ASA/PIX: NTP mit und ohne IPsec-Tunnel-Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Synchronisierung der PIX/ASA Security Appliance-Uhr mit einem Netzwerkzeitserver mithilfe von Network Time Protocol (NTP). ASA1 kommuniziert direkt mit dem Netzwerkzeitserver.ASA2 leitet NTP-Datenverkehr über einen IPsec-Tunnel an ASA1 weiter, der die Pakete wiederum an den Netzwerkzeitserver weiterleitet.

Weitere Informationen finden Sie unter ASA 8.3 und höher: NTP mit und ohne IPsec-Tunnel-Konfigurationsbeispiel für weitere Informationen zur identischen Konfiguration auf der Cisco ASA mit Version 8.3 und höher.

Hinweis: Ein Router kann auch als NTP-Server zum Synchronisieren der PIX/ASA Security Appliance-Uhr verwendet werden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Vor Beginn dieser NTP-Konfiguration muss eine End-to-End-IPsec-Verbindung eingerichtet werden.
- Die Security Appliance-Lizenz muss für die DES-Verschlüsselung (Data Encryption Standard) aktiviert werden (mindestens auf Verschlüsselungsebene).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco Adaptive Security Appliance (ASA) ab Version 7.x
- ASDM Version 5.x.x und höher

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance der Serie PIX 500 verwendet werden, die Version 7.x und höher ausführt.

Hinweis: NTP-Unterstützung wurde in PIX Version 6.2 hinzugefügt. Siehe PIX 6.2: NTP mit und ohne IPsec-Tunnel-Konfigurationsbeispiel zur Konfiguration von NTP in der Cisco PIX-Firewall.

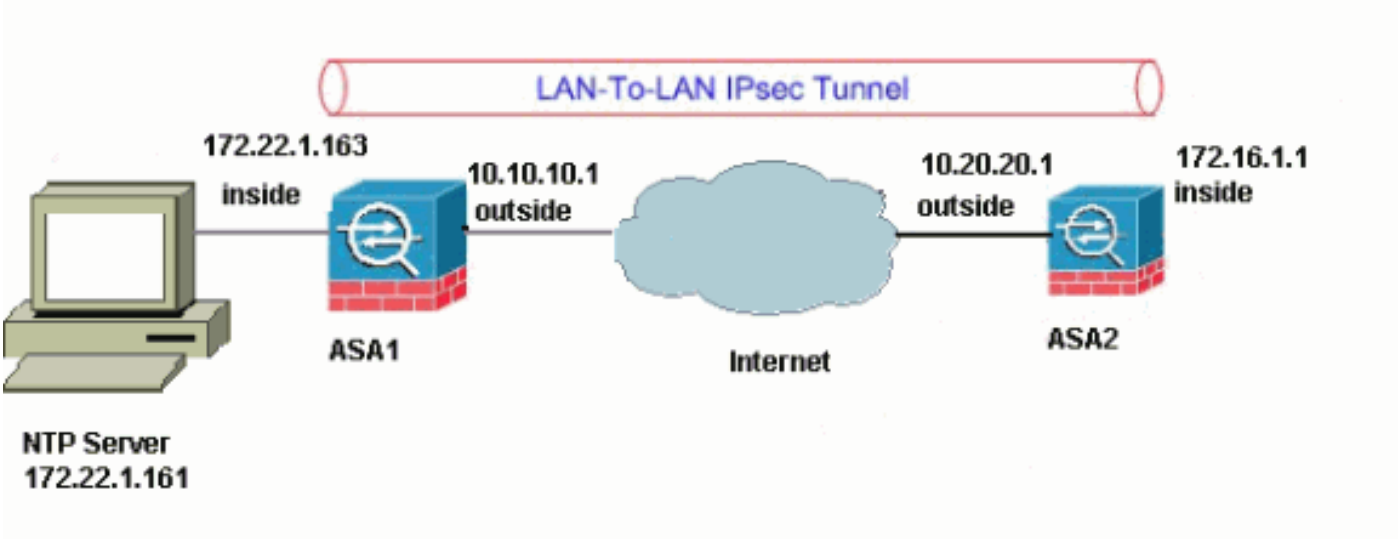
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.

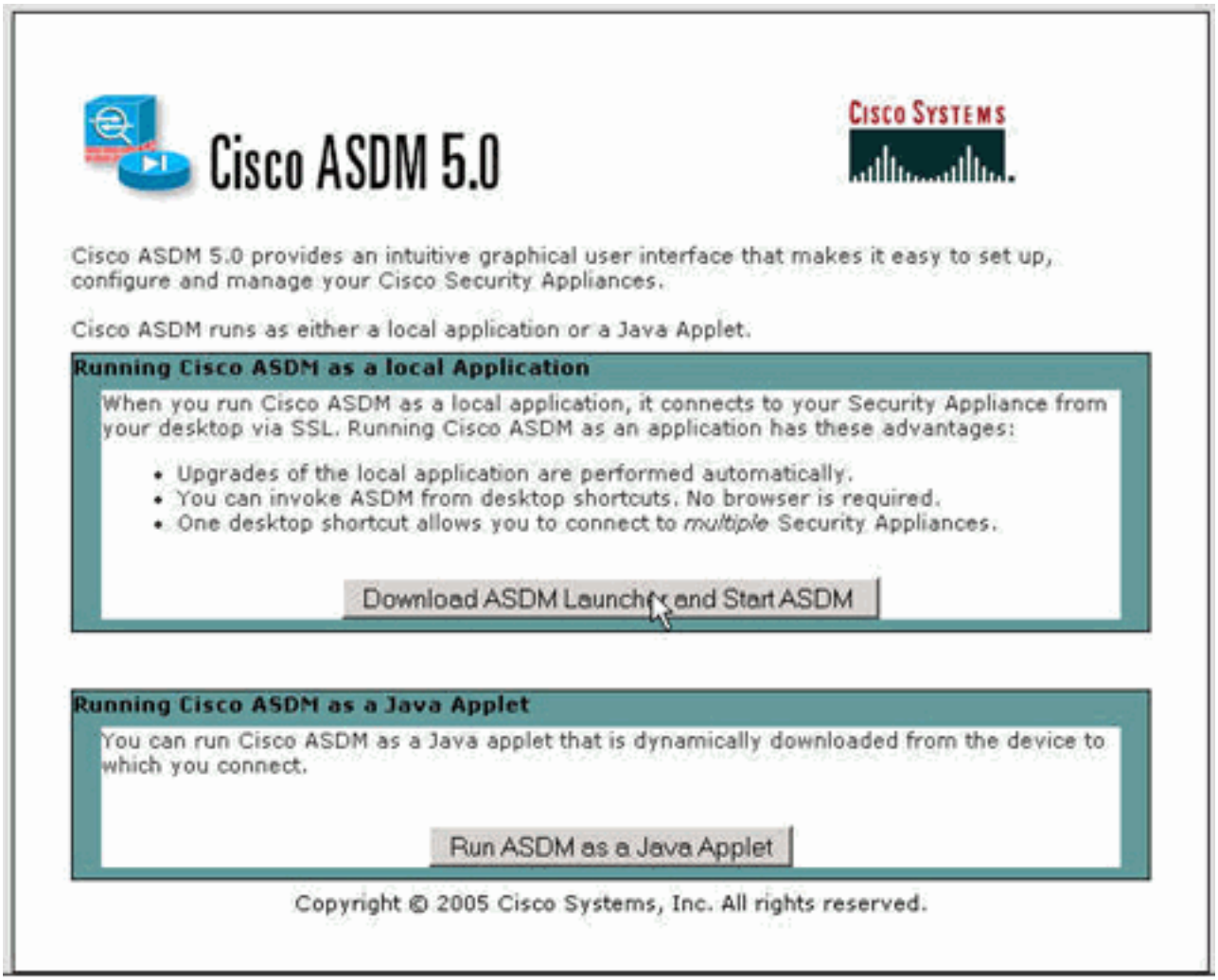


Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet werden.

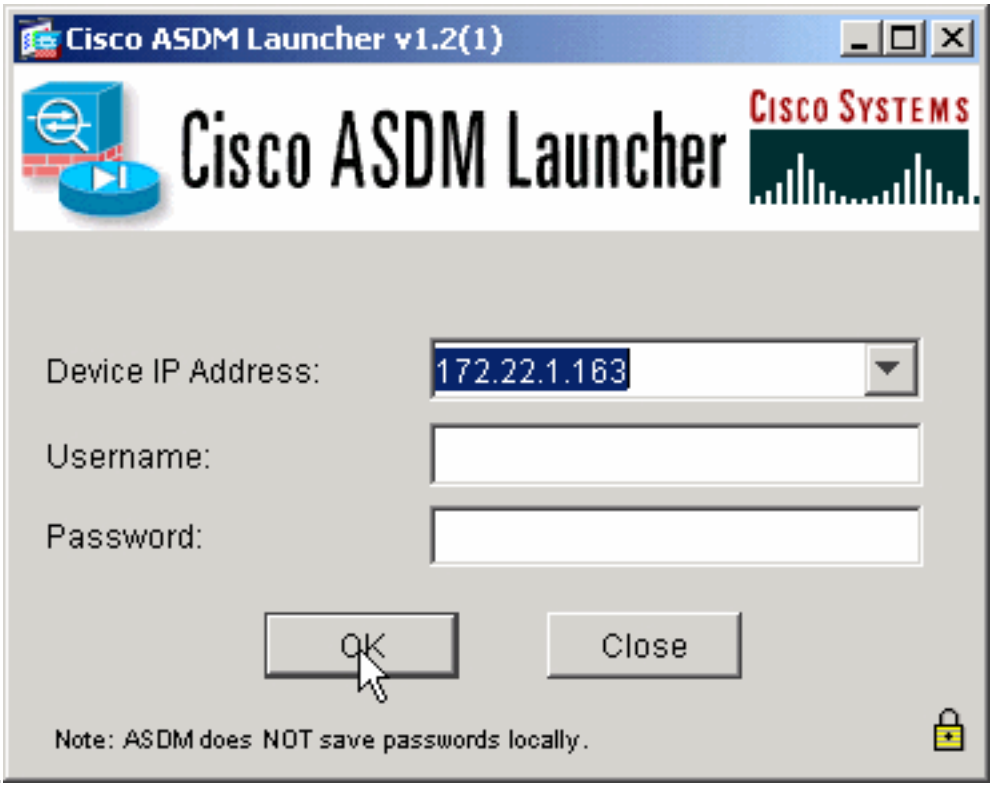
ASDM-Konfiguration für VPN-Tunnel

Gehen Sie wie folgt vor, um den VPN-Tunnel zu erstellen:

1. Öffnen Sie Ihren Browser, und geben Sie **https://<Inside_IP_Address_of_ASA>** ein, um auf das ASDM auf der ASA zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Die ASA präsentiert dieses Fenster, um den Download der ASDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet
ausgeführt.

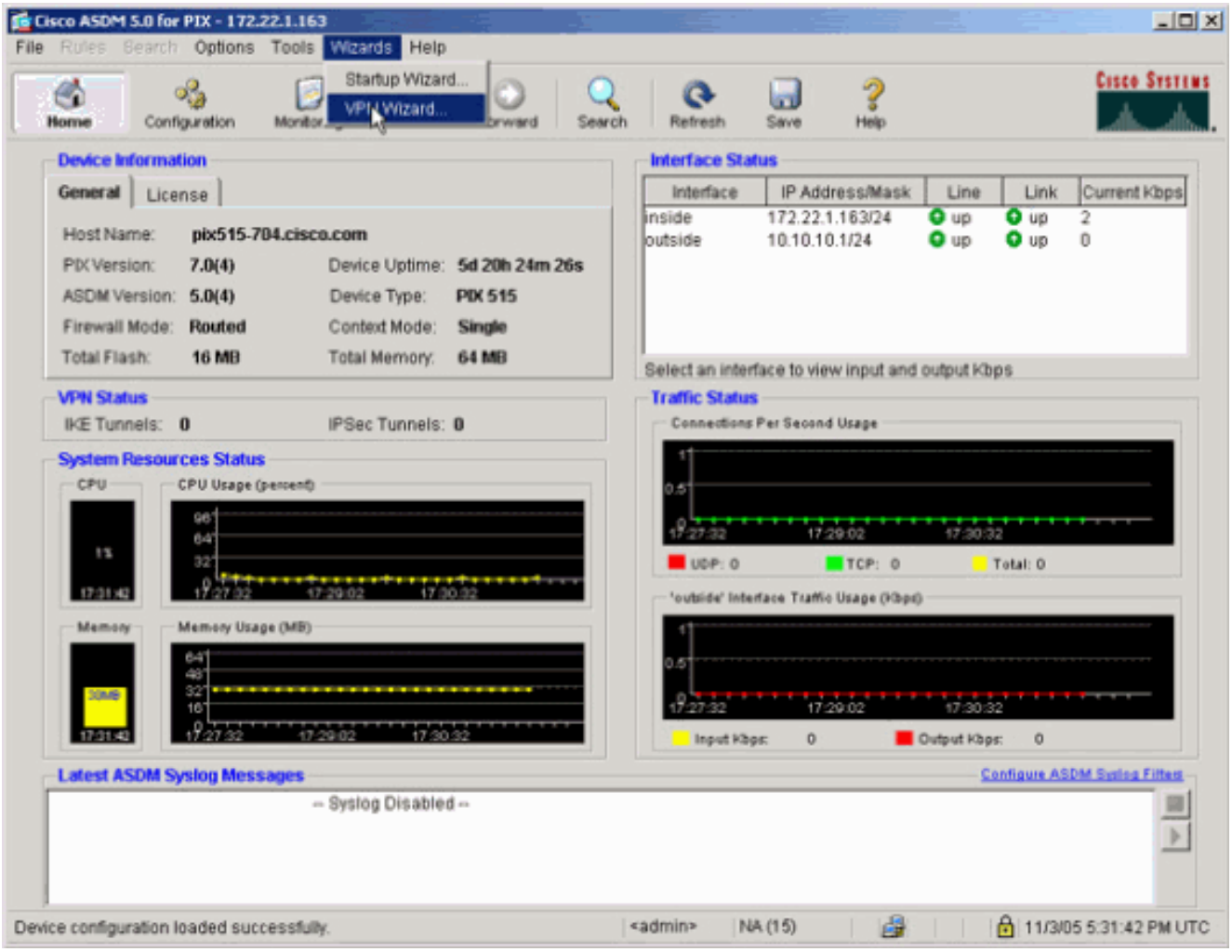


2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
3. Wenn der ASDM Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen zur Installation der Software und Ausführung des Cisco ASDM Launchers ausgeführt werden.
4. Geben Sie die IP-Adresse für die Schnittstelle ein, die Sie mit dem Befehl **http** konfiguriert haben, sowie einen Benutzernamen und ein Kennwort, wenn Sie einen Befehl angegeben haben.In diesem Beispiel werden ein leerer Benutzername und ein leeres Kennwort

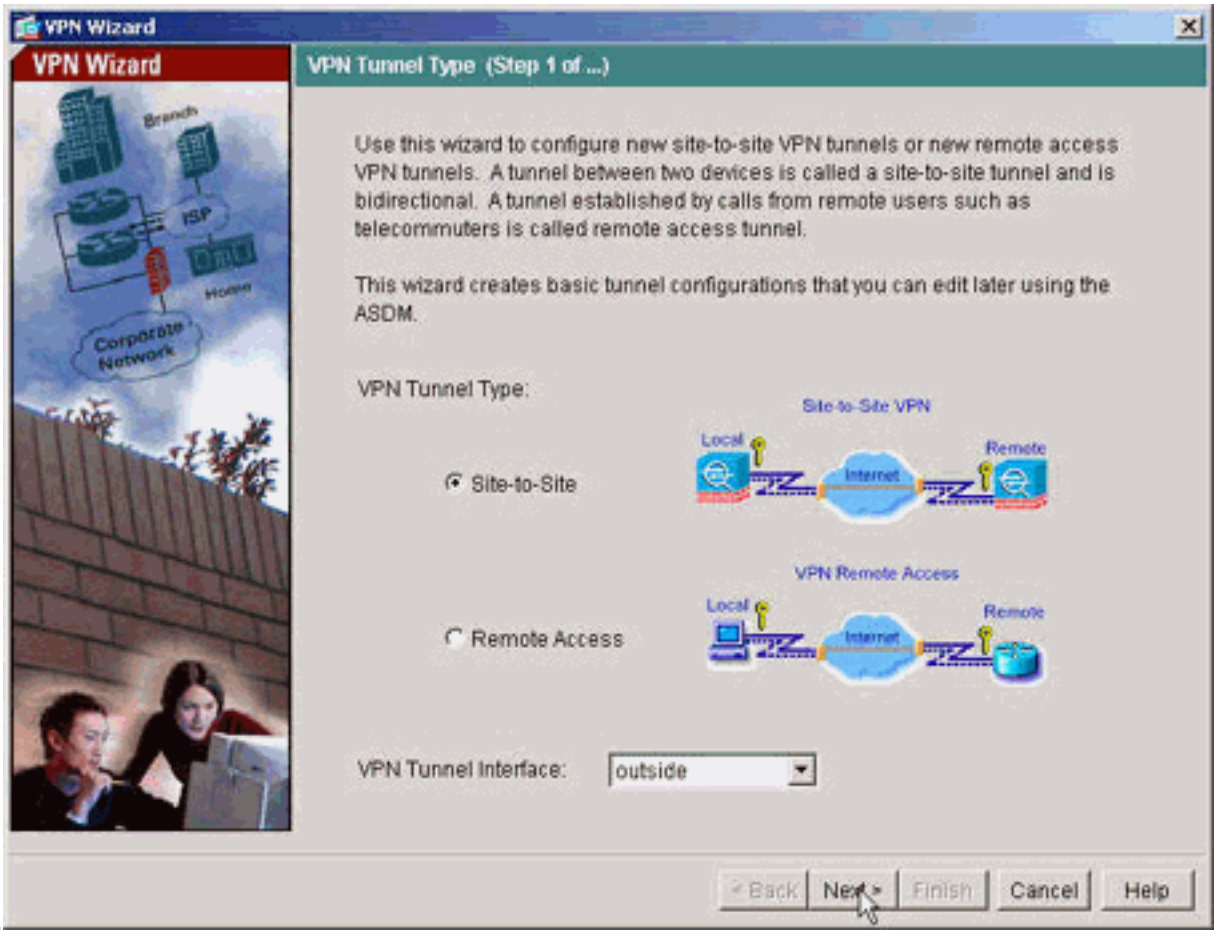


verwendet.

5. Führen Sie den VPN-Assistenten aus, sobald die ASDM-Anwendung eine Verbindung mit der ASA
herstellt.

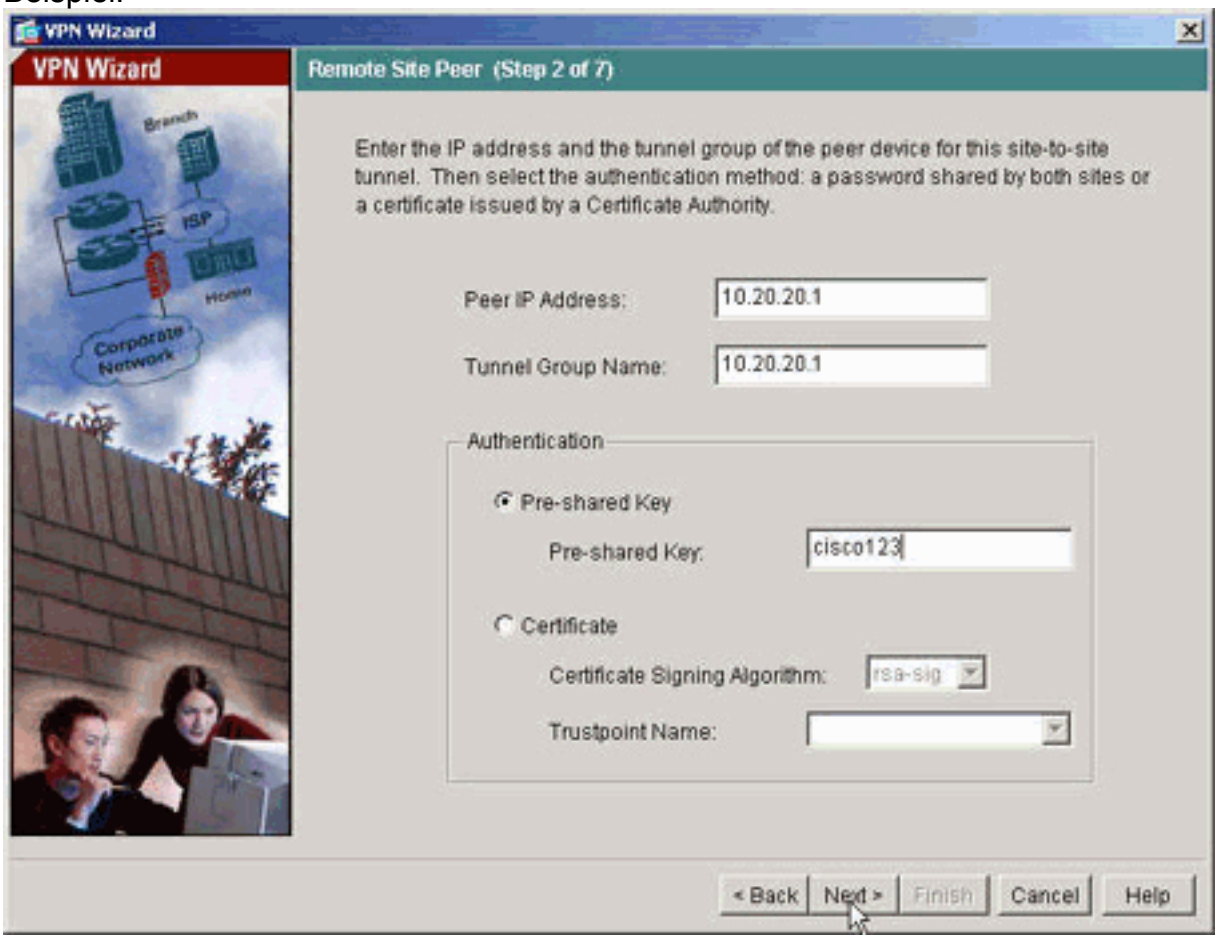


6. Wählen Sie den **Site-to-Site**-IPsec VPN-Tunneltyp



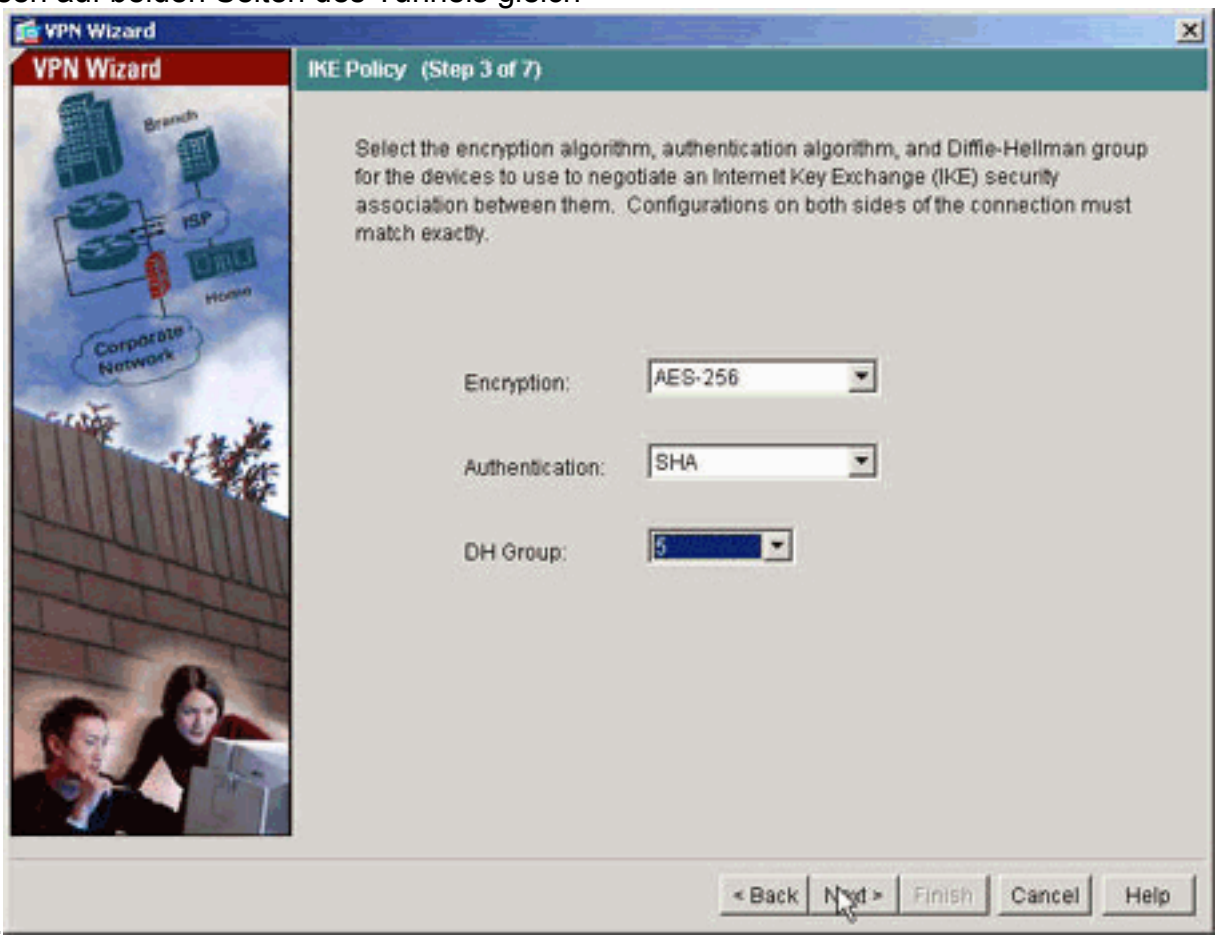
aus.

7. Geben Sie die externe IP-Adresse des Remote-Peers an. Geben Sie die zu verwendenden Authentifizierungsinformationen ein, d. h. den vorinstallierten Schlüssel in diesem Beispiel.

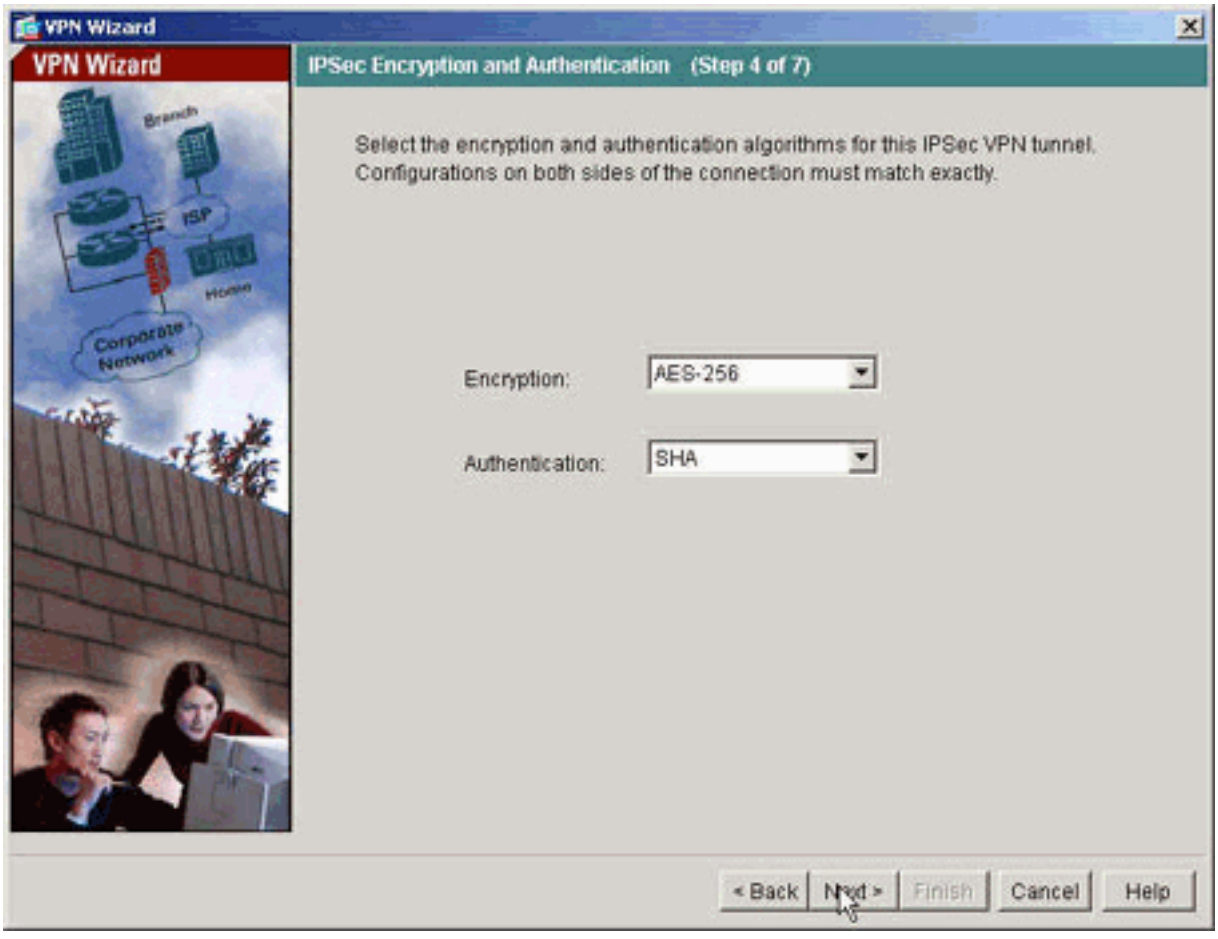


8. Geben Sie die Attribute für IKE an, die auch als Phase 1 bezeichnet werden. Diese Attribute

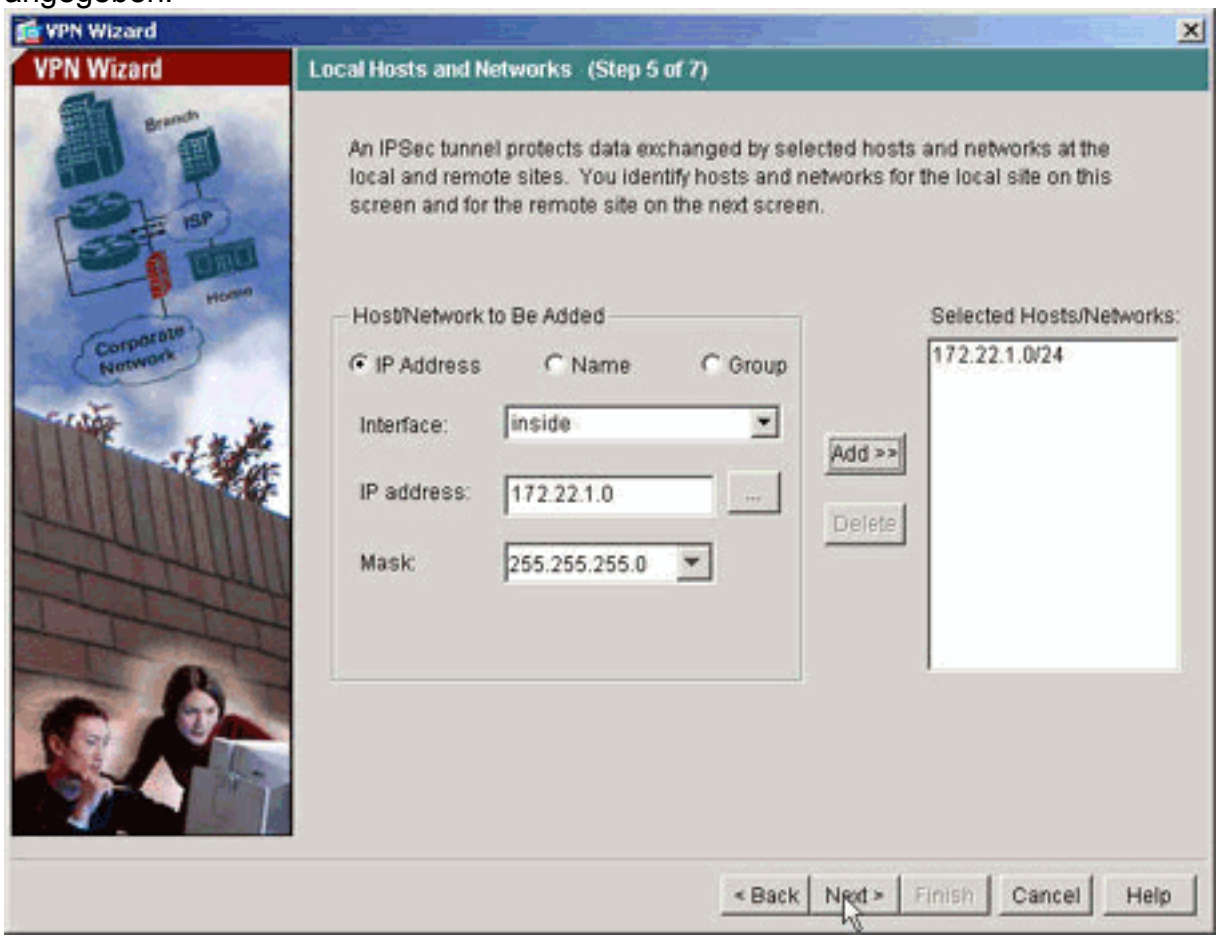
müssen auf beiden Seiten des Tunnels gleich sein.



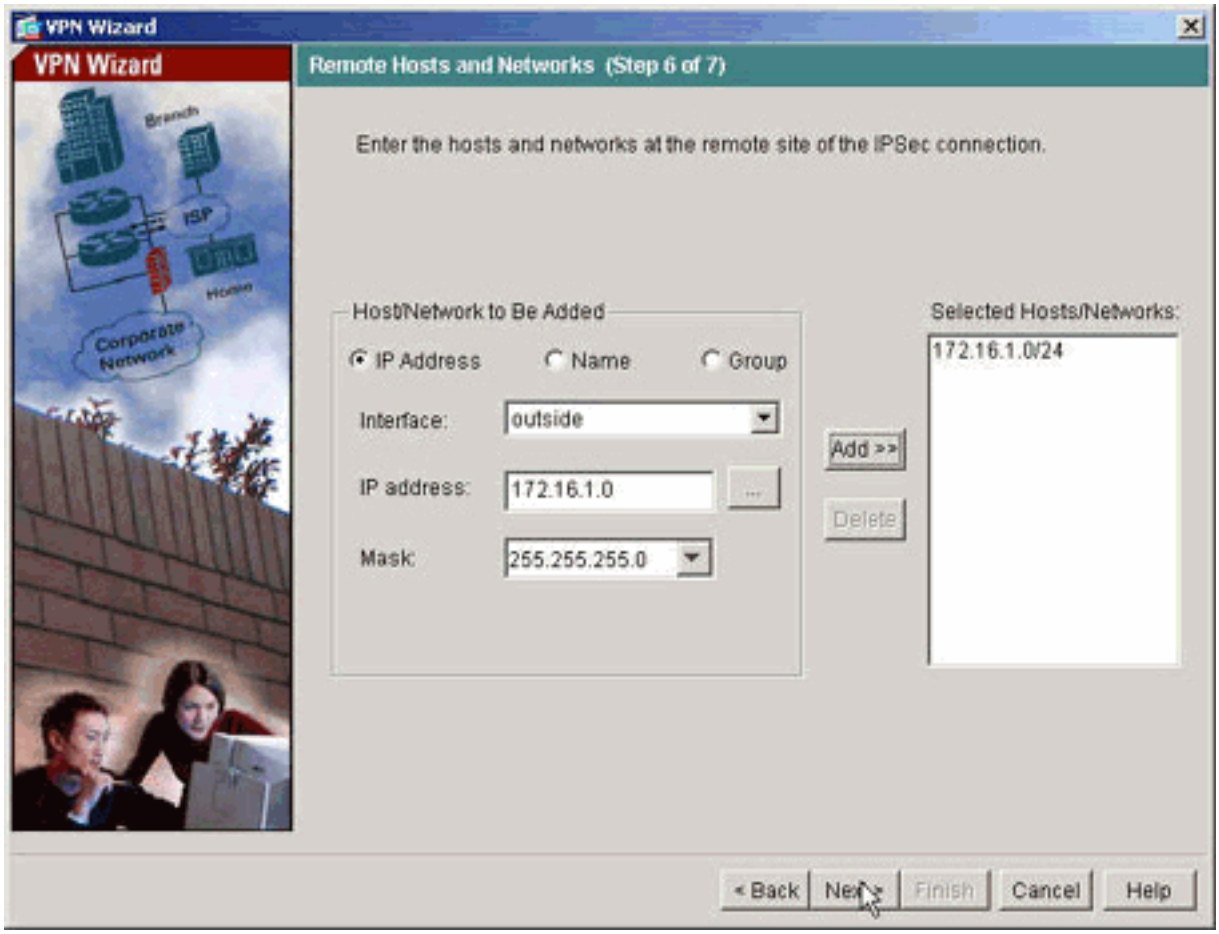
9. Geben Sie die Attribute an, die für IPsec verwendet werden sollen, auch als Phase 2 bezeichnet. Diese Attribute müssen auf beiden Seiten übereinstimmen.



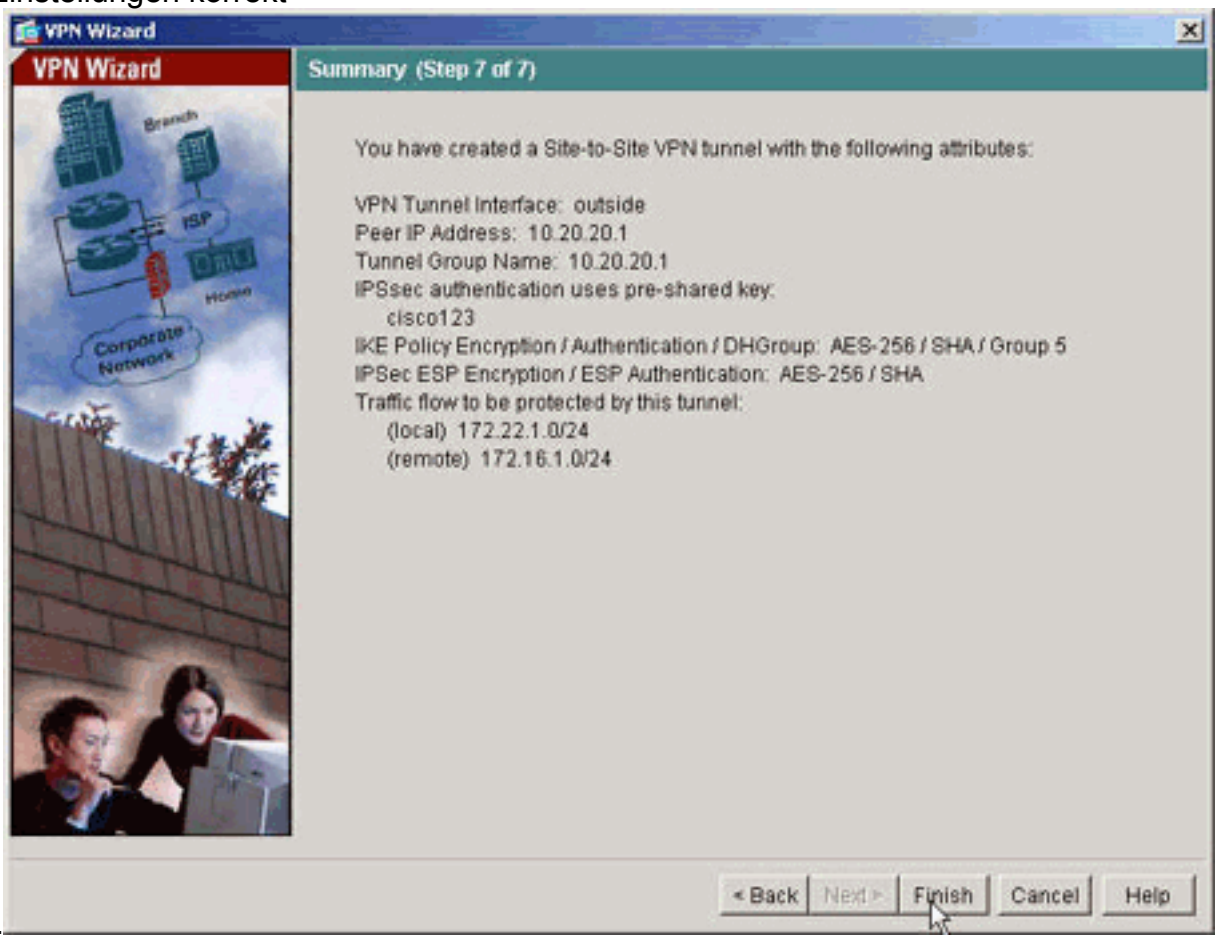
10. Geben Sie die Hosts an, deren Datenverkehr den VPN-Tunnel passieren darf. In diesem Schritt werden die lokalen Hosts für ASA1 angegeben.



11. Die Hosts und Netzwerke auf der Remote-Seite des Tunnels werden angegeben.



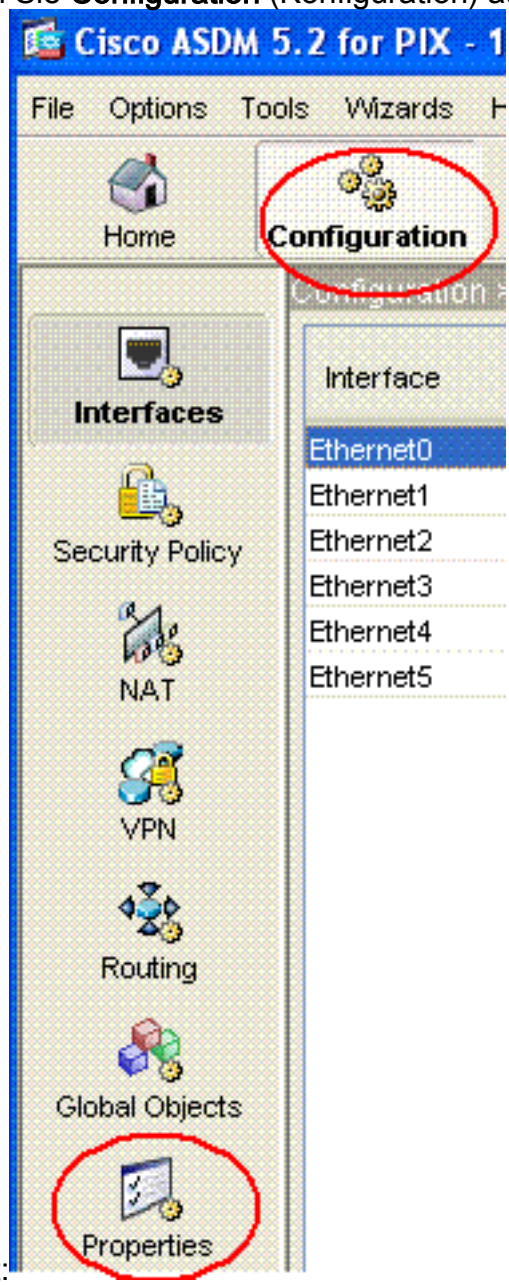
12. Die vom VPN-Assistenten definierten Attribute werden in dieser Zusammenfassung angezeigt. Überprüfen Sie die Konfiguration erneut, und klicken Sie auf **Fertig stellen**, wenn die Einstellungen korrekt sind.



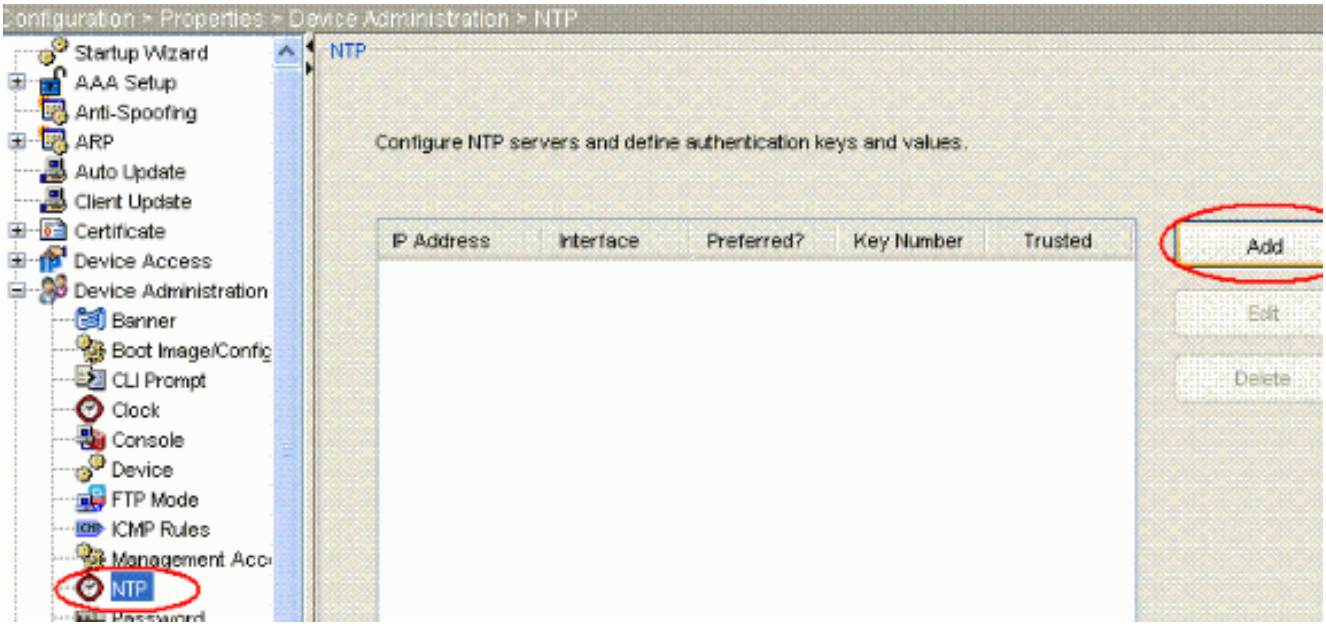
NTP ASDM-Konfiguration

Gehen Sie wie folgt vor, um NTP auf der Cisco Security Appliance zu konfigurieren:

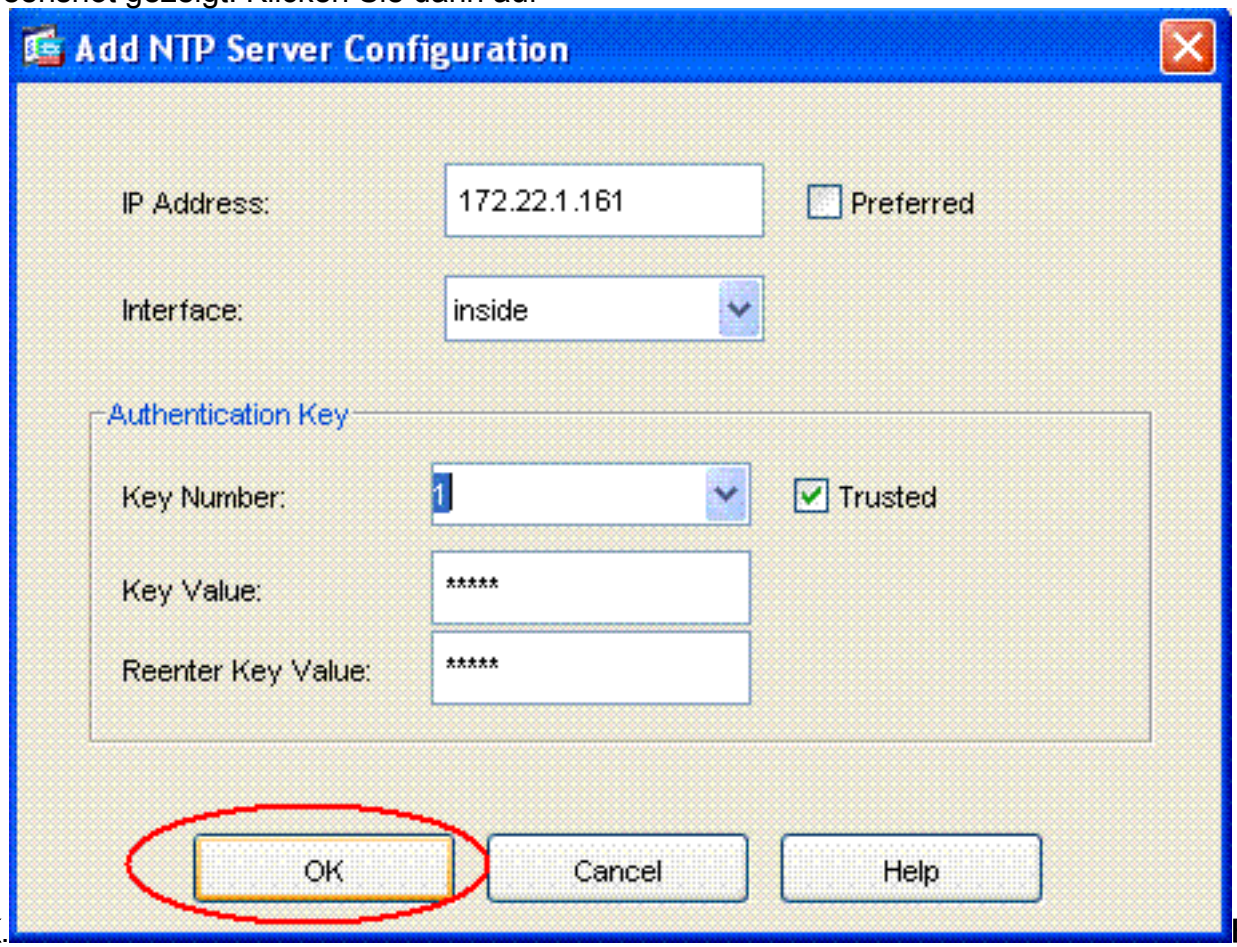
1. Wählen Sie **Configuration** (Konfiguration) auf der ASDM-Startseite aus, wie hier gezeigt:



2. Wählen Sie jetzt **Eigenschaften > Gerätemanagement > NTP**, um die **NTP-**Konfigurationsseite von ASDM zu öffnen, wie hier gezeigt:



3. Klicken Sie auf die Schaltfläche **ADD**, um einen NTP-Server hinzuzufügen und die erforderlichen Attribute wie IP-Adresse, Schnittstellenname (innen oder außen), Schlüsselnummer und Schlüsselwert für die Authentifizierung im neuen Fenster anzugeben, das angezeigt wird, nachdem Sie auf die Schaltfläche **ADD** geklickt haben, wie im Screenshot gezeigt. Klicken Sie dann auf

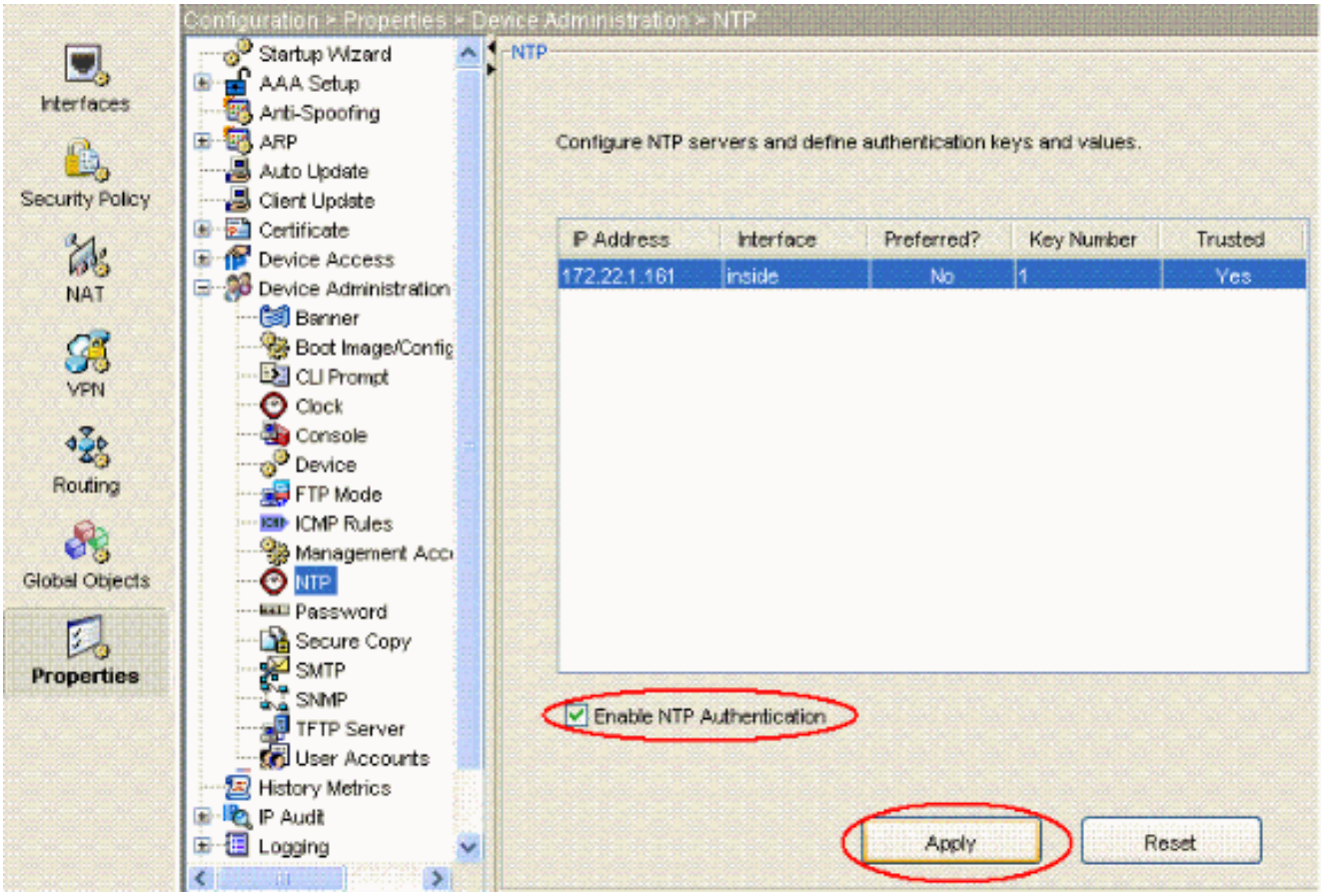


OK.**Hinweis:** Der Schnittstellenname sollte wie innen für ASA1 und außen für ASA2 ausgewählt werden.**Hinweis:** Der **NTP-Authentifizierungsschlüssel** muss in ASA und dem NTP-Server identisch sein.Die Konfiguration des Authentifizierungs-Attributs in CLI für ASA1 und ASA2 ist nachfolgend dargestellt:

```
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. Klicken Sie jetzt auf das Kontrollkästchen **NTP-Authentifizierung aktivieren** und dann auf **Übernehmen**, um die NTP-Konfigurationsaufgabe abzuschließen.



ASA1 CLI-Konfiguration

ASA1

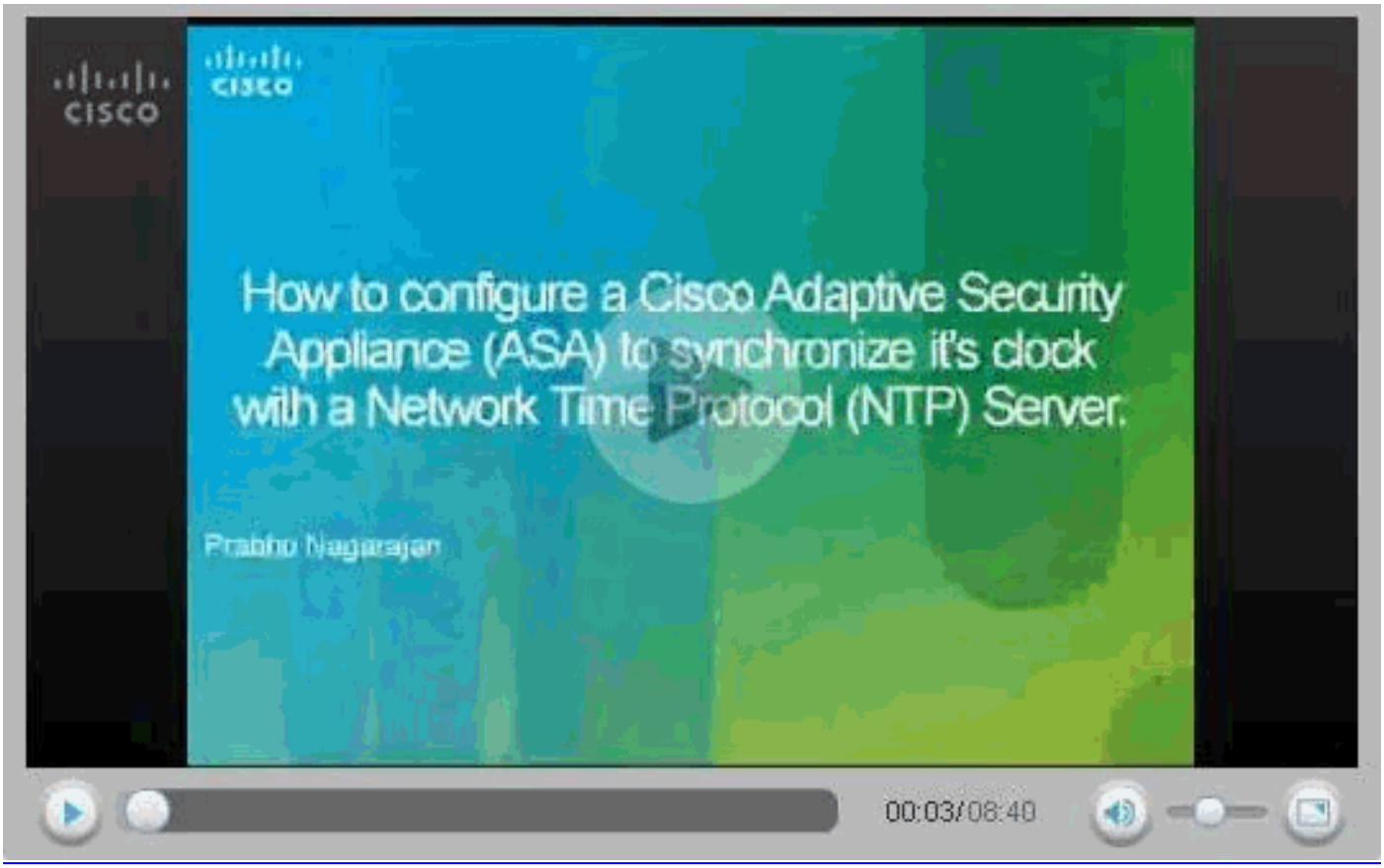
```
ASA#show run
: Saved
ASA Version 7.1(1)
!
hostname ASA1
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
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
```

In diesem Video, das auf der Cisco Support Community veröffentlicht wurde, wird das Verfahren zur Konfiguration von ASA als NTP-Client in einer Demo erläutert:

Konfigurieren einer Cisco Adaptive Security Appliance (ASA) zur Synchronisierung der Uhr mit einem NTP-Server (Network Time Protocol)



CLI-Konfiguration für 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 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#
```

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show ntp status** (NTP-Uhrenstatus anzeigen): Zeigt die NTP-Uhreninformationen an.
  ```
  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]**: Zeigt die konfigurierten Netzwerkzeitserverzuordnungen an.
  ```
  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
  ```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **debug ntp validation** (NTP-Peer-Uhrzeitvalidierung):Dies ist die **Debugausgabe** aus der Schlüsselungleichheit:

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

- **debug ntp packet**: Zeigt NTP-Paketinformationen an.Wenn der Server keine Antwort gibt, wird nur das `NTP-Exmit-`Paket auf der ASA ohne `NTP RCv`-Paket angezeigt.

```
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)
```

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems