

# ASA/PIX: Пример конфигурации NTP с туннелем IPsec и без него

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Родственные продукты](#)

[Условные обозначения](#)

[!--- конфигурацию](#)

[Схема сети](#)

[Настройка VPN-туннеля для ASDM](#)

[Конфигурация ASDM NTP](#)

[Конфигурация интерфейса командой строки ASA1](#)

[Конфигурация интерфейса командой строки ASA2](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

## **Введение**

Этот документ предоставляет пример конфигурации для синхронизации часов Устройства безопасности PIX/ASA с сервером сетевого времени с помощью Протокола NTP. ASA1 связывается непосредственно с сервером сетевого времени. ASA2 передает трафик NTP через Туннель IPsec к ASA1, который в свою очередь передает пакеты к серверу сетевого времени.

См. [ASA 8.3 и Позже: NTP с и без Примера конфигурации Туннеля IPsec](#) для получения дополнительной информации об одинаковой конфигурации на Cisco ASA с версиями 8.3 и позже.

**Примечание:** Маршрутизатор может также использоваться в качестве сервера NTP для синхронизации часов Устройства безопасности PIX/ASA.

## **Предварительные условия**

### **Требования**

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем

попробовать эту конфигурацию:

- Подключение Сквозного IPSec должно быть установлено прежде, чем запустить эту конфигурацию NTP.
- Необходимо активировать лицензию устройства защиты для стандарта шифрования DES (на минимальном уровне шифрования).

## Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Устройство адаптивной защиты Cisco (ASA) с версией 7.x и позже
- ASDM версий 5.x и выше

**Примечание:** [Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.](#)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Родственные продукты

Эту конфигурацию также можно использовать для устройств защиты Cisco PIX серии 500, работающих под управлением ПО версии 7.x и более поздних версий.

**Примечание:** Поддержка NTP была добавлена в Версии PIX 6.2. См. [PIX 6.2: NTP с и без Примера конфигурации Туннеля IPSec](#) для настройки NTP на Межсетевом экране Cisco PIX.

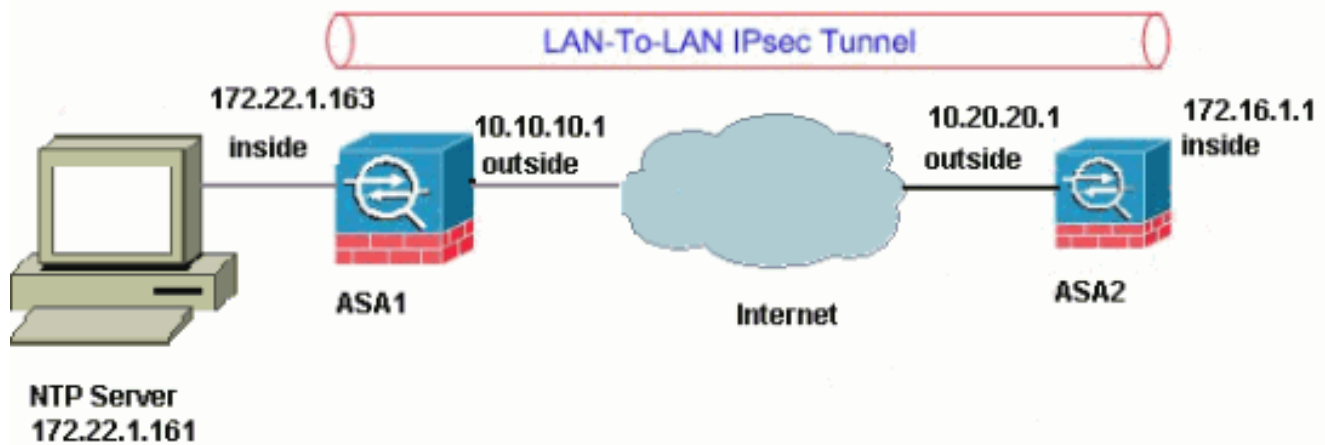
## Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

## !--- конфигурацию

## Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



**Примечание:** Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. [Это адреса RFC 1918, используемые в лабораторной среде.](#)

- [Настройка VPN-туннеля для ASDM](#)
- [Конфигурация ASDM NTP](#)
- [Конфигурация интерфейса командой строки ASA1](#)
- [Конфигурация интерфейса командой строки ASA2](#)

## [Настройка VPN-туннеля для ASDM](#)

Выполните эти шаги для создания VPN-туннеля:

1. Откройте свой браузер и введите **https://<Inside\_IP\_Address\_of\_ASA>** для доступа к ASDM на ASA. Обязательно авторизуйте любые предупреждения, которые ваш браузер дает вам отнесенный подлинности сертификата SSL. По умолчанию имя пользователя и пароль являются пустыми. ASA отобразит следующее окно для загрузки приложения ASDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение 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](#)

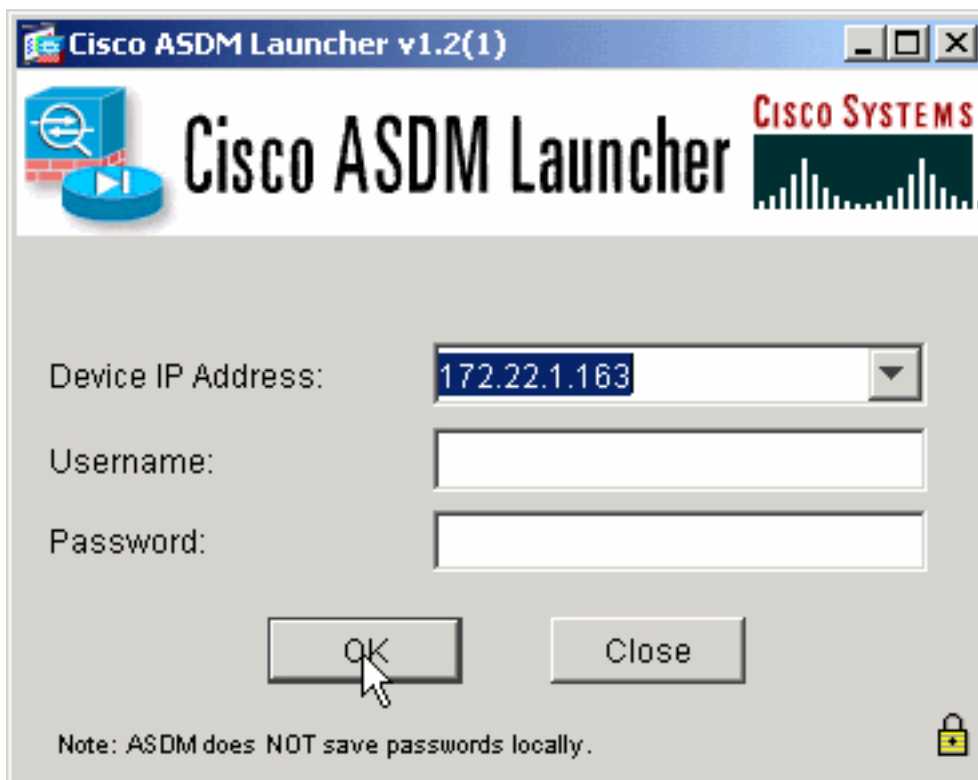
## Running Cisco ASDM as a Java Applet

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](#)

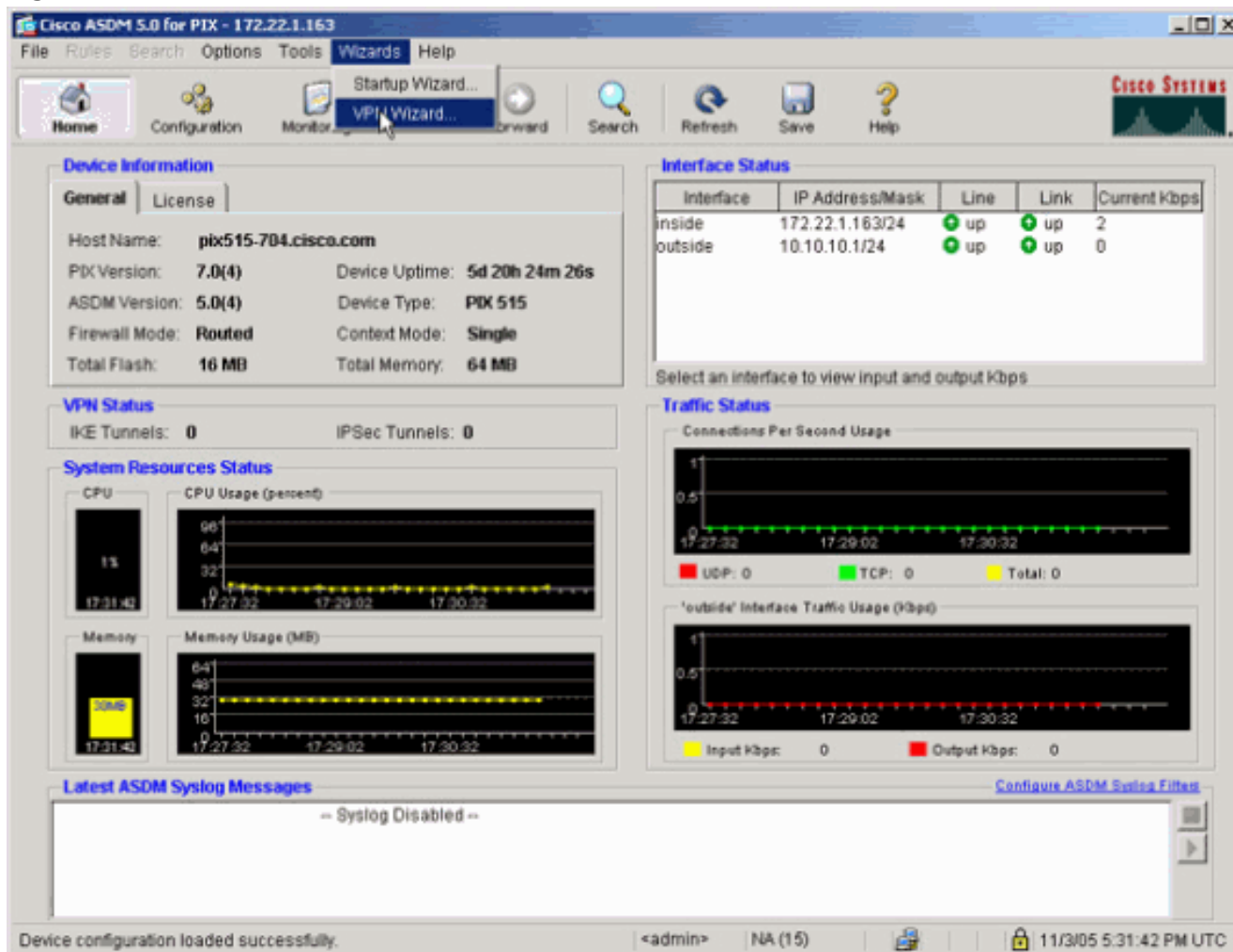
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

2. Нажмите кнопку **Download ASDM Launcher and Start ASDM**, чтобы загрузить файл установки приложения ASDM.
3. После загрузки ASDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска Cisco ASDM Launcher.
4. Введите в поле **Device IP Address** IP-адрес настроенного интерфейса с помощью команды `http -`, а также имя пользователя (в поле **Username**) и пароль (в поле **Password**), если они были заданы. Данный пример использует неопределенное имя пользователя и пароль, заданное по

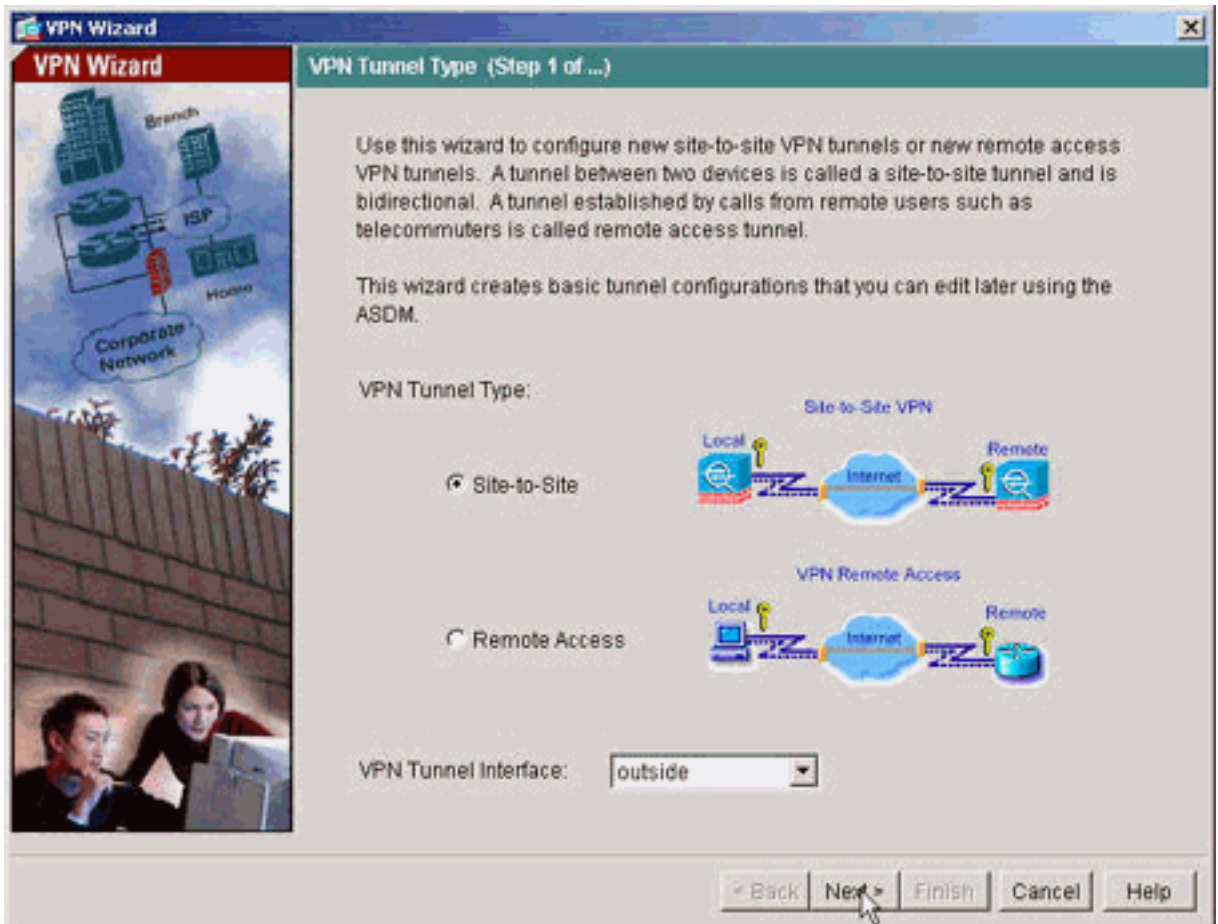


умолчанию.

5. Выполните Мастера VPN, как только приложение ASDM соединяется с ASA.

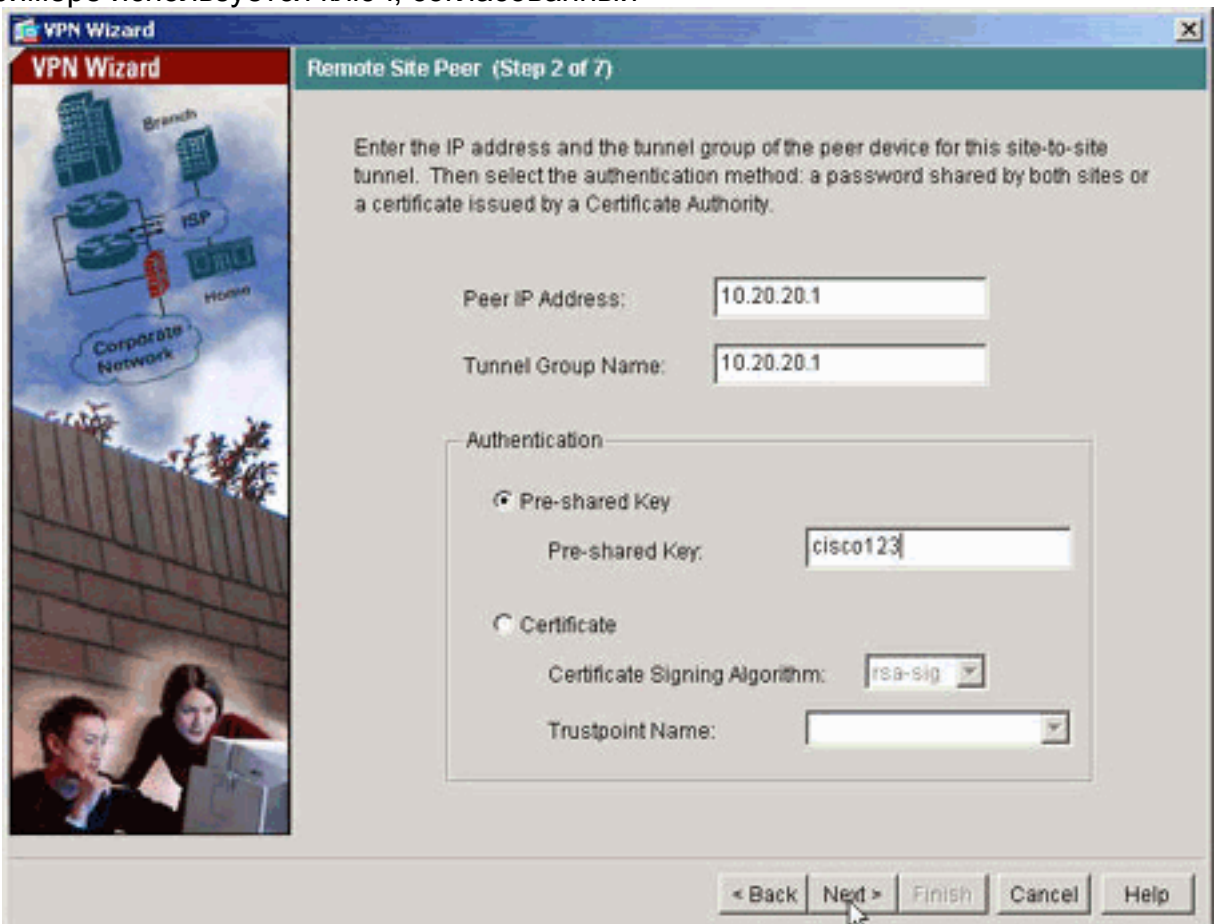


6. Выберите тип VPN-туннеля Защищенного взаимодействия между сетями Site-to-Site



IPsec.

- Укажите внешний IP-адрес удаленного узла. Введите данные для аутентификации (в этом примере используется ключ, согласованный

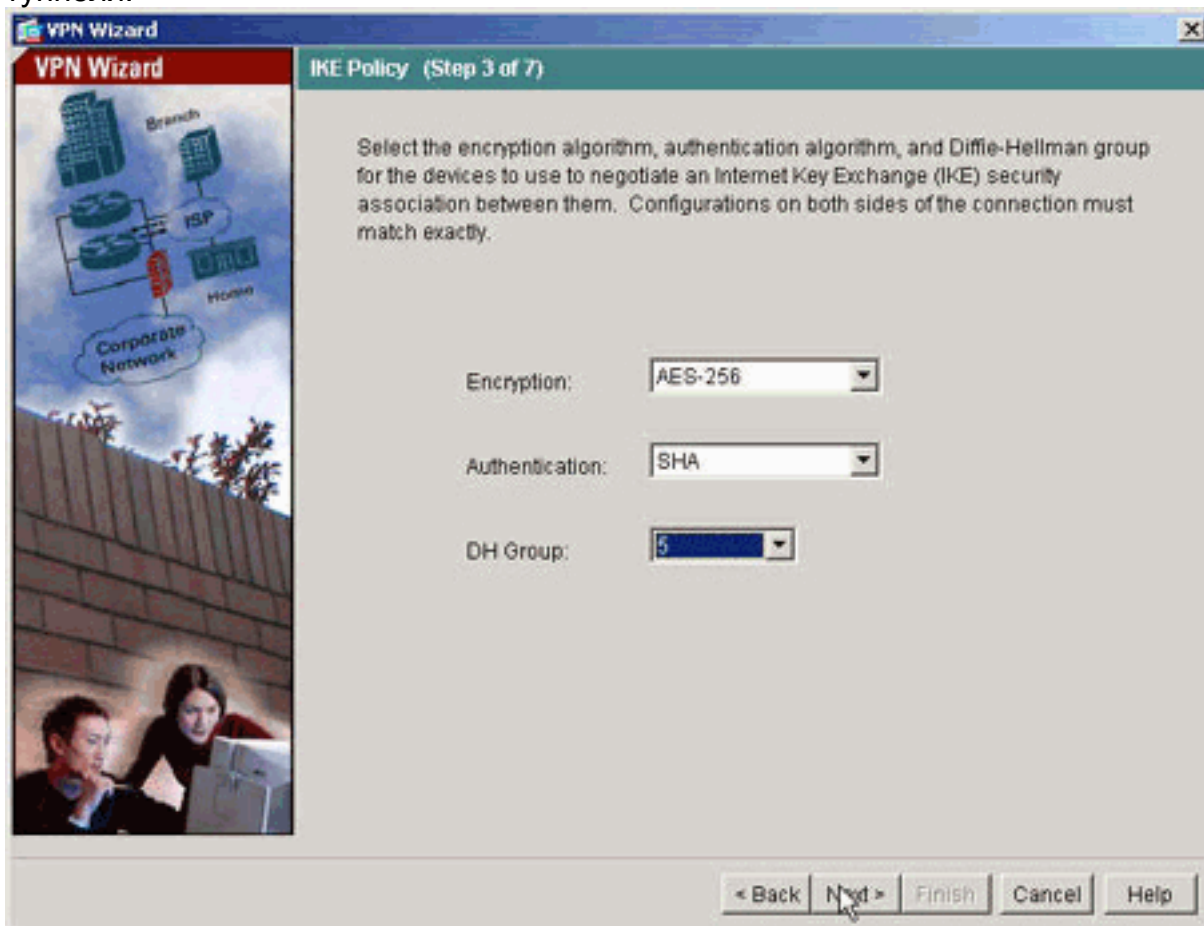


ранее).

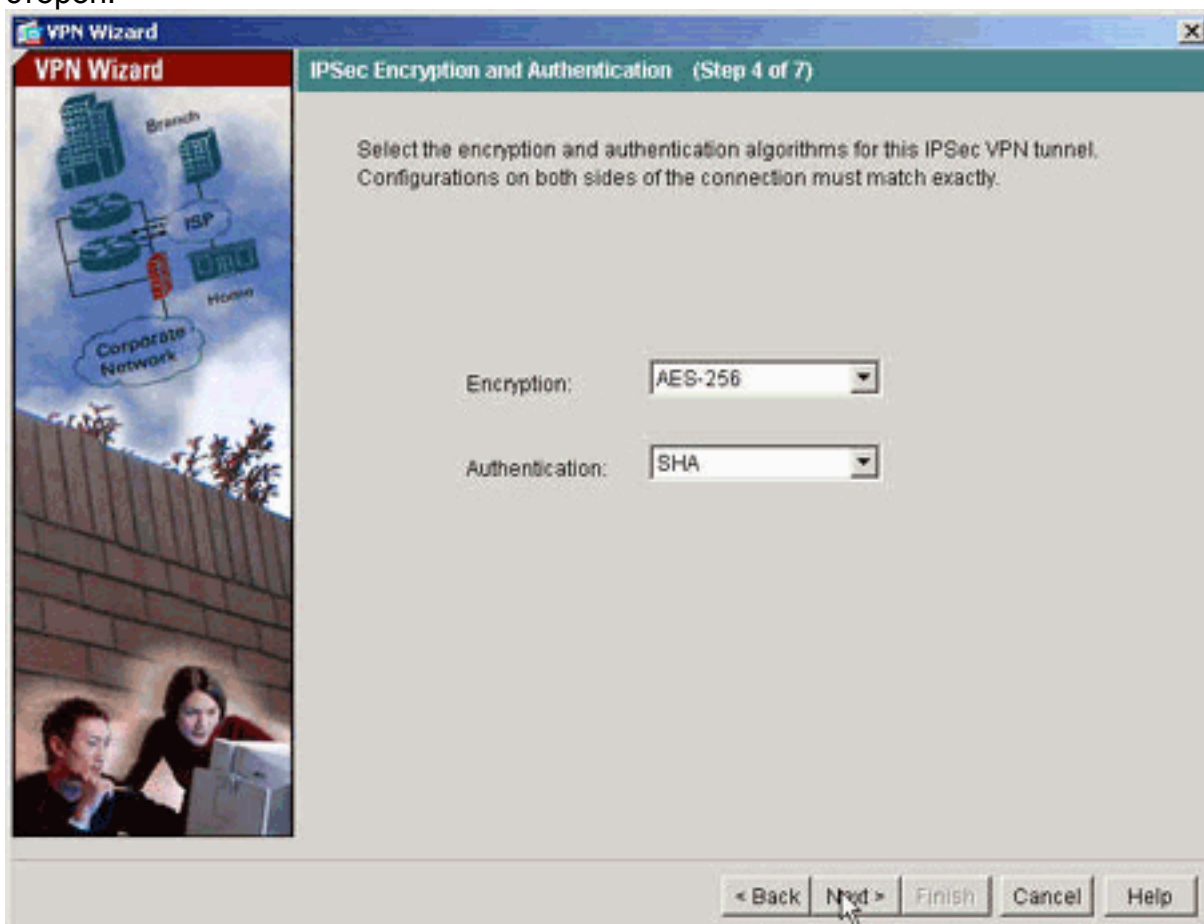
- Задайте атрибуты для использования для IKE, также известного как Фаза 1. Эти атрибуты должны быть тем же с обеих сторон



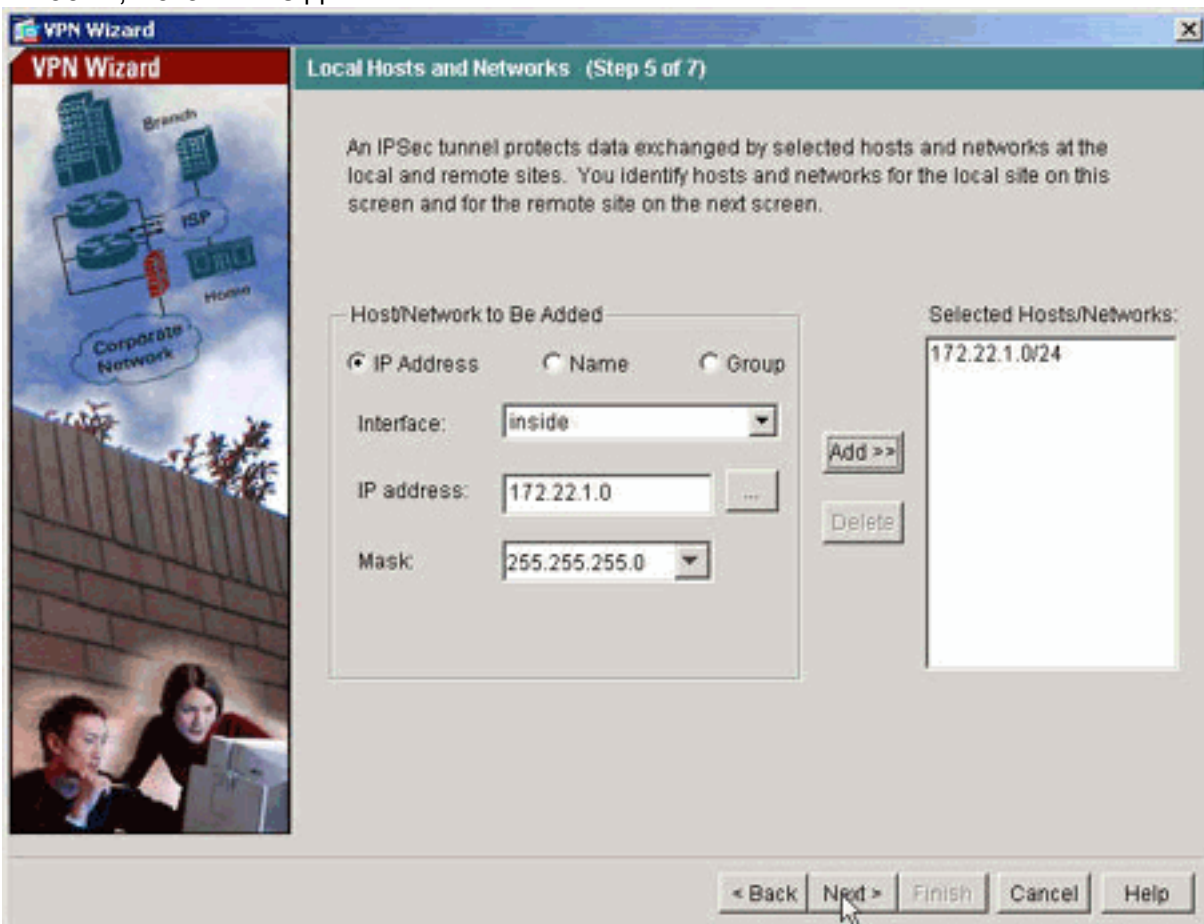
туннеля.



9. Задайте атрибуты для использования для IPsec, также известного как Фаза 2. Эти атрибуты должны совпасть с обеих сторон.

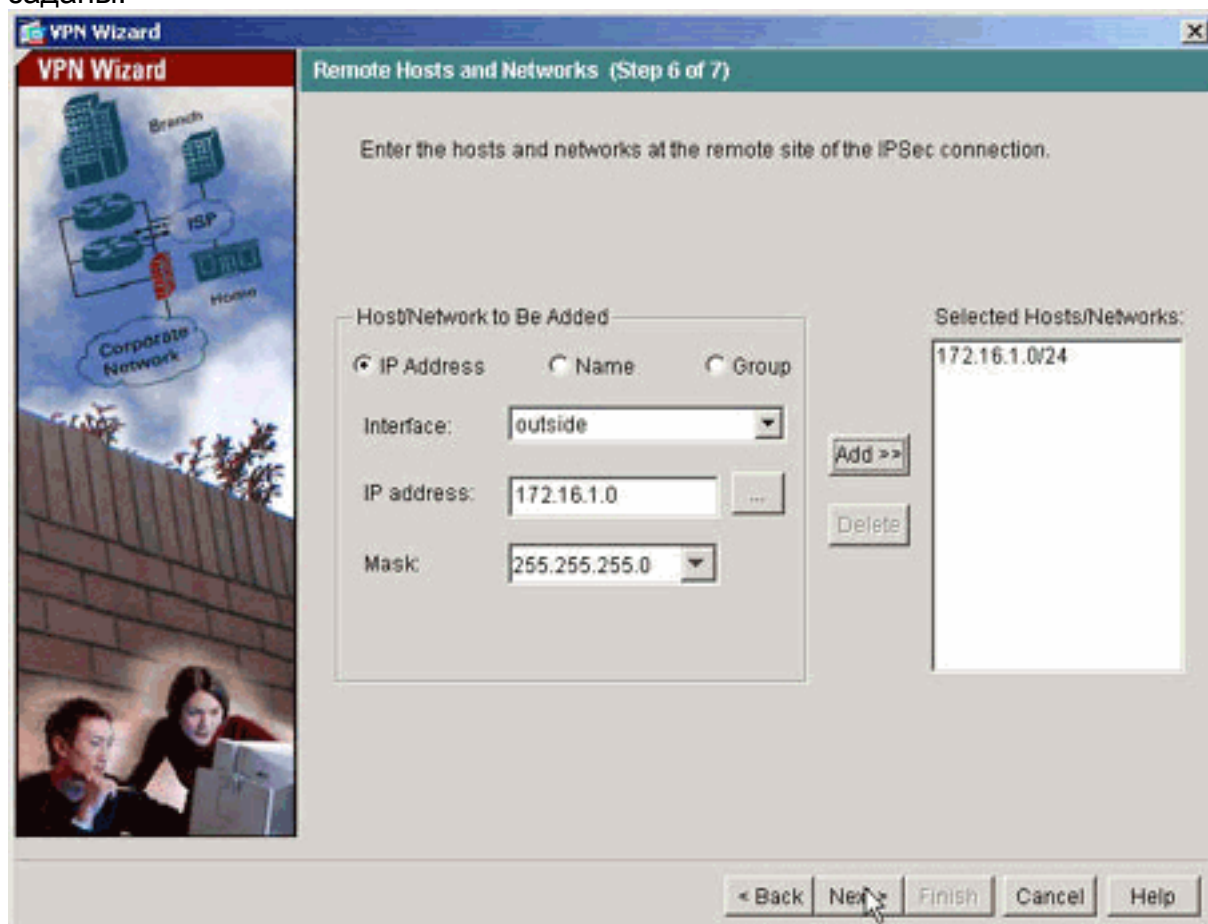


10. Укажите хосты, трафик которых будет разрешен через VPN-туннель. В этом шаге заданы хосты, локальные для



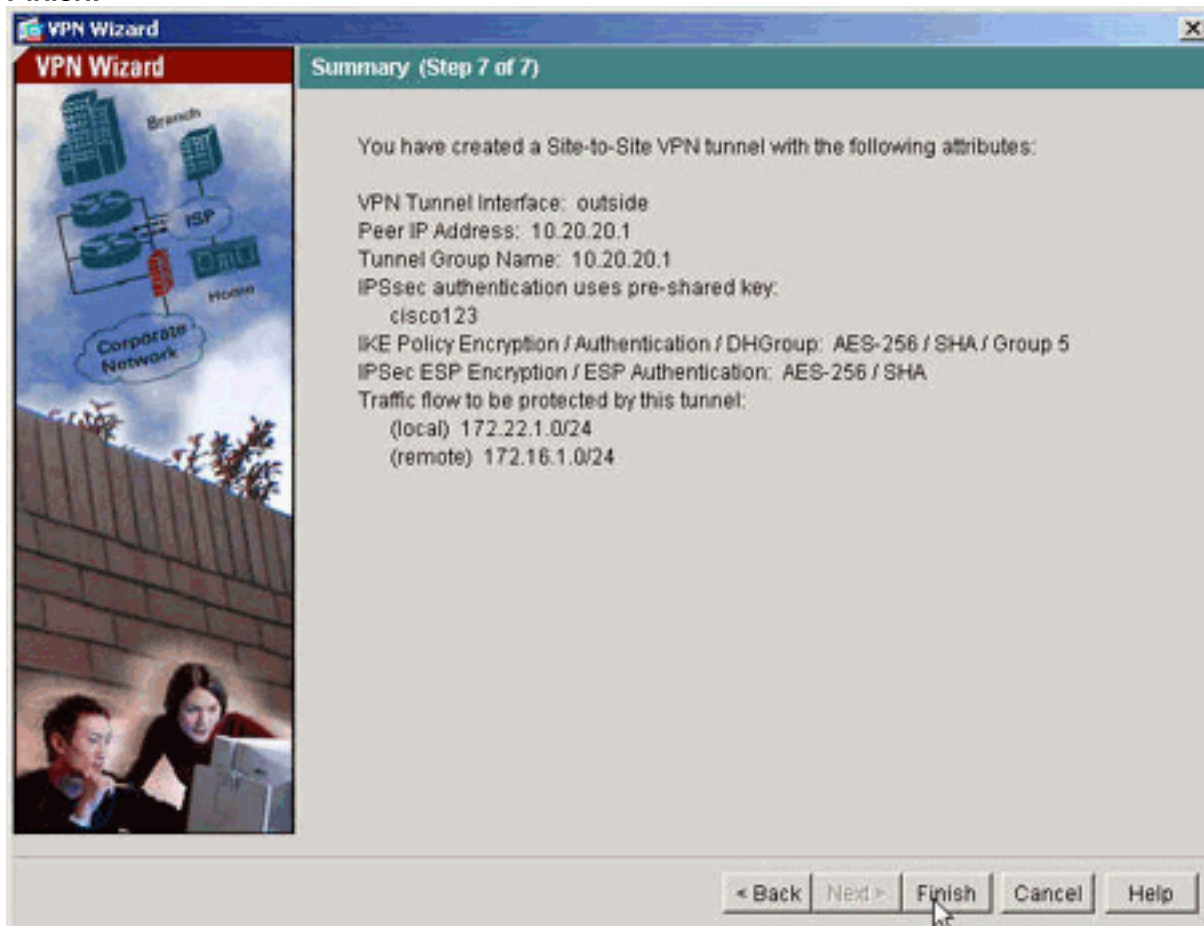
ASA1.

11. Хосты и сети на удаленной стороне туннеля заданы.





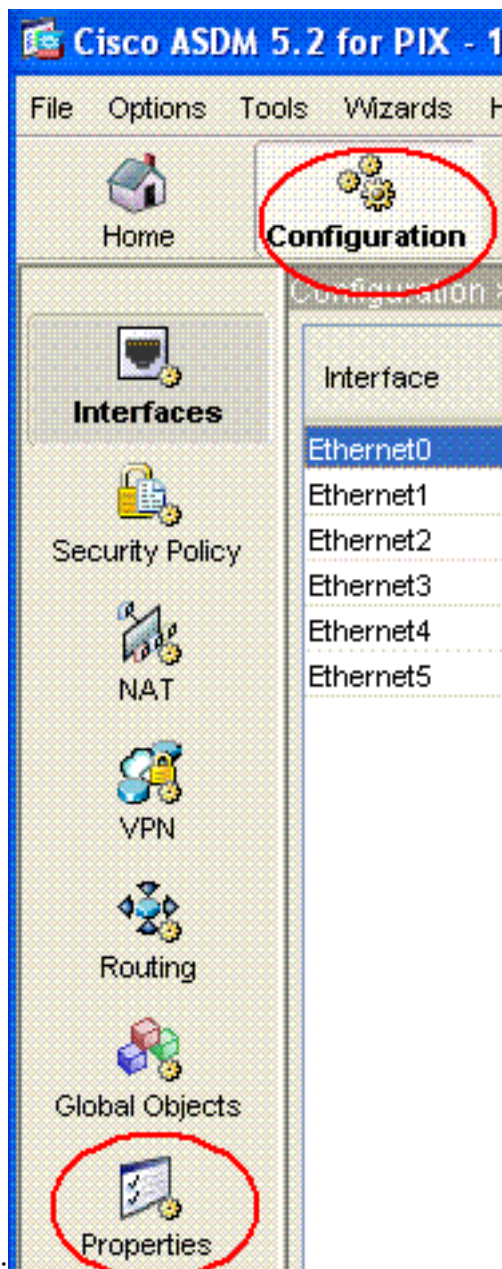
12. Все параметры, установленные с помощью мастера "VPN Wizard" отобразятся на странице "Summary". **Дважды проверьте настройки и, если они верны, нажмите кнопку Finish.**



## Конфигурация ASDM NTP

Выполните эти шаги для настройки NTP на Cisco Security Appliance:

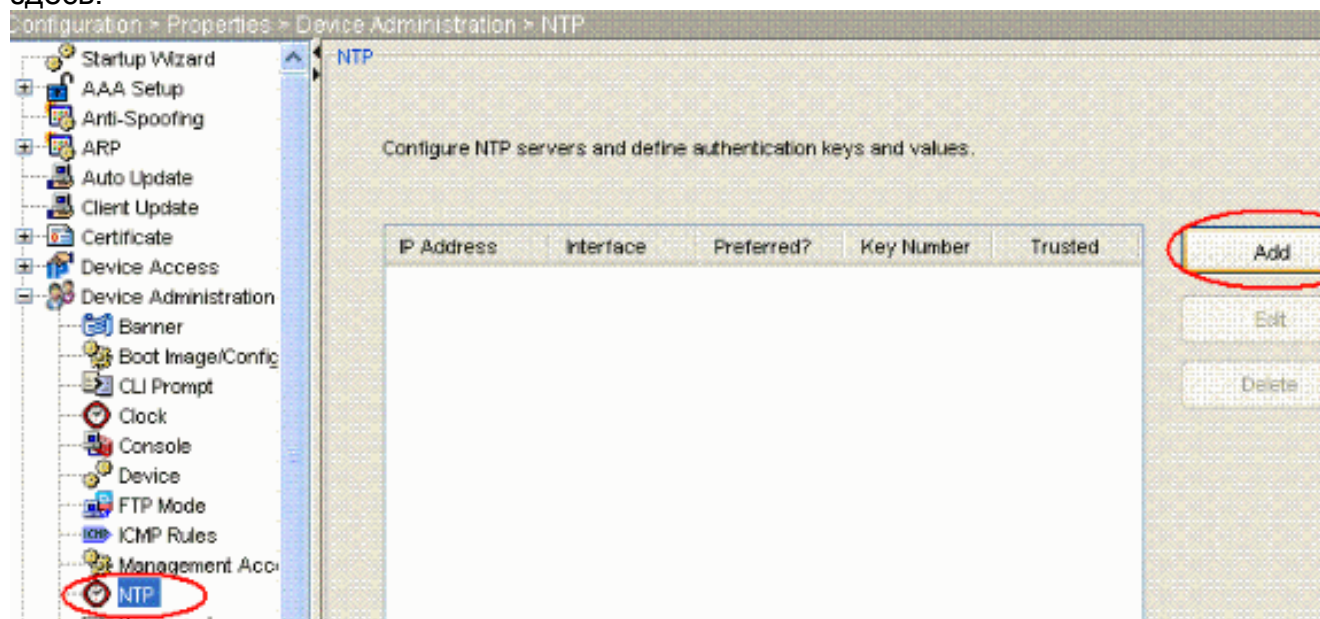
1. Выберите **Configuration** в домашней странице ASDM как показано



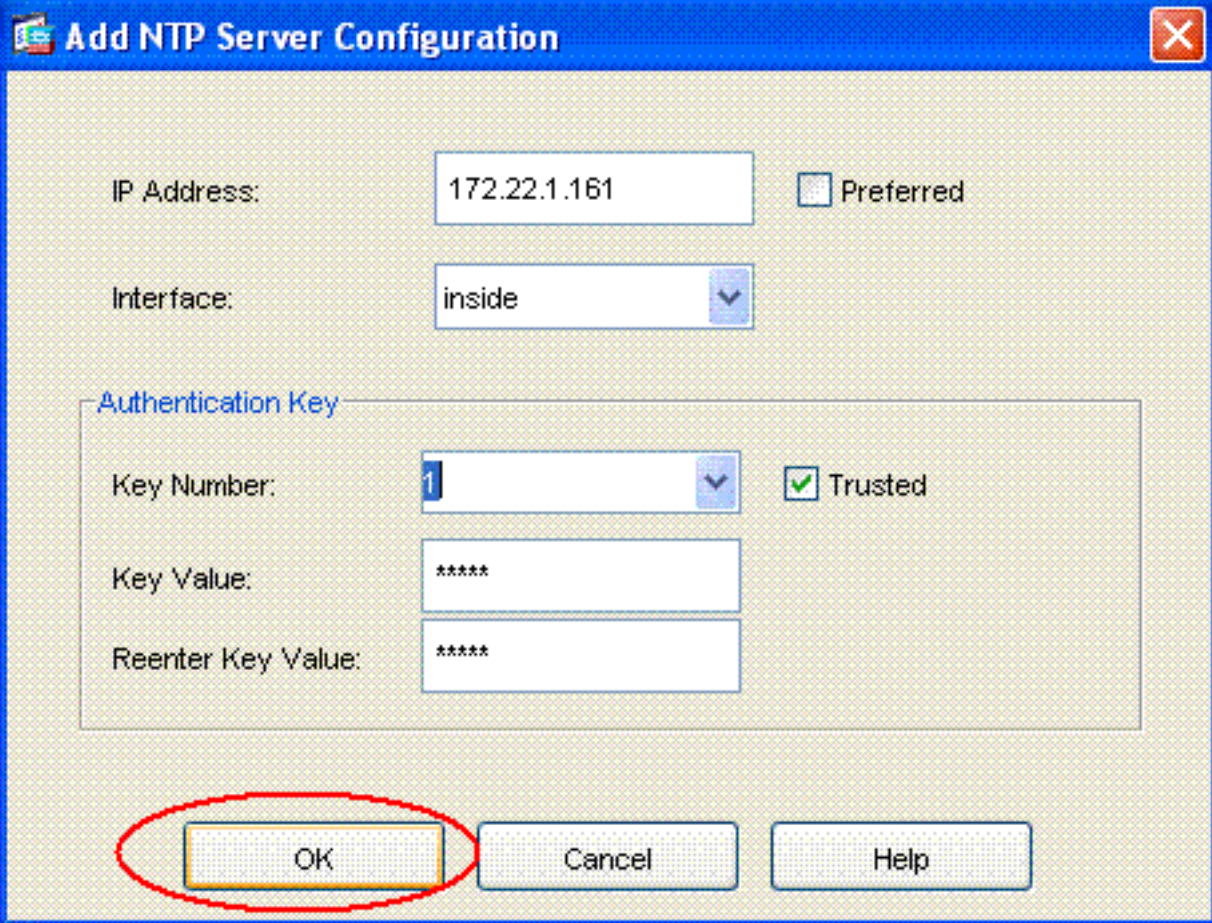
здесь:

2. Теперь выберите **Properties**> **Device Management**> **NTP** для открытия страницы конфигурации NTP ASDM как показано

здесь:



3. Нажмите кнопку **ADD**, чтобы добавить сервер NTP и предоставить обязательные атрибуты, такие как IP-адрес, Имя интерфейса (Внутри или снаружи), ключевой номер и значение параметра для Authentication в новом окне, которое подходит после щелчка по кнопке **ADD** как показано в снимке экрана. Затем щелкните по



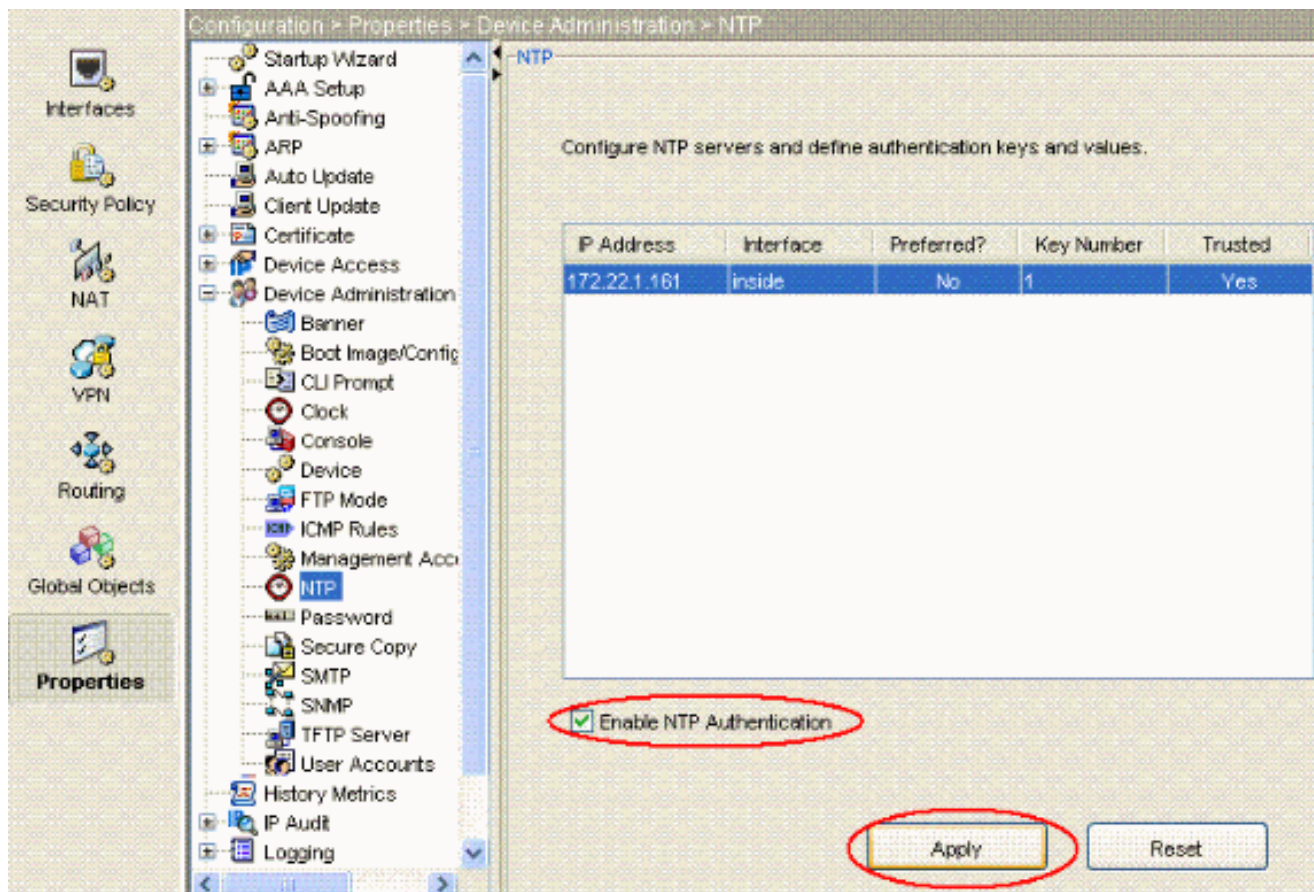
OK.

Пр

**имечание:** Имя интерфейса должно быть выбрано как внутри для ASA1 и снаружи для ASA2. **Примечание:** Аутентификационный ключ NTP должен быть тем же в ASA и сервере NTP. Конфигурацию атрибута Authentication в cli для ASA1 и ASA2 показывают НИЖЕ: 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. Теперь нажмите флажок **Enable NTP Authentication** и нажмите **Apply**, который выполняет задачу конфигурации NTP.





## Конфигурация интерфейса командой строки 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

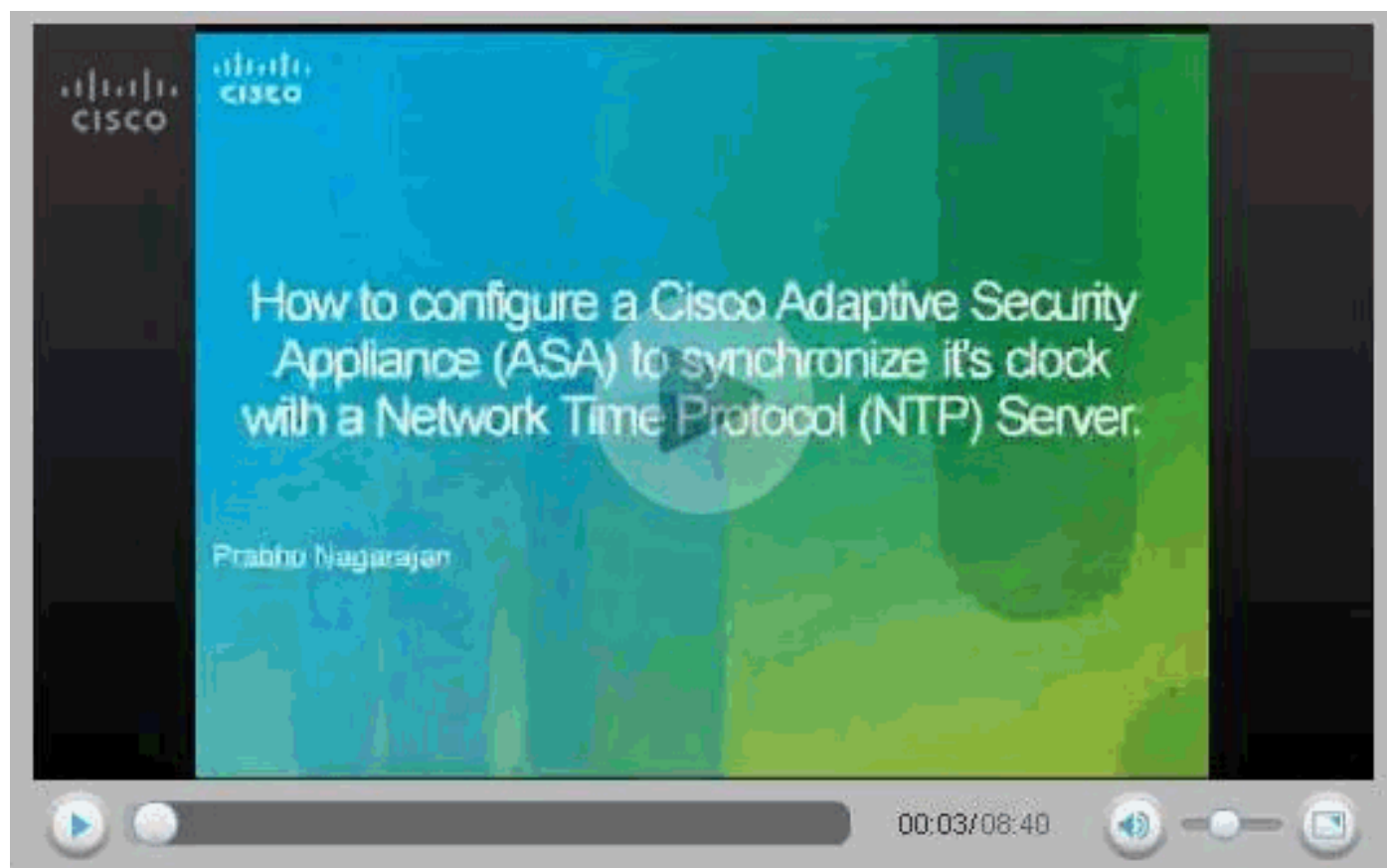
```

Это видео, зарегистрированное к [Сообществу Cisco Support](#), объясняет с демонстрацией,



процедура для настройки ASA как клиента NTP:

[Как настроить устройство адаптивной защиты Cisco \(ASA\) для синхронизации его часов с Сервером Протокола NTP.](#)



## [Конфигурация интерфейса командой строки 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#

```

## Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Некоторые команды **show** поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды **show**.

- **[show ntp status](#)** сведения о синхронизации 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 \[detail\]](#)** — Отображает настроенные сетевые ассоциации временного сервера.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 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
```

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

### Команды для устранения неполадок

Некоторые команды `show` поддерживаются Средством интерпретации выходных данных (только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды `show`.

**Примечание:** Прежде чем вызывать команды `debug`, обратитесь к разделу **Важные сведения о командах отладки**.

- **законность `debug ntp`** — Отображает достоверность синхронизации NTP-узлов. Это - **выходные данные отладки от основной несогласованности:**

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

- **пакет `debug ntp`** — Отображает информацию о пакете NTP. Когда нет никакого ответа от сервера, только пакет NTP `xmit` замечен на ASA без пакета NTP `rcv`. 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)
```

## Дополнительные сведения

- [Cisco PIX Firewall Software](#)
- [Диспетчер адаптивных устройств защиты Cisco \(Cisco Adaptive Security Device Manager\)](#)
- [CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES](#)
- [Справочники по командам для межсетевого экрана PIX Cisco Secure](#)
- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)