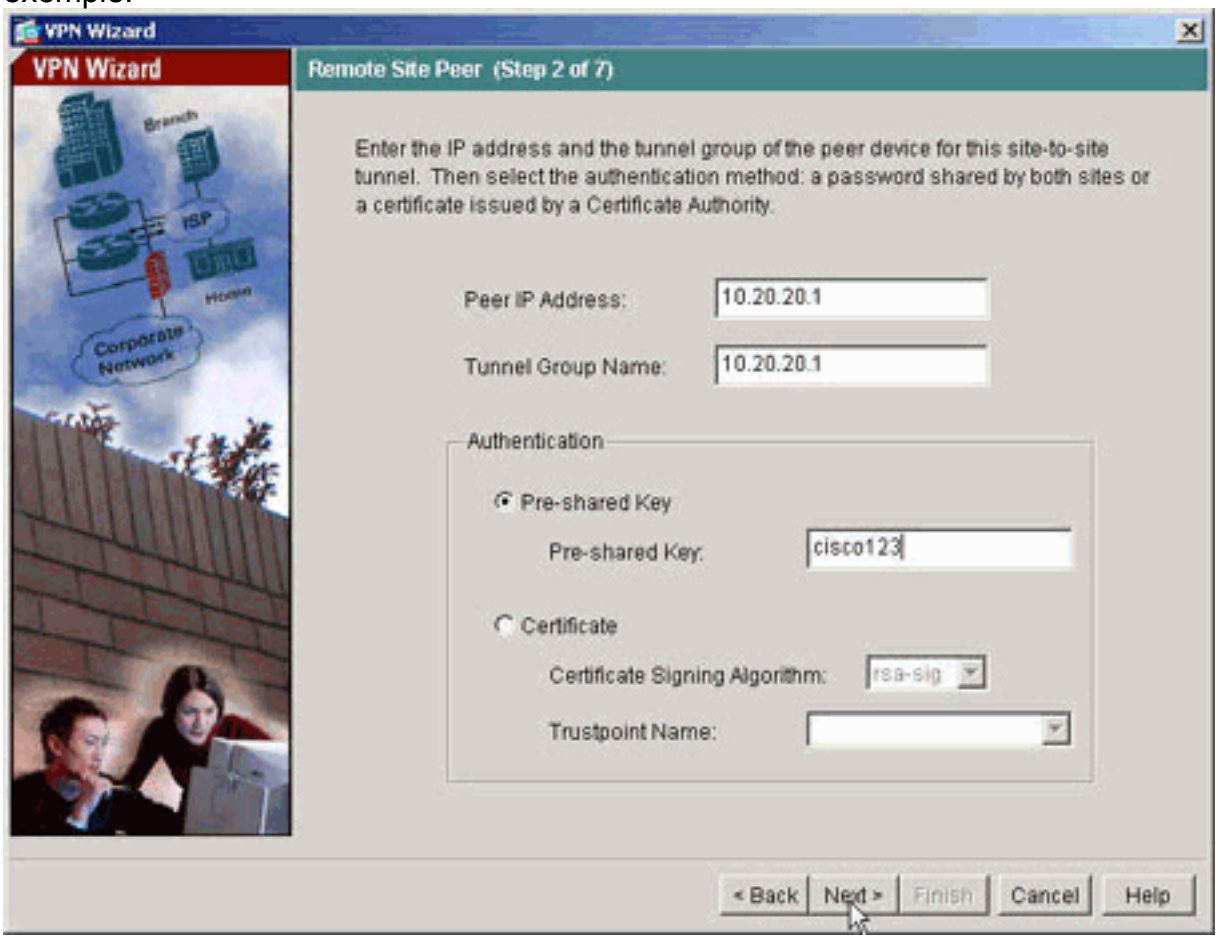


6. Choisissez le type de tunnel VPN d'IPsec de **site à**



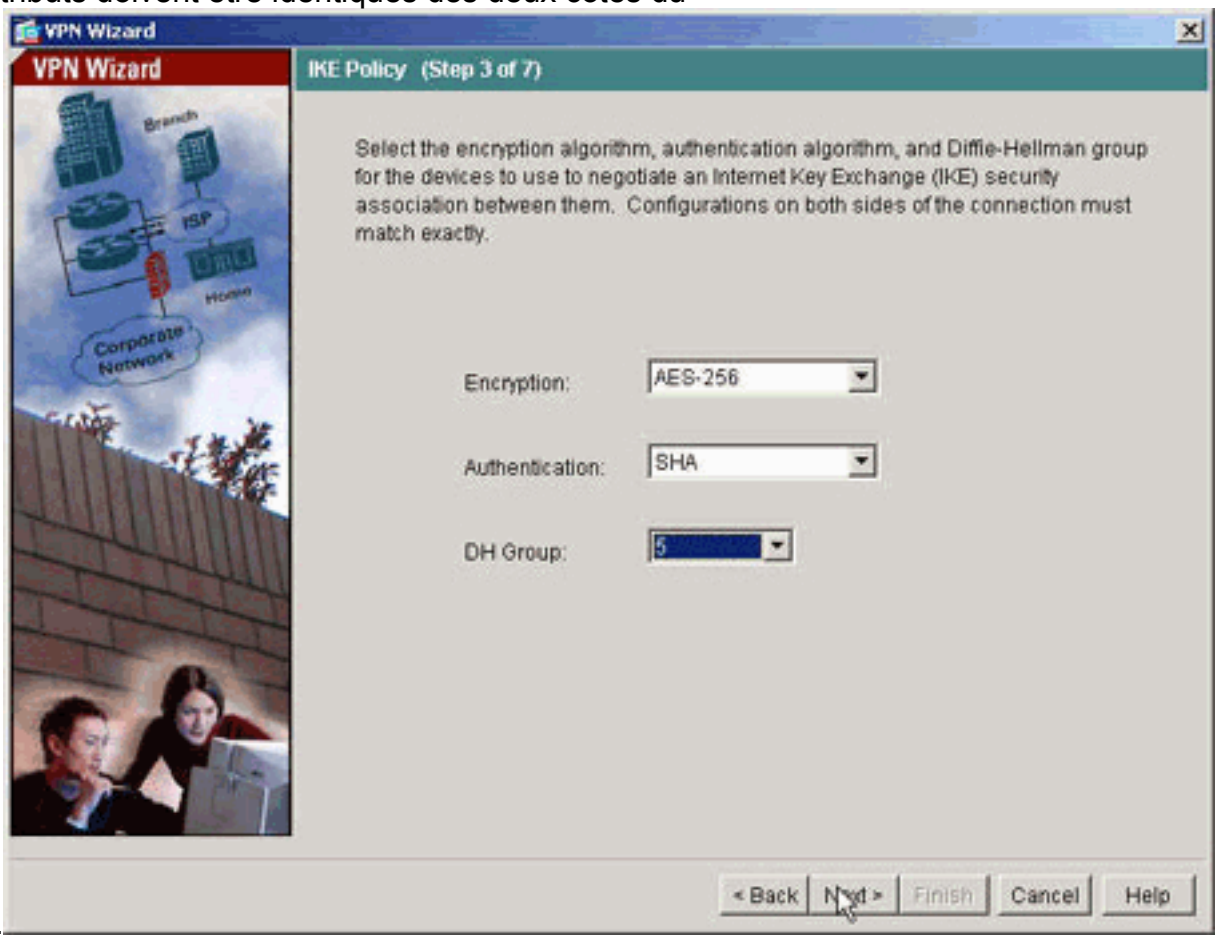
site.

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

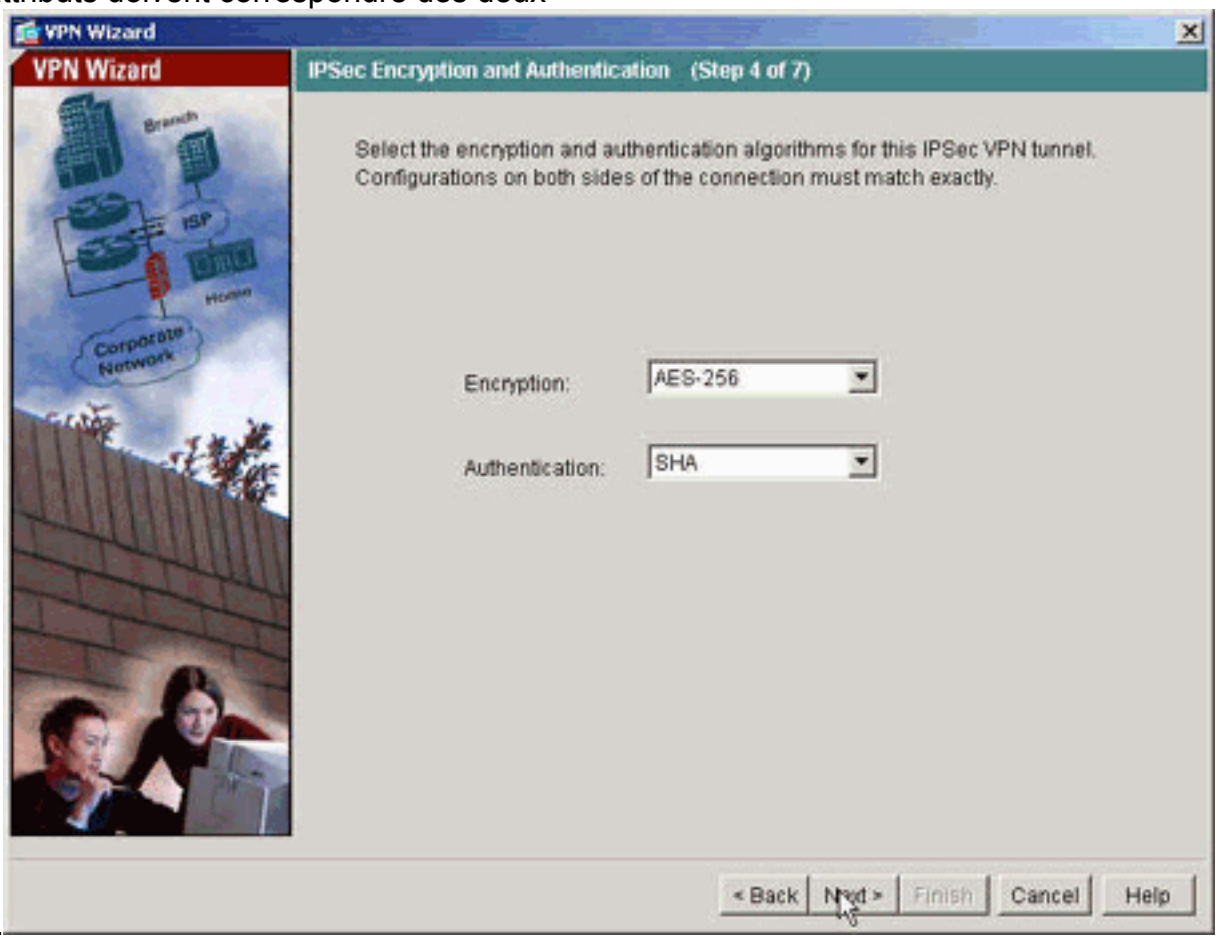


8. Spécifiez les attributs à utiliser pour l'IKE, également connus sous le nom de « Phase 1 ».

Ces attributs doivent être identiques des deux côtés du tunnel.

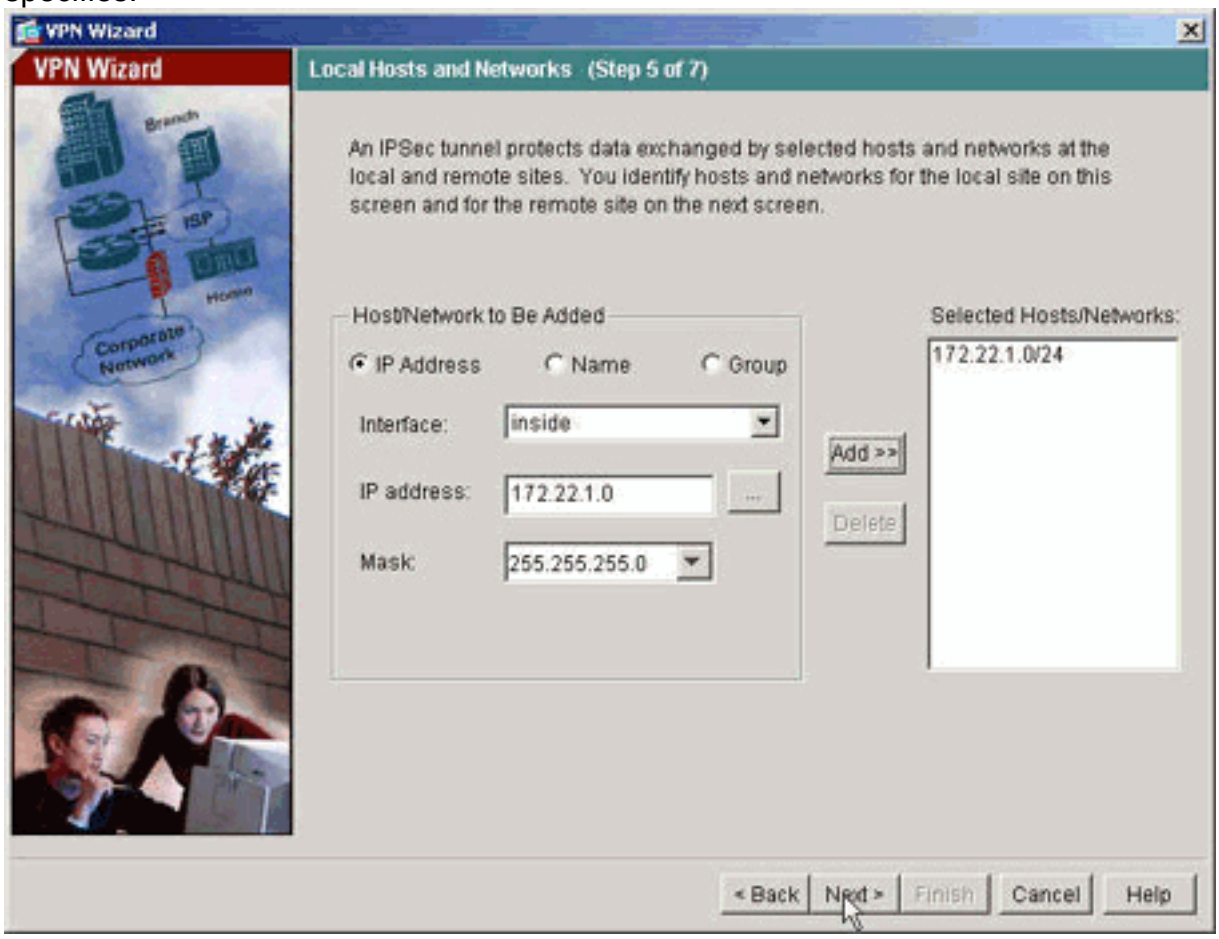


9. Spécifiez les attributs à utiliser pour IPsec, également connus sous le nom de « Phase 2 ». Ces attributs doivent correspondre des deux côtés.

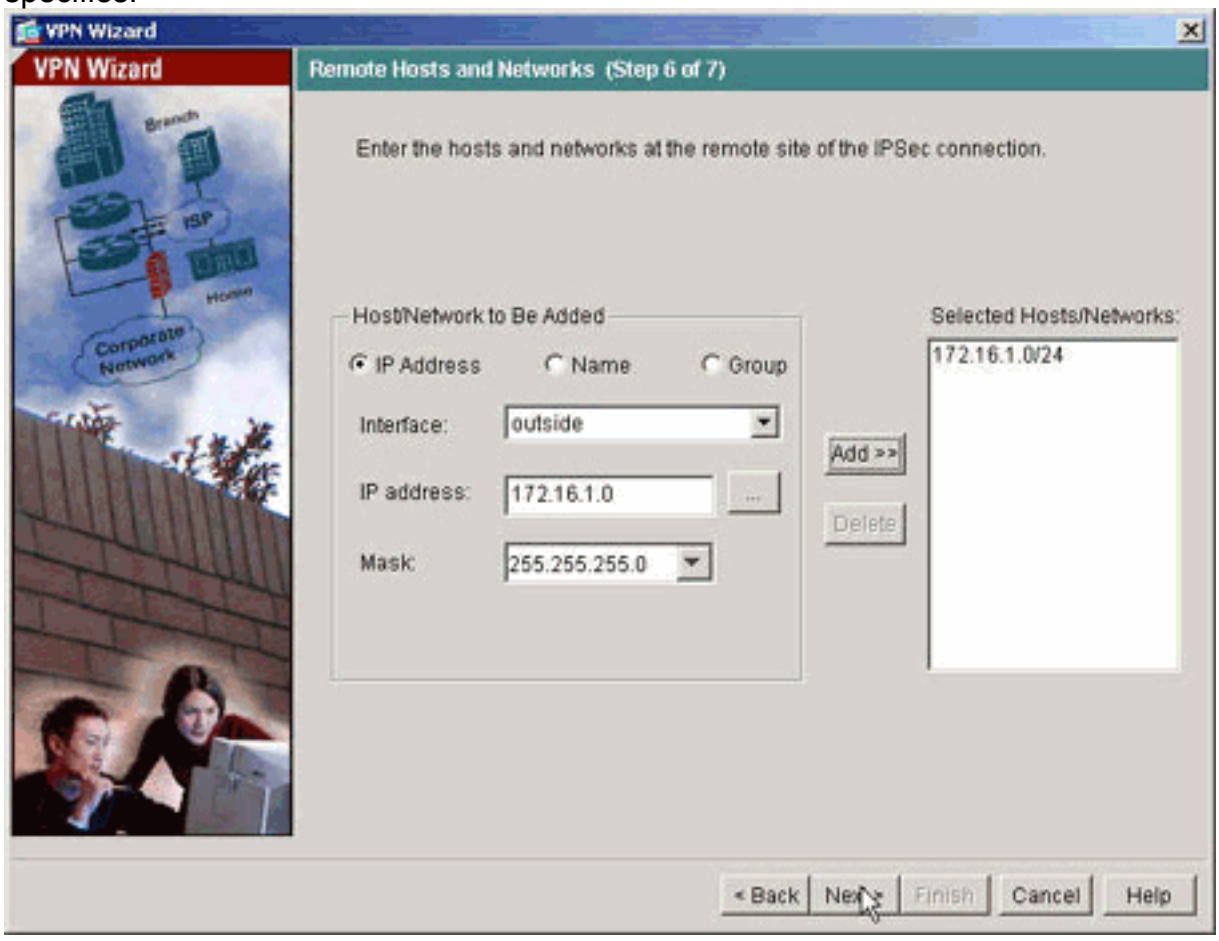


10. Spécifiez les hôtes dont le trafic devrait être autorisé à passer par le tunnel VPN. Dans

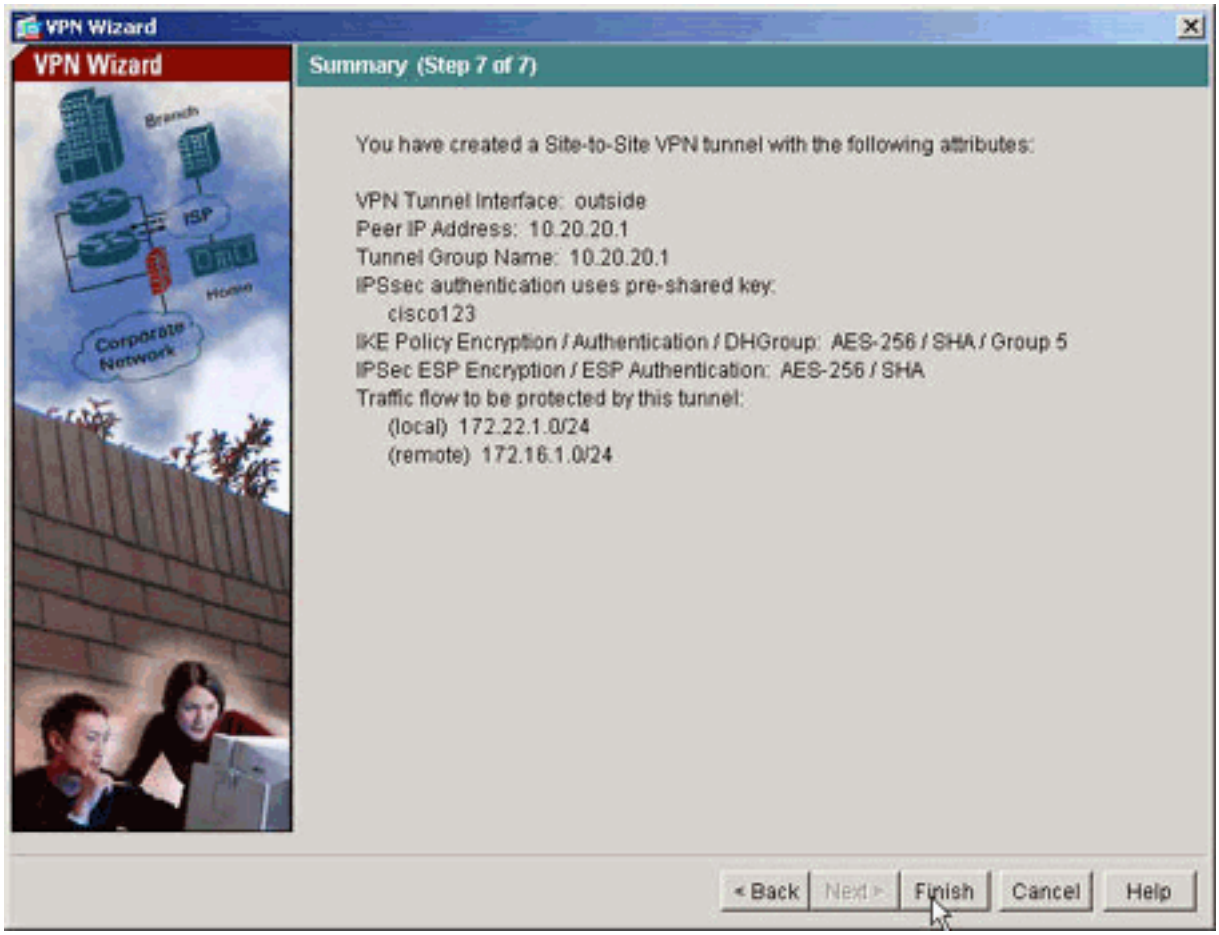
cette étape, les hôtes locaux à ASA1 sont spécifiés.



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



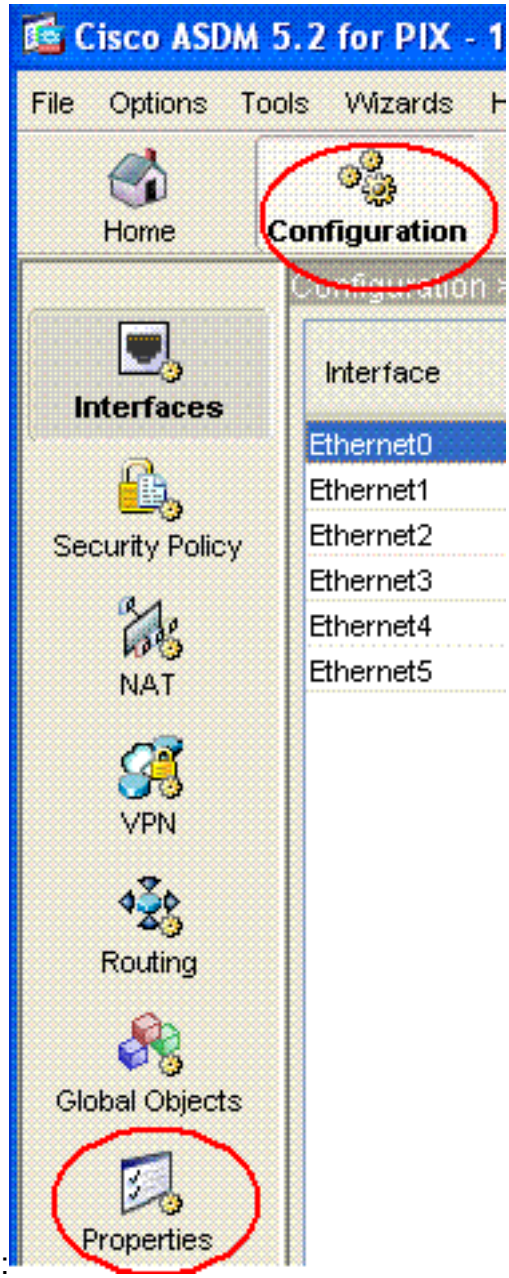
12. Les attributs définis par l'assistant VPN sont affichés dans ce récapitulatif. Vérifiez une deuxième fois la configuration et cliquez sur **Finish** quand vous êtes sûr que les paramètres sont
corrects.



Configuration du NTP ASDM

Terminez-vous ces étapes pour configurer le NTP sur l'appliance de sécurité Cisco :

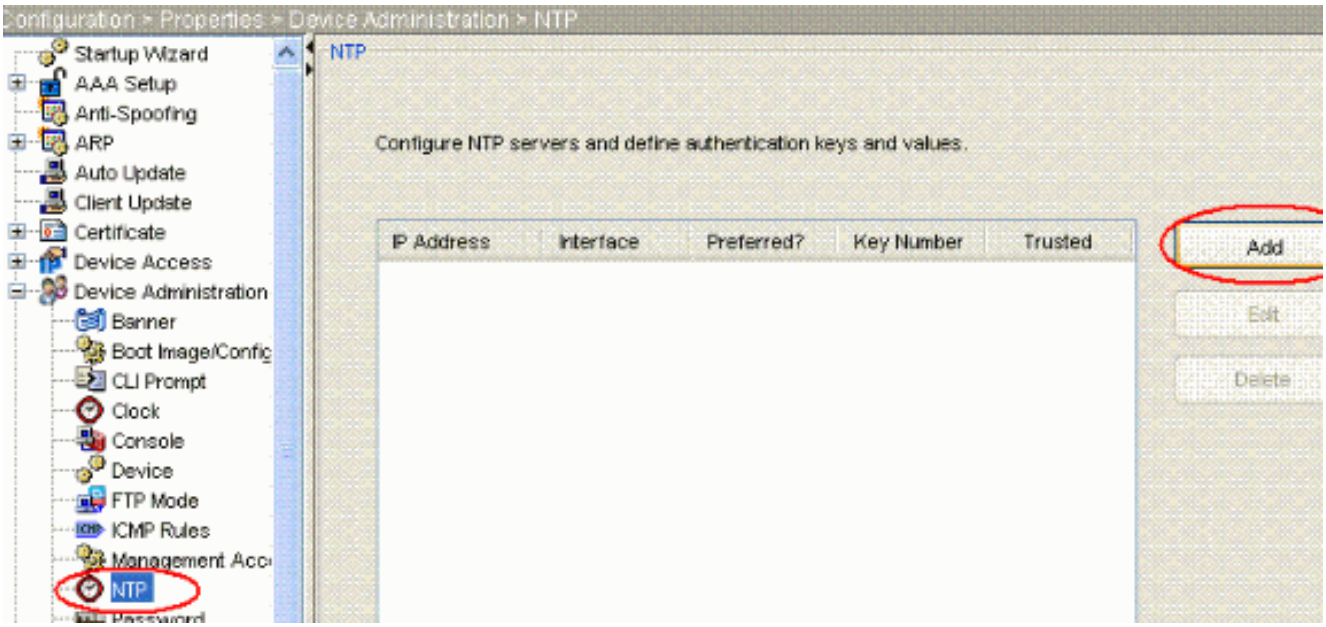
1. Choisissez la **configuration** dans la page d'accueil ASDM comme affiché ici



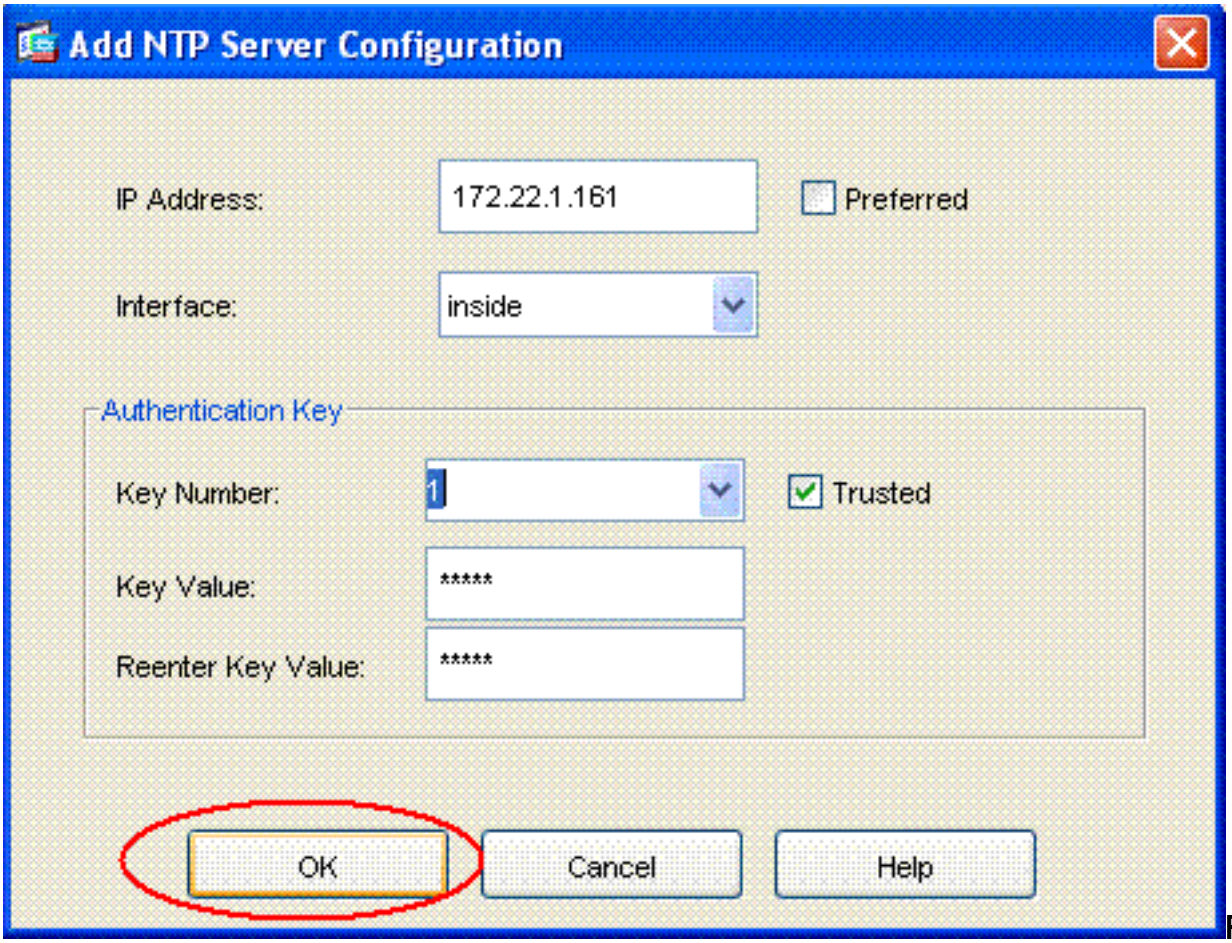
:

2. Choisissez Properties maintenant **> Gestion de périphériques > NTP** afin d'ouvrir la page de configuration de **NTP de l'**ASDM comme affiché ici

:

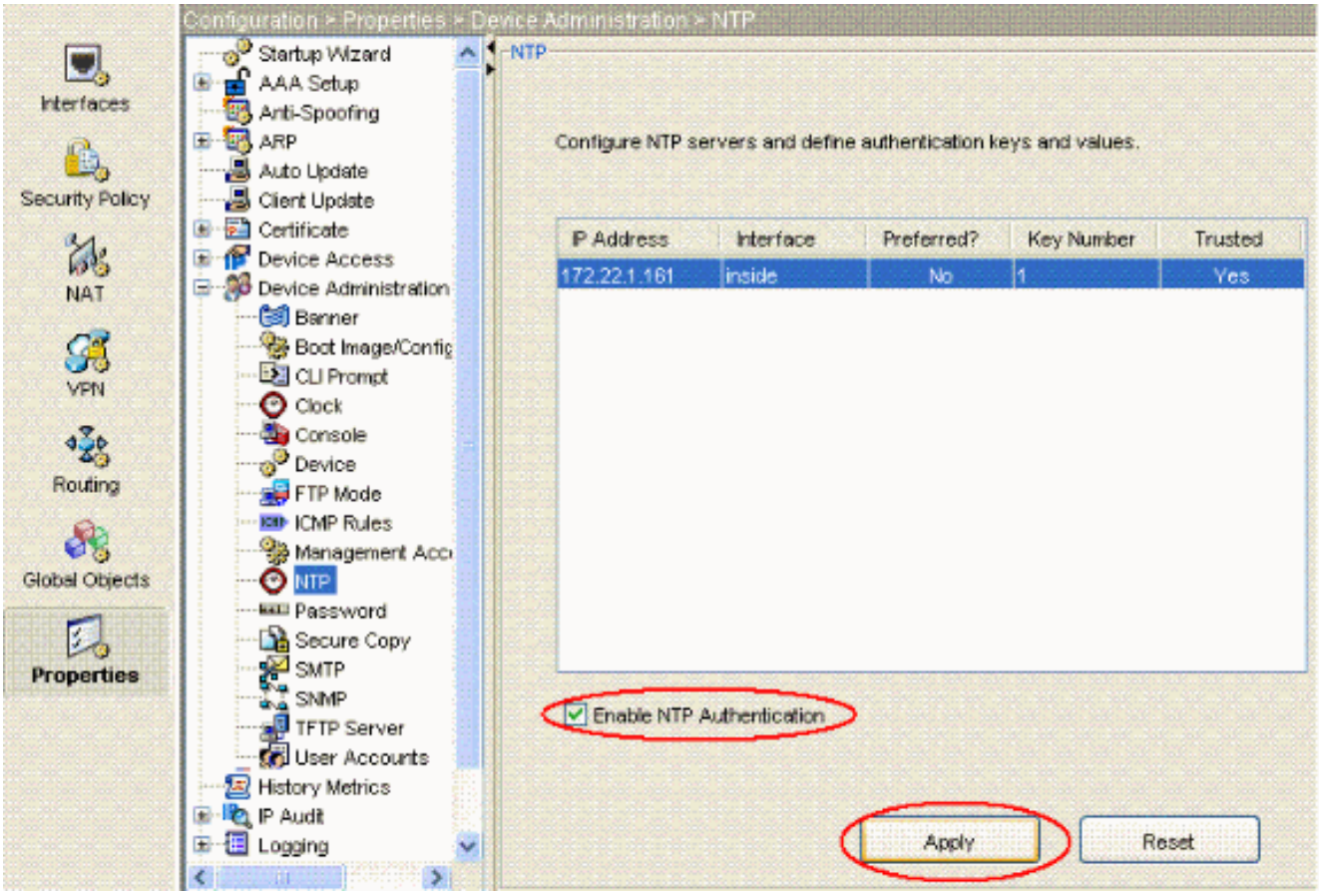


3. Cliquez sur le bouton d'**AJOUTER** afin d'ajouter un serveur de NTP et fournir les attributs requis tels que le nom d'adresse IP, d'interface (intérieur ou extérieur), le nombre de clé et la valeur principale pour Authetication dans la nouvelle fenêtre qui monte après que vous ayez cliqué sur en fonction le bouton d'**AJOUTER** suivant les indications de la copie d'écran. Cliquez sur alors en fonction
CORRECT.



Remarque: Le nom d'interface devrait être choisi en tant qu'à l'intérieur pour ASA1 et extérieur pour ASA2.**Remarque: La clé d'authentification de ntp** devrait être identique dans l'ASA et le serveur de NTP.La configuration d'attribut d'Authetication dans le cli pour ASA1 et ASA2 sont affichés ci-dessous :`ASA1#`**`ntp authentication-key 1 md5 cisco`** `ntp trusted-key 1 ntp server 172.22.1.161 key 1 source inside ASA2#`**`ntp authentication-key 1 md5 cisco`** `ntp trusted-key 1 ntp server 172.22.1.161 key 1 source outside`

4. Maintenant cliquez sur l'**authentification de NTP d'enable de** case à cocher et cliquez sur Apply, qui se termine la tâche de configuration de
NTP.



Configuration ASA1 CLI

ASA1

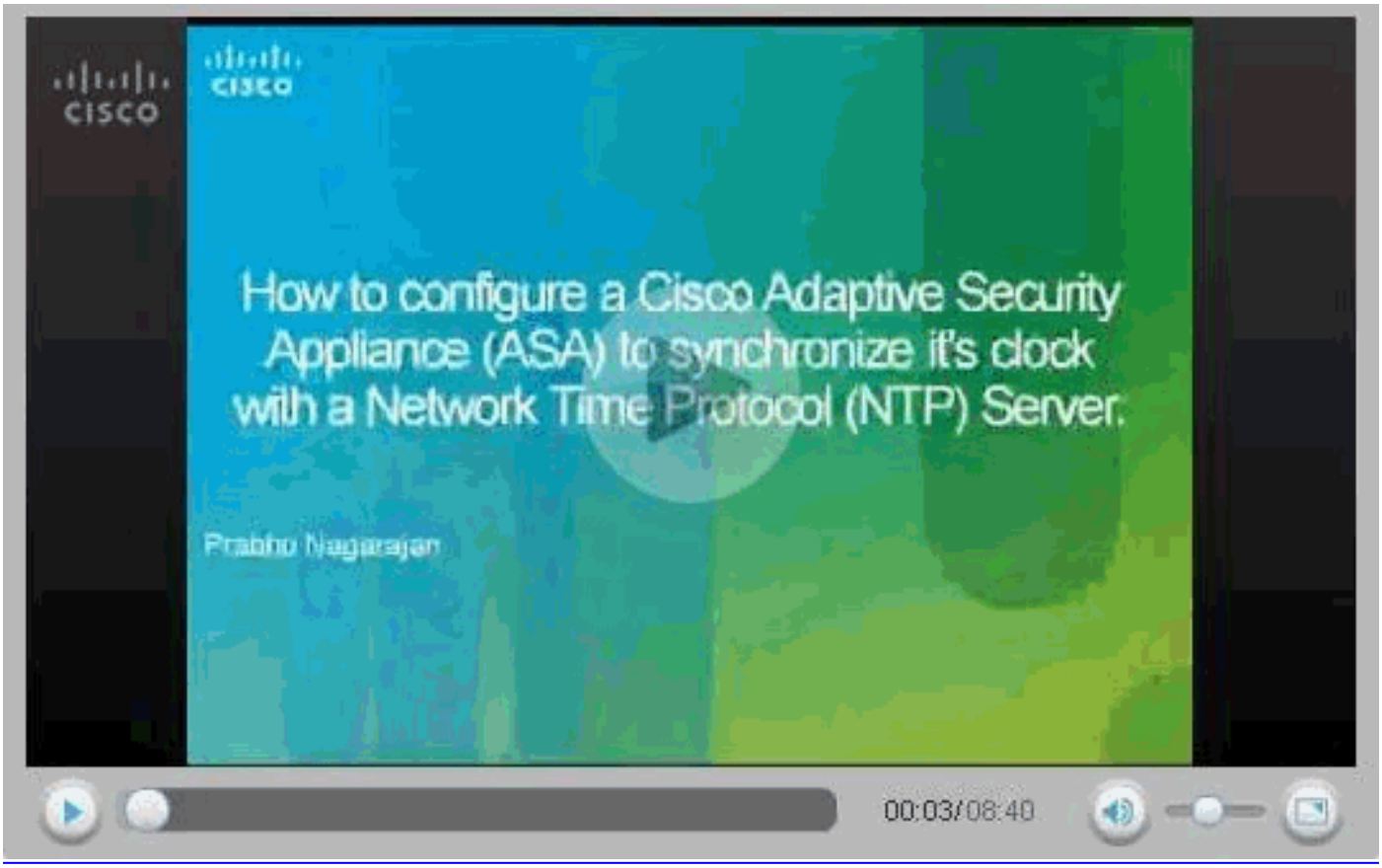
```
ASA#show run : Saved ASA Version 7.1(1) ! hostname ASA1
domain-name default.domain.invalid enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0
nameif outside security-level 0 ip address 10.10.10.1
255.255.255.0 !--- Configure the outside interface. !
interface Ethernet1 nameif 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 command !--- tunnel-group
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
!--- Define the NTP server autentication-key,Trusted-key
!--- and the NTP server address for configuring NTP. ntp
authentication-key 1 md5 * ntp trusted-key 1 !--- The
NTP server source is to be mentioned as inside for ASA1
ntp server 172.22.1.161 key 1 source inside
Cryptochecksum:ce7210254f4a0bd263a9072a4ccb7cf7 : end
```

Ce vidéo signalé à la Communauté de support de Cisco explique avec une démonstration, la

procédure pour configurer l'ASA comme client de NTP :

[Comment configurer une appliance de sécurité adaptable Cisco (ASA) pour synchroniser son horloge avec un serveur de Protocole NTP (Network Time Protocol).]



Configuration ASA2 CLI

ASA2

```
ASA Version 7.1(1)
!
hostname ASA2
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 ASA1. 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 ASA1. 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 !--- Define the NTP
server autentication-key,Trusted-key !--- and the NTP
server address for configuring NTP. ntp authentication-
key 1 md5 * ntp trusted-key 1 !--- The NTP server source
is to be mentioned as outside for ASA2. ntp server
172.22.1.161 key 1 source outside
Cryptochecksum:d5e2ee898f5e8bd28e6f027aeed7f41b : end
ASA#
```

Vérifiez

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 ntp status — Affiche les informations d'horloge de NTP.`ASA1#`**`show ntp status Clock is synchronized`**`, stratum 2, reference is 172.22.1.161 nominal freq is 99.9984 Hz, actual freq is 99.9983 Hz, precision is 2**6 reference time is ccf22b77.f7a6e7b6 (13:28:23.967 UTC Tue Dec 16 2008) clock offset is 34.8049 msec, root delay is 4.78 msec root dispersion is 60.23 msec, peer dispersion is 25.41 msec`
- show ntp associations [détail] — Affiche les associations configurées de Serveur de synchronisation de réseau.`ASA1#`**`show ntp associations detail 172.22.1.161 configured, authenticated`**`, our_master, sane, valid, stratum 1 ref ID .LOCL., time ccf2287d.3668b946 (13:15:41.212 UTC Tue Dec 16 2008) our mode client, peer mode server, our poll intvl 64, peer poll intvl 64 root delay 0.00 msec, root disp 0.03, reach 7, sync dist 23.087 delay 4.52 msec, offset 9.7649 msec, dispersion 20.80 precision 2**19, version 3 org time`

```
ccf22896.f1a4fca3 (13:16:06.943 UTC Tue Dec 16 2008) rcv time ccf22896.efb94b28
(13:16:06.936 UTC Tue Dec 16 2008) xmt time ccf22896.ee5691dc (13:16:06.931 UTC Tue Dec 16
2008) filtdelay = 4.52 4.68 4.61 0.00 0.00 0.00 0.00 0.00 filtoffset = 9.76 7.09 3.85 0.00
0.00 0.00 0.00 0.00 filterror = 15.63 16.60 17.58 14904.3 14904.3 14904.3 14904.3 14904.3
```

Dépannez

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

Dépannage des commandes

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.

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

- **validité de debug ntp** — Validité d'horloge de ntp peer d'affichages.C'est **sortie de débogage de la** non-concordance principale :
  `NTP: packet from 172.22.1.161 failed validity tests 10 Authentication failed`
- **paquet de debug ntp** — Les informations de paquet de NTP d'affichages.Quand il n'y a aucune réponse du serveur, seulement le paquet de `xmit de NTP` est vu sur l'ASA sans le paquet `récepteur de NTP.ASA1# NTP: xmit packet to 172.22.1.161:`

```
 leap 0, mode 3, version 3, stratum 2, ppoll 64
 rtdel 012b (4.562), rtdsp 0cb6 (49.652), refid ac1601a1 (172.22.1.161)
 ref ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)
 org ccf22916.f426232d (13:18:14.953 UTC Tue Dec 16 2008)
 rec ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)
 xmt ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)
NTP: rcv packet from 172.22.1.161 to 172.22.1.163 on inside:
 leap 0, mode 4, version 3, stratum 1, ppoll 64
 rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 4c4f434c (76.79.67.76)
 ref ccf2293d.366a4808 (13:18:53.212 UTC Tue Dec 16 2008)
 org ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)
 rec ccf22956.f52e480e (13:19:18.957 UTC Tue Dec 16 2008)
 xmt ccf22956.f5688c29 (13:19:18.958 UTC Tue Dec 16 2008)
 inp ccf22956.f982bcd9 (13:19:18.974 UTC Tue Dec 16 2008)
```

Informations connexes

- 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
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems