

ASA/PIX: NTP con y sin un ejemplo de configuración del túnel IPsec

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Configuración](#)

[Diagrama de la red](#)

[Configuración de ASDM del túnel VPN](#)

[Configuración de ASDM NTP](#)

[Configuración CLI ASA1](#)

[Configuración CLI ASA2](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento aporta una configuración de muestra para sincronizar el reloj del dispositivo de seguridad de PIX/ASA con un servidor de hora de la red mediante el uso de Network Time Protocol (NTP). ASA1 comunica directamente con el tráfico de los pasos NTP del tiempo de la red server.ASA2 a través de un túnel IPsec a ASA1, que a su vez adelanta los paquetes al servidor de tiempo de la red.

Refiera a [ASA 8.3 y posterior: NTP con y sin un ejemplo de configuración del túnel IPsec](#) para más información sobre la configuración idéntica en Cisco ASA con las versiones 8.3 y posterior.

Nota: Un router puede también ser utilizado como servidor NTP para sincronizar el reloj del dispositivo de seguridad del PIX/ASA.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- La Conectividad del IPSEC de extremo a extremo debe ser establecida antes de comenzar esta configuración del NTP.
- La licencia del dispositivo de seguridad se debe habilitar para el cifrado del Data Encryption Standard (DES) (en un nivel mínimo del cifrado).

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Seguridad adaptante Appliance(ASA) de Cisco con la versión 7.x y posterior
- Versión 5.x.and del ASDM más adelante

Nota: Consulte [Cómo Permitir el Acceso HTTPS para el ASDM](#) para que el ASA sea configurado por el ASDM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con el dispositivo de seguridad de la serie del Cisco PIX 500, que funciona con la versión 7.x y posterior.

Nota: El soporte NTP fue agregado en la versión de PIX 6.2. Refiera a [PIX 6.2: NTP con y sin un ejemplo de configuración del túnel IPsec](#) para configurar el NTP en el Cisco PIX Firewall.

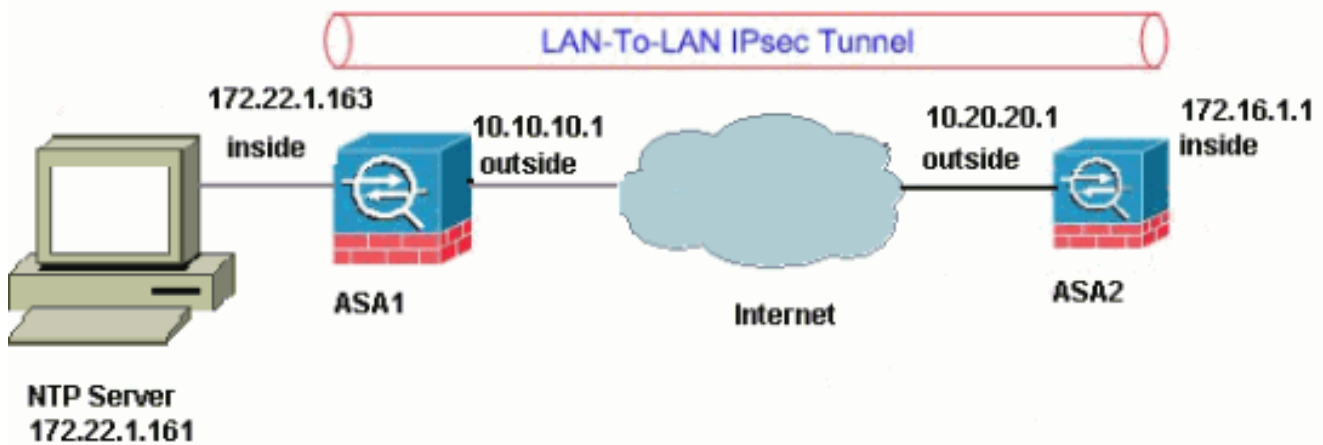
Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Configuración

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del [RFC 1918](#), que se han utilizado en un ambiente de laboratorio.

- [Configuración de ASDM del túnel VPN](#)
- [Configuración de ASDM NTP](#)
- [Configuración CLI ASA1](#)
- [Configuración CLI ASA2](#)

[Configuración de ASDM del túnel VPN](#)

Complete estos pasos para crear el túnel VPN:

1. Abra su **<Inside_IP_Address_of_ASA>** de **https://** del navegador y del tipo para acceder el ASDM en el ASA. Esté seguro de autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco. El ASA presenta esta ventana para permitir la descarga de la aplicación ASDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas java.



Cisco ASDM 5.0



Cisco ASDM 5.0 provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or a Java Applet.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- Upgrades of the local application are performed automatically.
- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

[Download ASDM Launcher and Start ASDM](#)

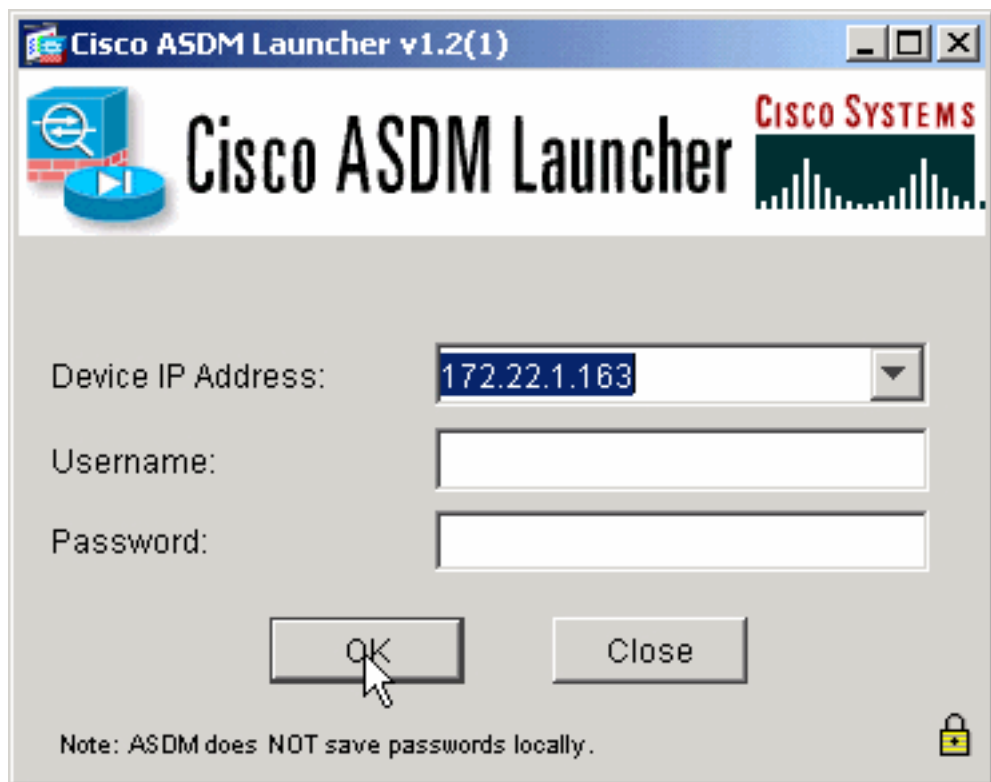
Running Cisco ASDM as a Java Applet

You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

[Run ASDM as a Java Applet](#)

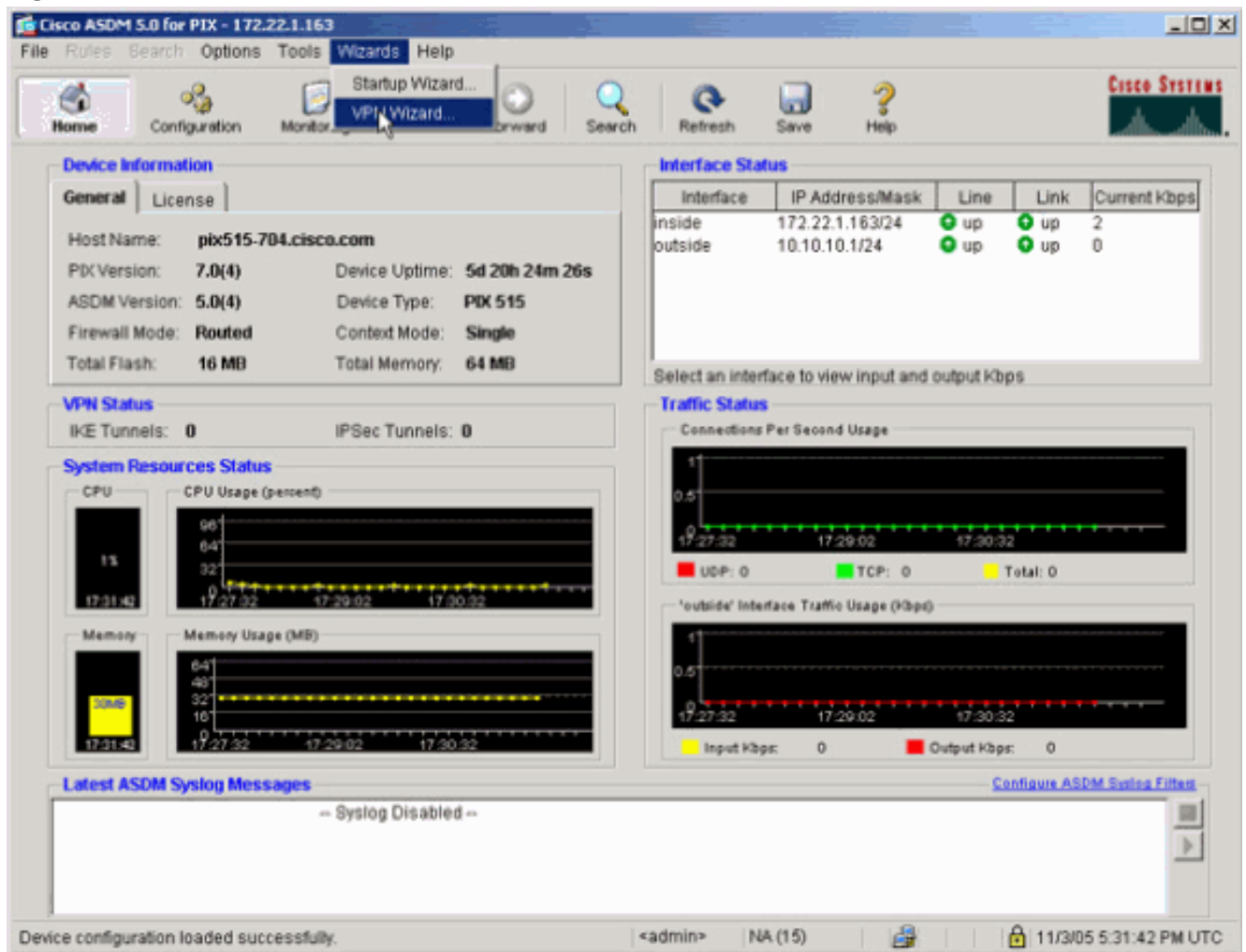
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

2. Haga clic el **activador de ASDM de la descarga** y comience el ASDM para descargar el instalador para la aplicación ASDM.
3. Una vez que el activador de ASDM descarga, complete los pasos ordenados por los prompts para instalar el software y funcionar con el Cisco ASDM launcher.
4. Ingrese el IP Address para la interfaz que usted configuró con el **HTTP** - ordene y un nombre de usuario y contraseña si usted especificó uno. Este ejemplo utiliza el nombre de usuario y contraseña en blanco

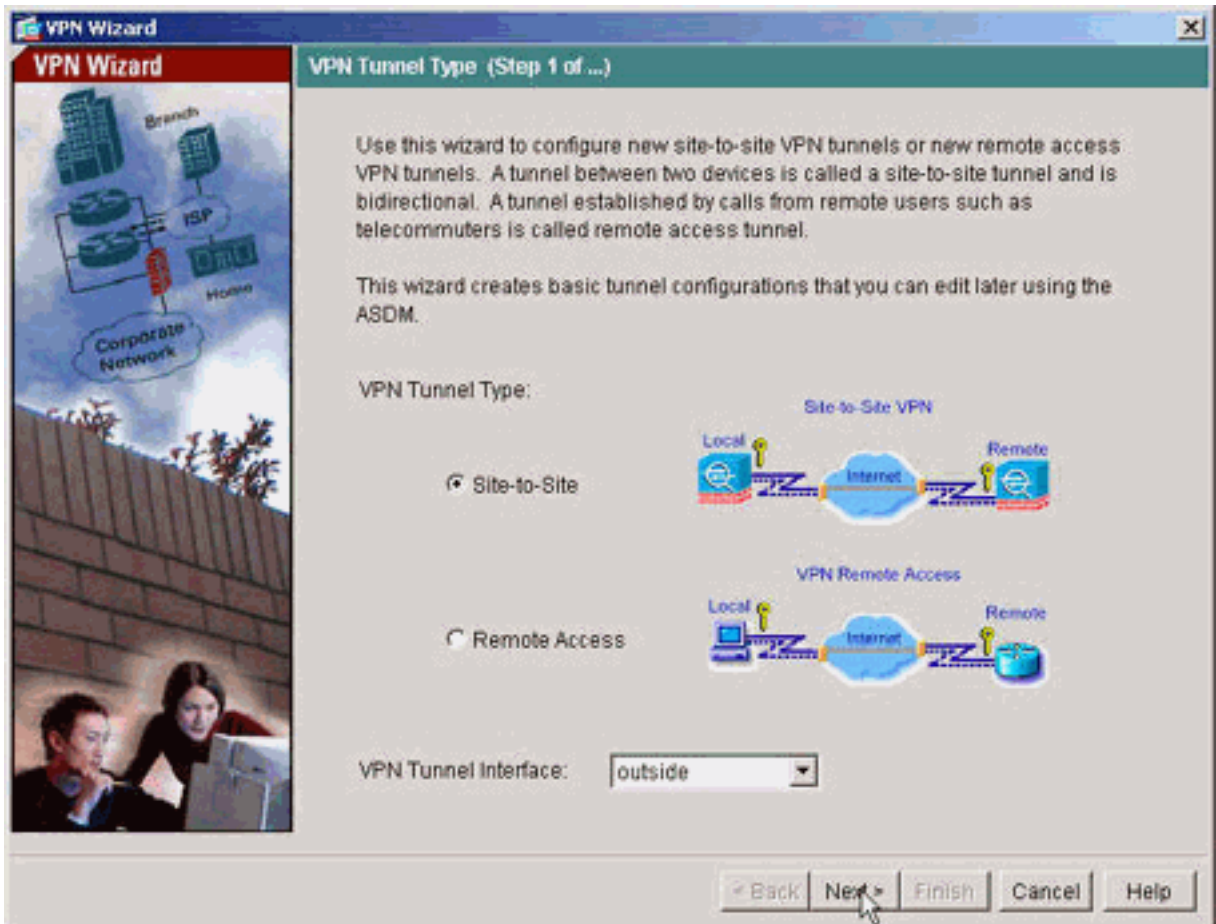


predeterminado.

5. Funcione con el Asistente VPN una vez que la aplicación ASDM conecta con el ASA.

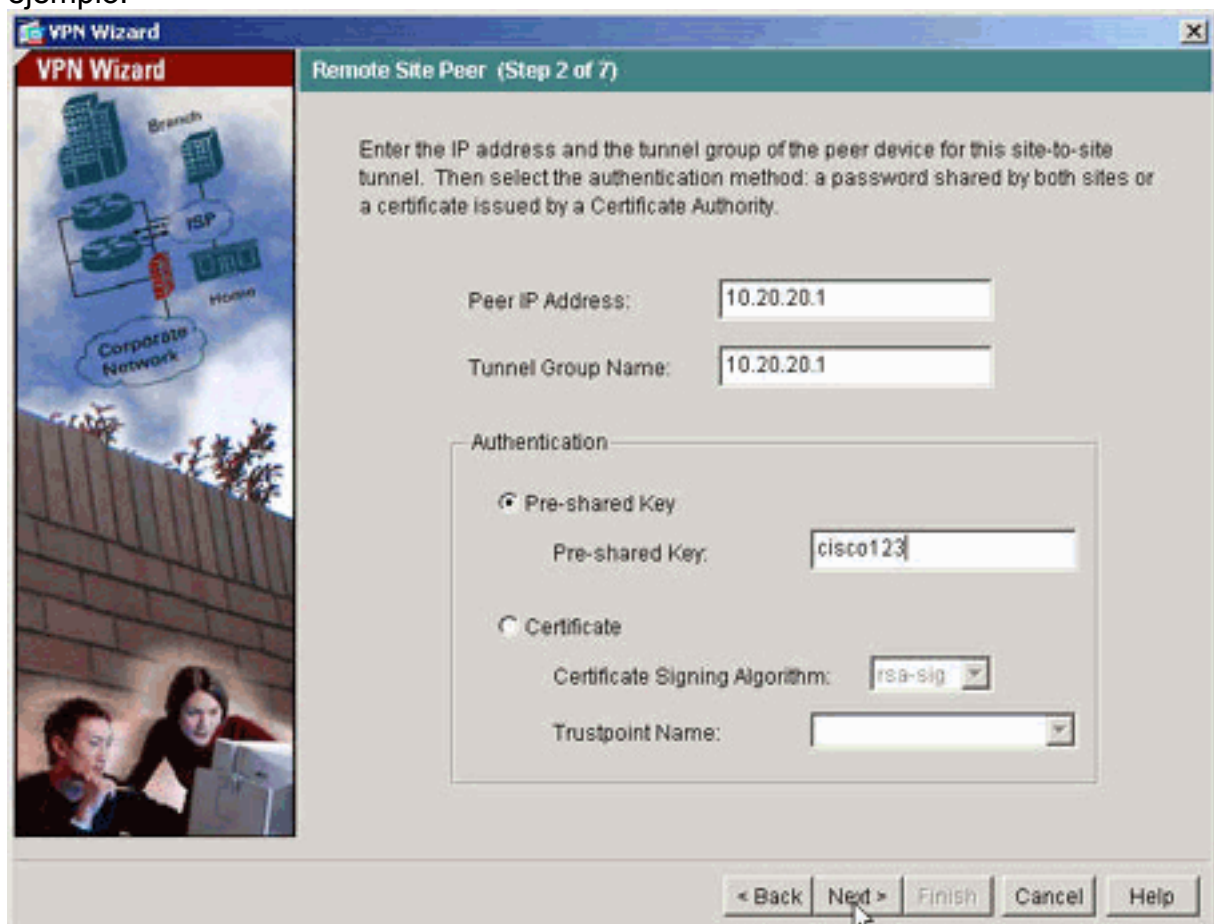


6. Elija IPsec sitio a sitio el tipo de túnel



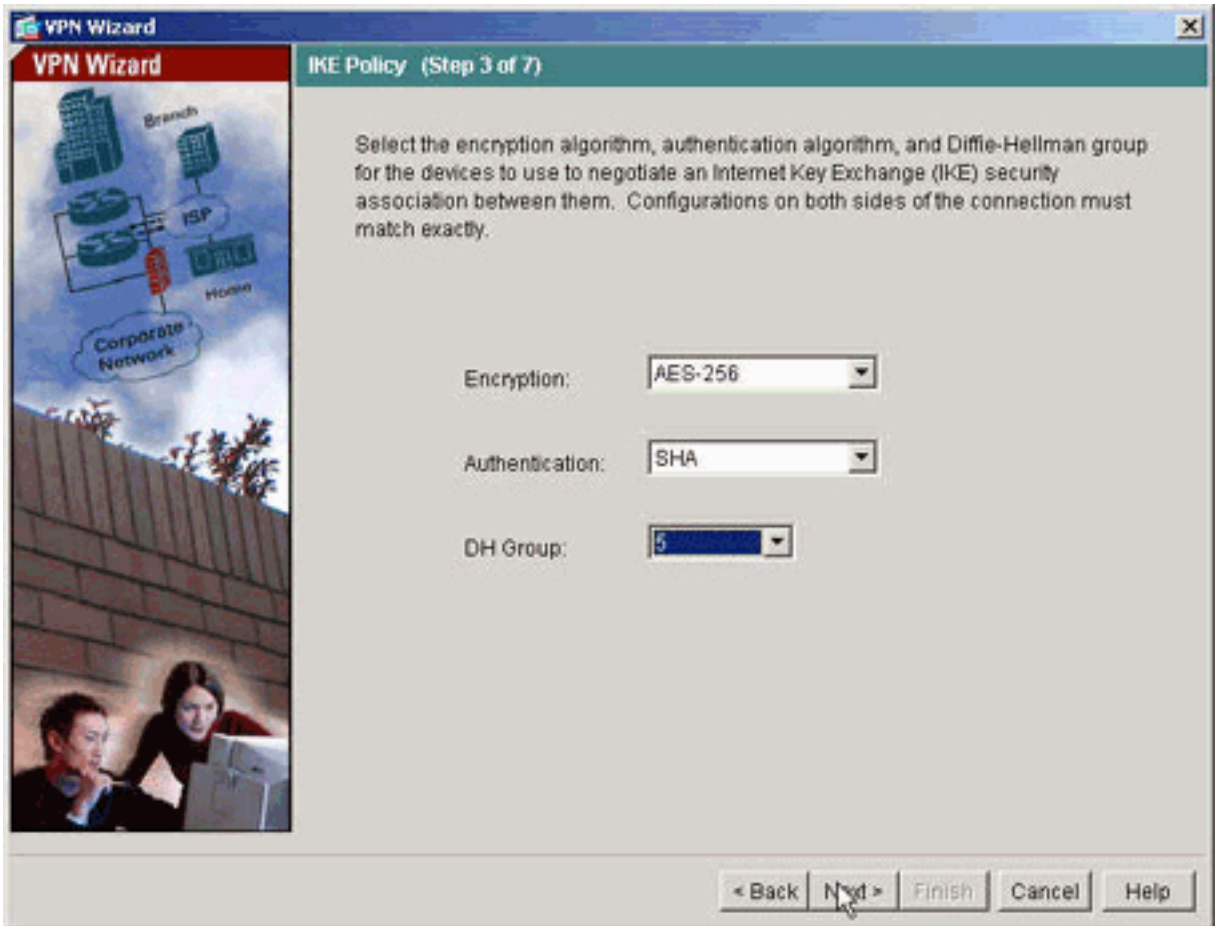
VPN.

7. Especifique el IP Address externo del peer remoto. Ingrese la información de autenticación para utilizar, que es la clave previamente compartida en este ejemplo.



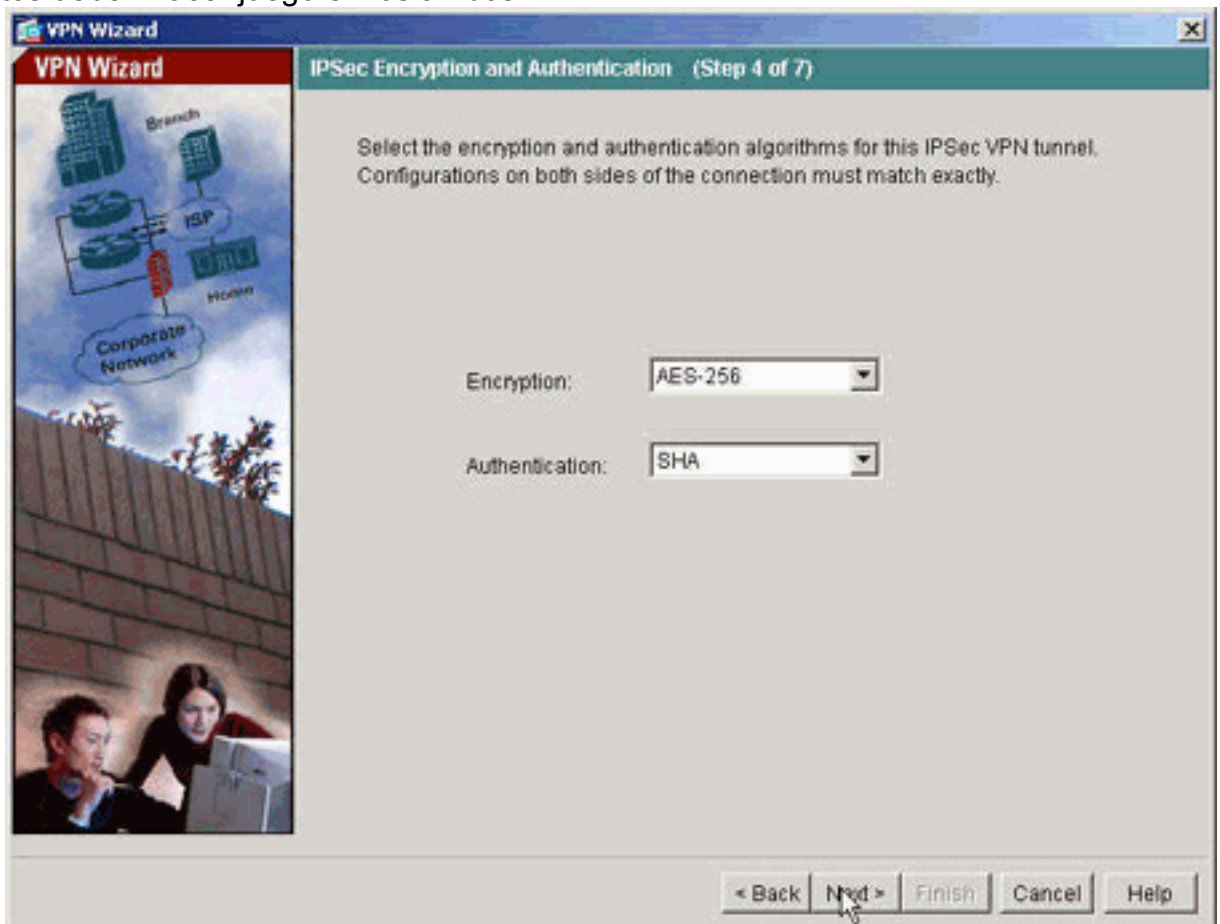
8. Especifique los atributos para utilizar para el IKE, también conocido como fase 1. Estos

atributos deben ser lo mismo a ambos lados del



túnel.

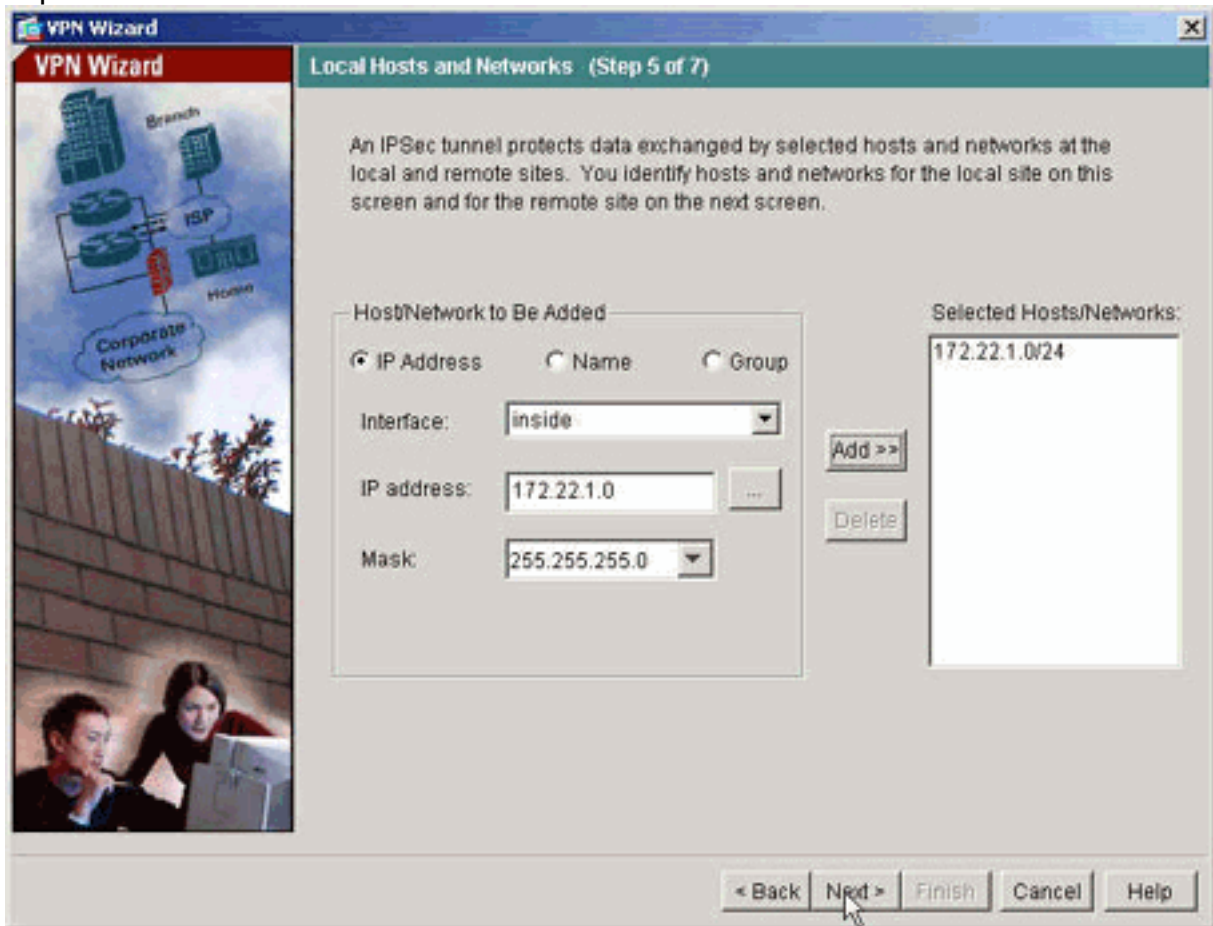
9. Especifique los atributos para utilizar para el IPSec, también conocido como fase 2. Estos atributos deben hacer juego en los ambos



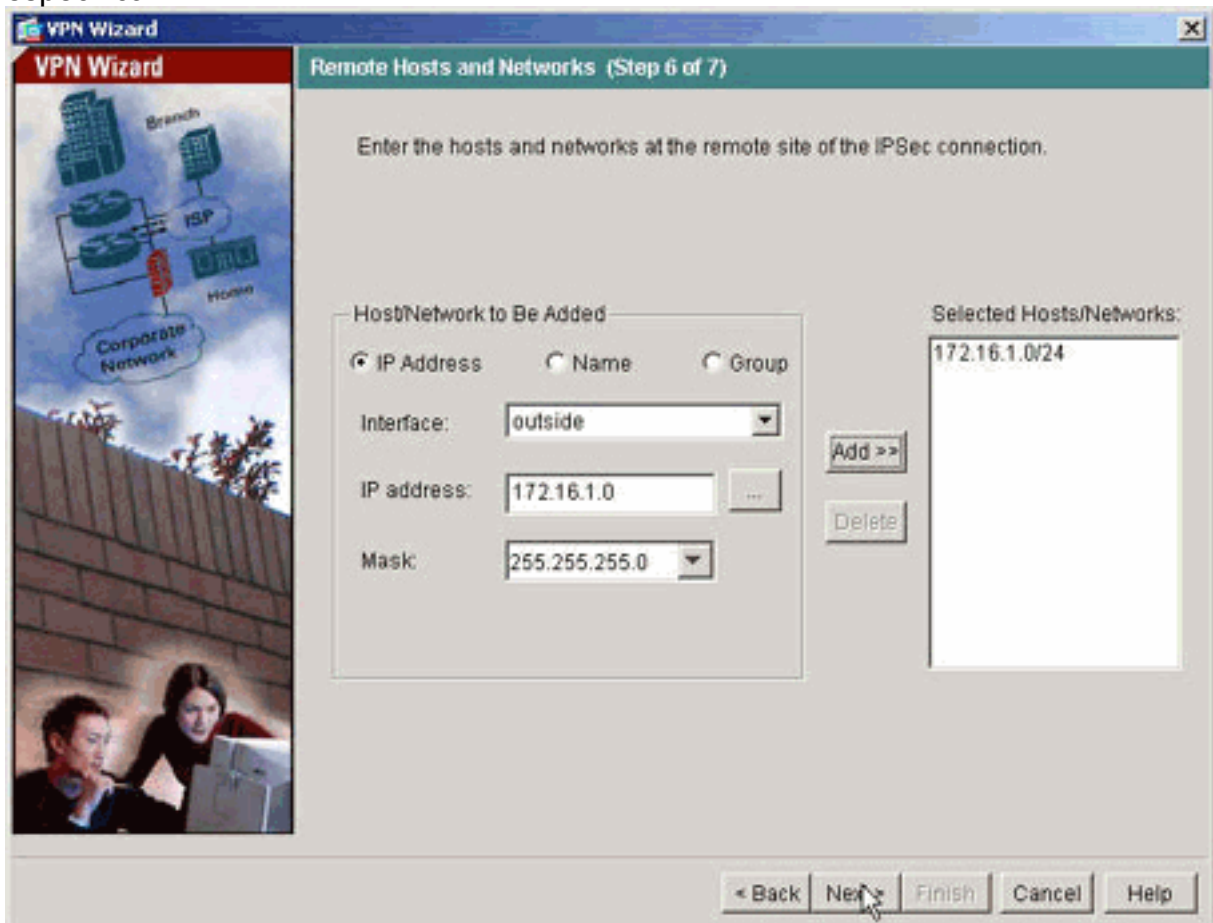
lados.

10. Especifique a los host cuyo tráfico se debe permitir pasar a través del túnel VPN. En este

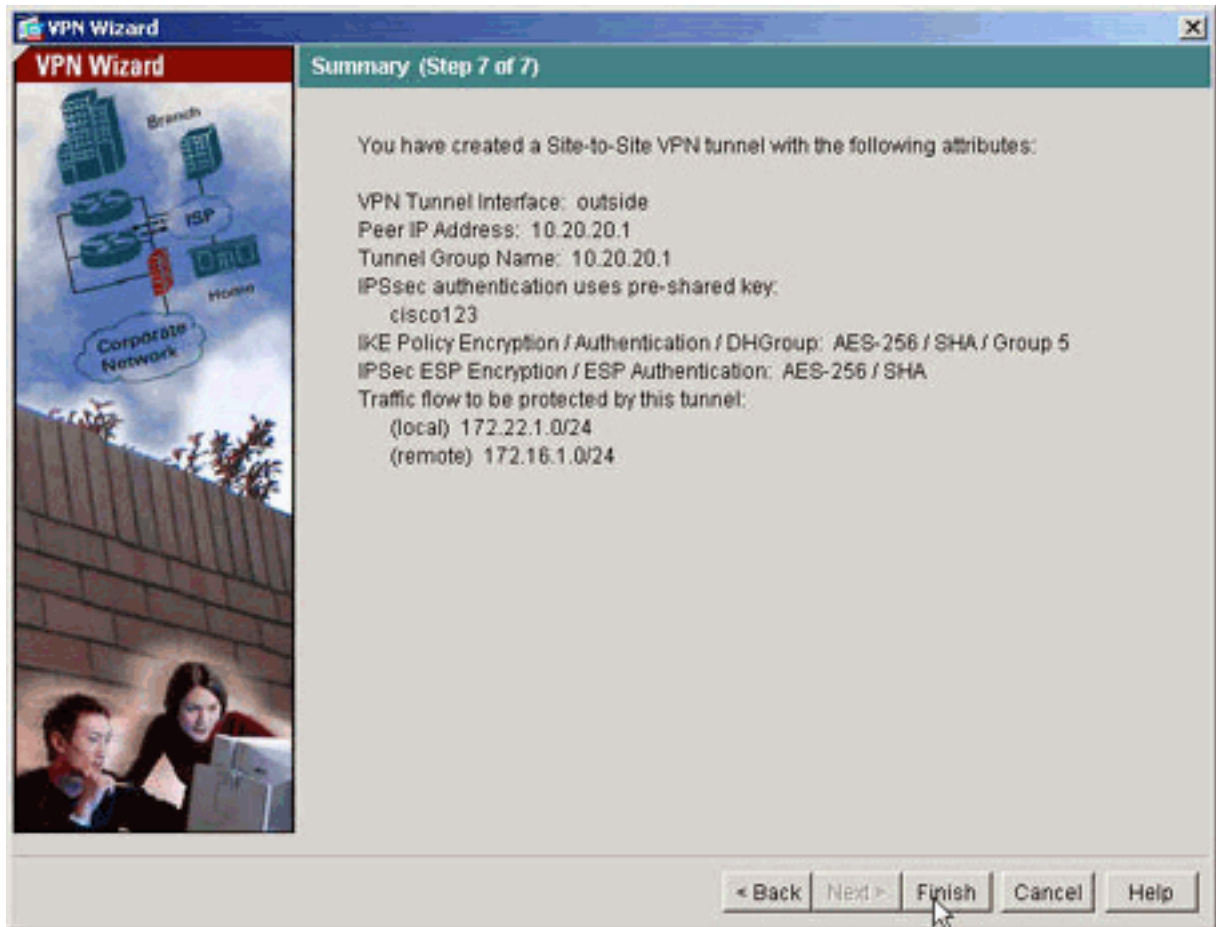
paso, los host locales a ASA1 se especifican.



11. Los host y las redes en el lado remoto del túnel se especifican.



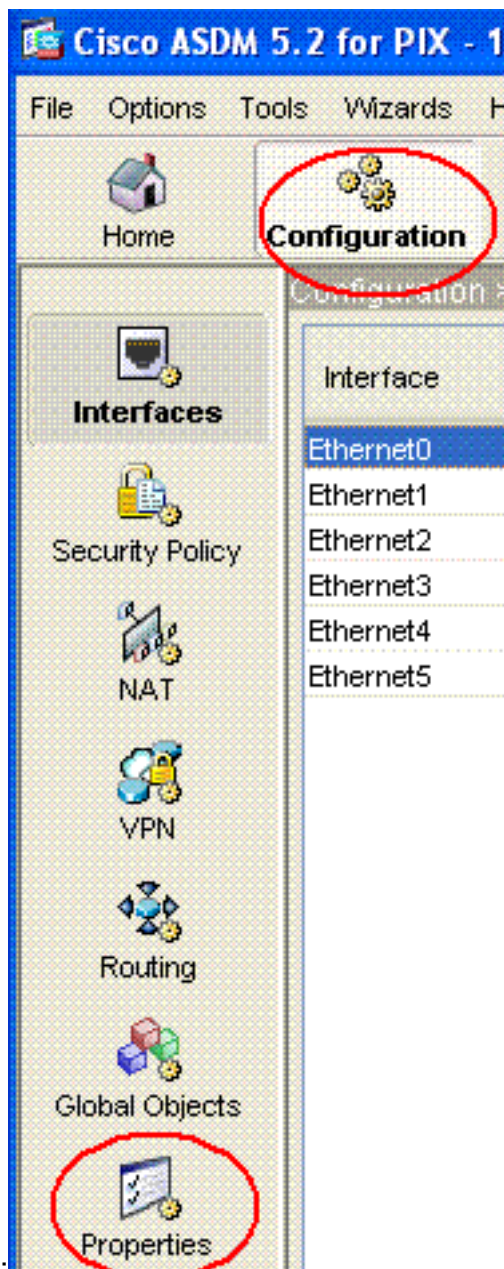
12. Los atributos definidos por el Asistente VPN se visualizan en este resumen. Compruebe la configuración con minuciosidad y el clic en Finalizar cuando le satisfacen las configuraciones está correcto.



Configuración de ASDM NTP

Complete estos pasos para configurar el NTP en el dispositivo del Cisco Security:

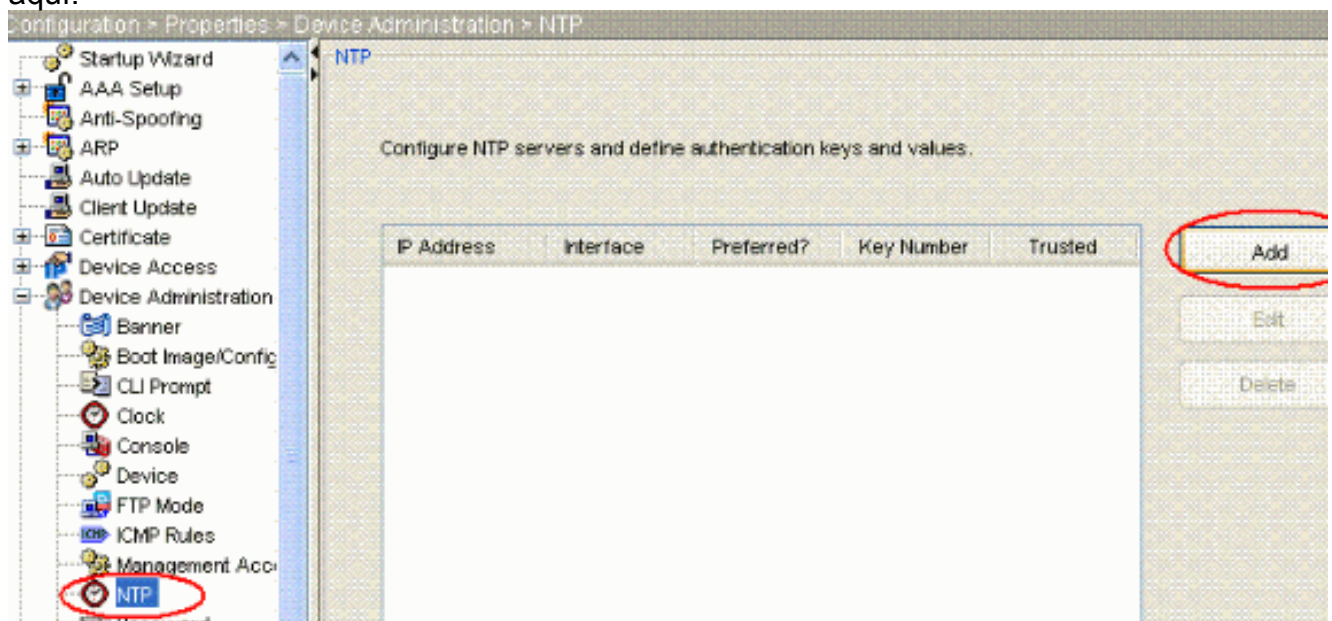
1. Elija la **configuración** en el Home Page del ASDM como se muestra



aquí:

2. Ahora elija las propiedades > la Administración de dispositivos > el NTP para abrir la página de la configuración del NTP del ASDM como se muestra

aquí:



3. Haga clic el **botón Add** para agregar a un servidor NTP y proporcionar los atributos requeridos tales como nombre del IP Address, de la interfaz (interno o externo), número y valor de la clave dominantes para Authetication en la nueva ventana que sube después de que usted haya hecho clic en el **botón Add** tal y como se muestra en de la captura de pantalla. Entonces haga clic en

The screenshot shows a dialog box titled "Add NTP Server Configuration". It contains the following fields and controls:

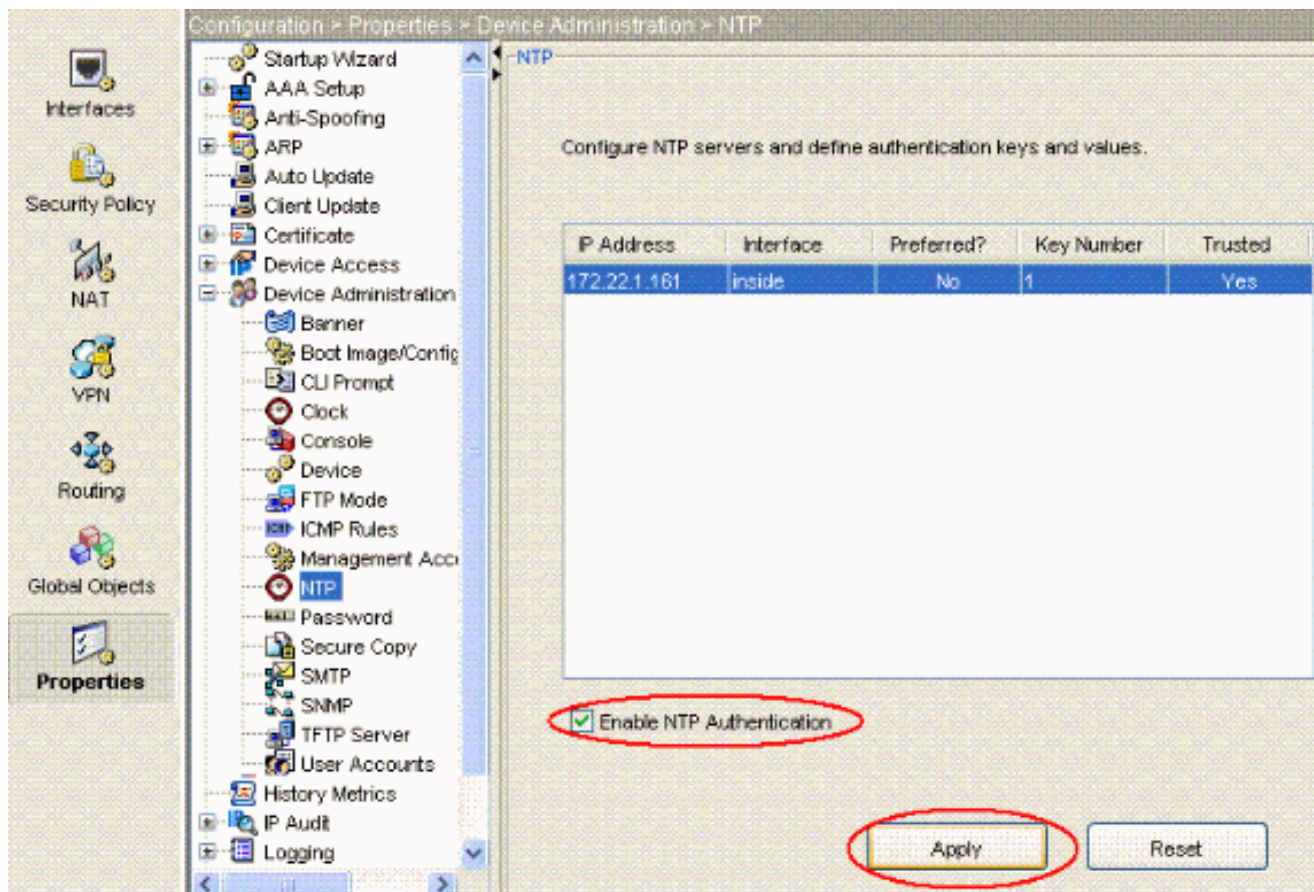
- IP Address: 172.22.1.161
- Interface: inside
- Key Number: 1
- Key Value: *****
- Reenter Key Value: *****
- Preferred:
- Trusted:
- Buttons: OK, Cancel, Help

OK.

No

ta: El nombre de la interfaz se debe elegir como dentro para ASA1 y el exterior para ASA2.**Nota: Autenticación NTP el dominante** debe ser lo mismo en el ASA y el servidor NTP.La configuración del atributo de Authetication en el cli para ASA1 y ASA2 se muestran abajo: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. Ahora haga clic el **permiso del checkbox autenticación NTP** y el tecleo **se aplica**, que completa la tarea de la configuración del NTP.



Configuración CLI ASA1

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
```

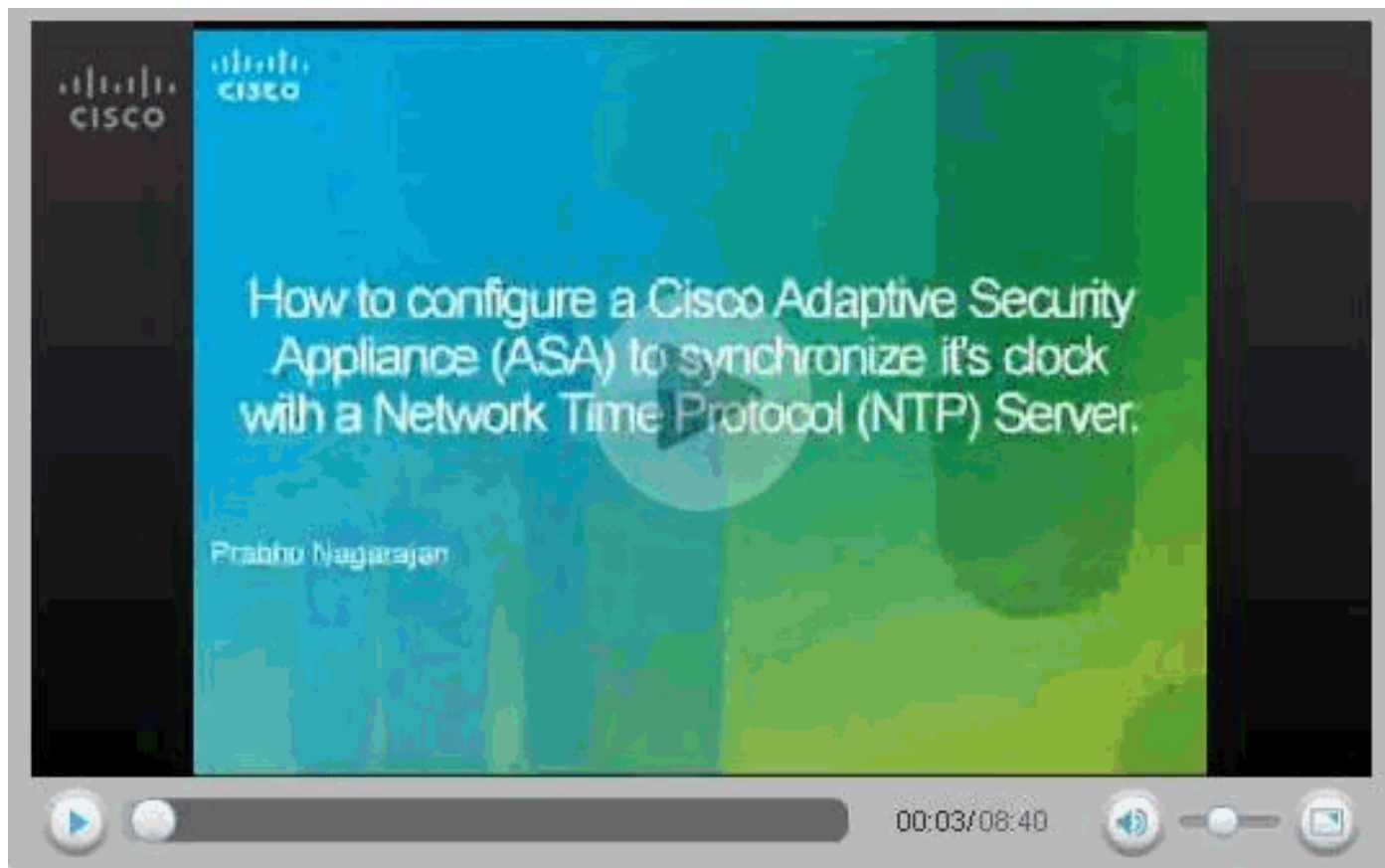
```

!--- 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
esmtplib inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
!--- Define the NTP server authentication-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

```

programa, el procedimiento para configurar el ASA como cliente NTP:

[Cómo configurar un dispositivo de seguridad adaptante de Cisco \(ASA\) para sincronizar su reloj con un servidor del Network Time Protocol \(NTP\).](#)



Configuración CLI ASA2

```
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 authentication-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#

```

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- [muestre a se muestra el estados NTP la](#) información del reloj 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 detail](#) — Visualiza las asociaciones del Servidor de tiempo de la red configurada. `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 filtererror = 15.63 16.60 17.58 14904.3 14904.3 14904.3 14904.3 14904.3
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: [Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.](#)

- **haga el debug de la validez NTP** — Validez del reloj del par de las visualizaciones NTP.Ésta es salida de los debugs de la discrepancia de clave:

```
NTP: packet from 172.22.1.161 failed validity tests 10 Authentication failed
```

- **paquete NTP del debug** — Información del paquete NTP de las visualizaciones.Cuando no hay respuesta del servidor, sólo paquete xmit NTP se ve en el ASA sin el paquete rcv 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)
```

Información Relacionada

- [Cisco PIX Firewall Software](#)
- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)