PIX/ASA 7.x и выше: Пример конфигурации VPN-туннеля OT PIX К PIX

Содержание

Введение

В этом документе описана процедура настройки VPN-туннелей между двумя межсетевыми экранами PIX с использованием диспетчера устройств адаптивной защиты Cisco (ASDM). ASDM представляет собой средство настройки на основе приложения, призванное помочь пользователю в установке, настройке и управлении межсетевым экраном PIX при помощи графического интерфейса. Межсетевые экраны PIX размещаются на двух разных территориальных объектах.

Туннель сформирован с помощью IPsec. IPsec является комбинацией открытых стандартов, которые предоставляют конфиденциальность данных, целостность данных и проверку подлинности источника данных между узлами IPsec.

Примечание: В PIX версии 7.1 и более поздних версиях команда 1sysopt connection permit-ipsec заменена на sysopt connection permit-vpn. Эта команда позволяет трафик, который поступает в устройство безопасности через VPN-туннель и тогда дешифрован, для обхода списков доступа к интерфейсам. К трафику продолжают применяться групповые политики и списки авторизации доступа на уровне отдельных пользователей. Для отключения этой опции используйте **эту команду с параметром no**. Эта команда не видима в конфигурации

интерфейса командой строки.

См. документ PIX 6.x: Пример конфигурации простого VPN-туннеля PIX-PIX для получения дополнительных сведений о сценарии, в котором устройство защиты Cisco PIX работает под управлением ПО версии 6.x.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе указывают, что этот узел инициирует первый частный обмен для определения соответствующего равноправного узла, с которым можно соединиться.

- Устройство защиты Cisco PIX серии 500 с версией 7.x и позже
- ASDM версий 5.x и выше

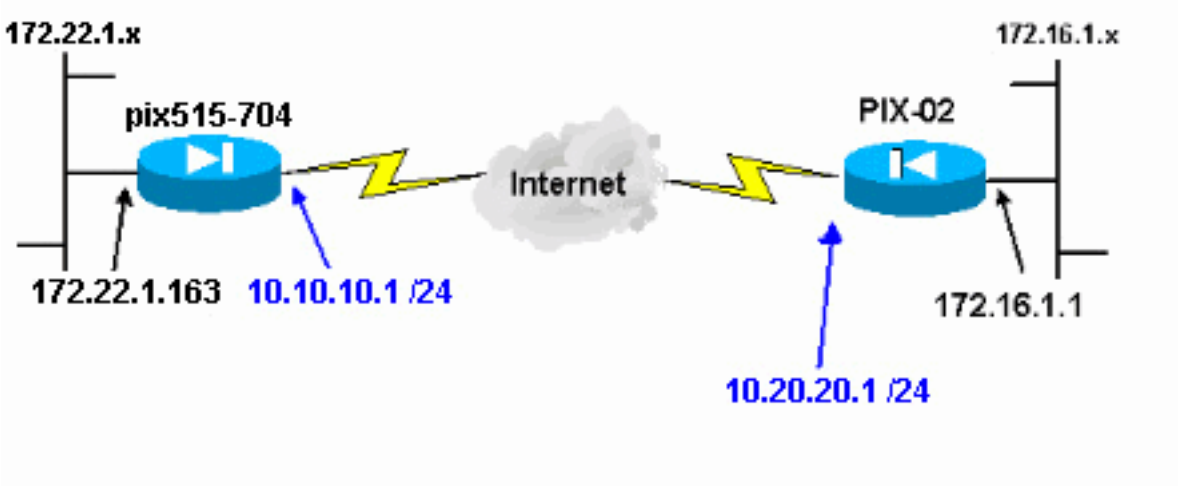
Примечание: Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.

Примечание: Модуль ASA серии 5500 версий 7.x/8.x выполняет то же программное обеспечение, замеченное в Версии PIX 7.x/8. x. Настройки, приведенные в этом документе, применимы к обеим линиям продуктов.

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.

Схема сети

В настоящем документе используется следующая схема сети:



Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Согласование IPsec может быть разделено на пять этапов и включает две фазы Протокола IKE.

1. Туннель IPSec инициирован содержательным трафиком. Трафик считается содержательным при передаче между двумя одноранговыми узлами IPsec.
2. На втором этапе обмена ключами (IKE) для равноправных пользователей протокола IPSec выполняется согласование установленной политики сопоставлений безопасности (SA) IKE. По завершении аутентификации одноранговых узлов создается защищенный туннель с применением протокола ISAKMP.
3. На втором этапе обмена ключами (IKE) одноранговые узлы IPsec используют проверенный и безопасный туннель для согласования преобразований IPSec SA. Согласование общей политики определяет то, как будет установлен туннель IPSec.
4. Туннель IPSec создан, и данные передаются между узлами IPSec на основании параметров IPSec, настроенных в наборах преобразования IPSec.
5. Разъединение туннеля IPSec выполняется при удалении сопоставлений безопасности (IPSec SA) или по истечении срока их действия.**Примечание:** Если SA на обеих из фаз IKE не совпадают на узлах, согласование IPsec между этими двумя PIX отказывает.

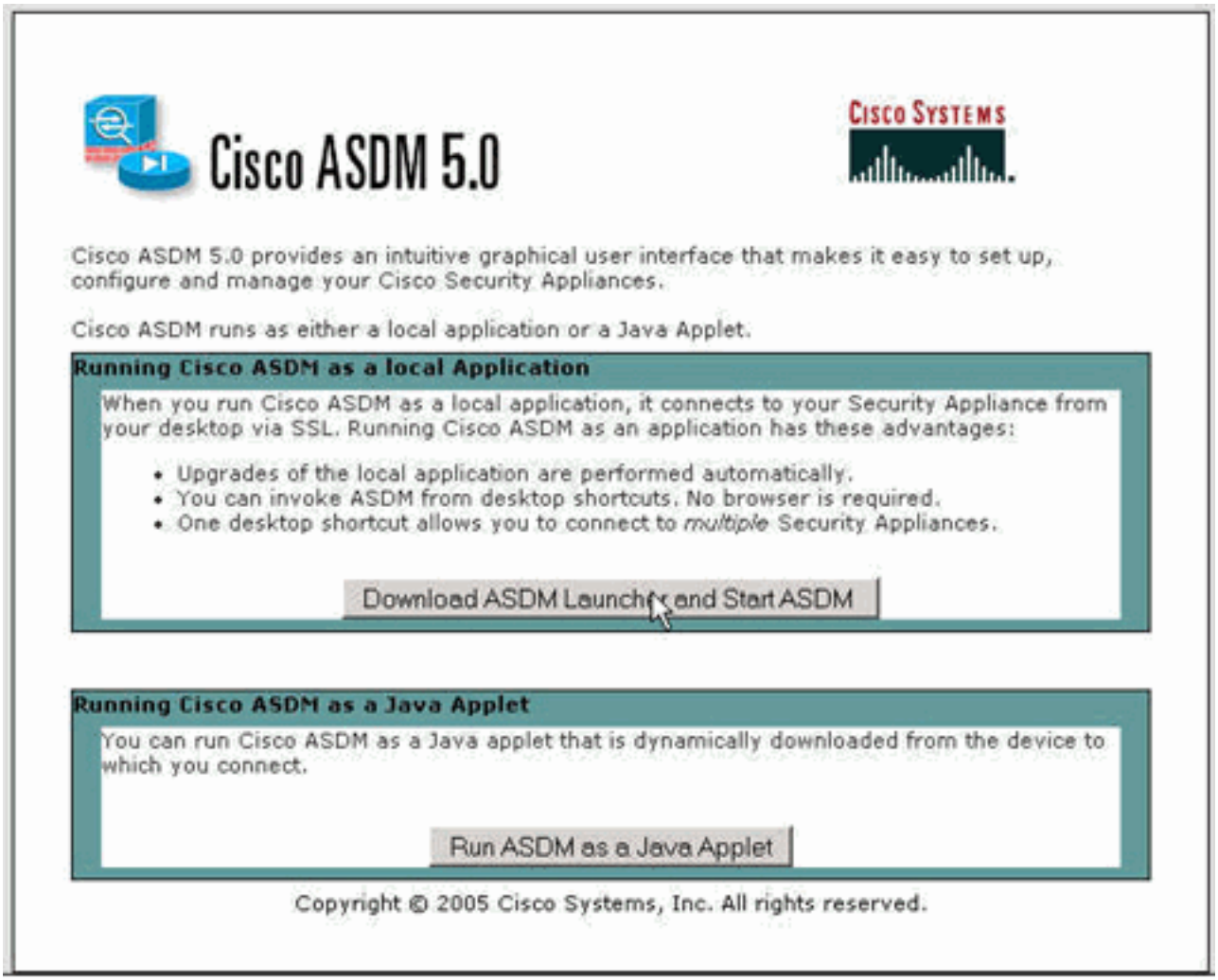
!--- конфигурацию

- Настройка посредством ASDM
- Настройки PIX с помощью CLI

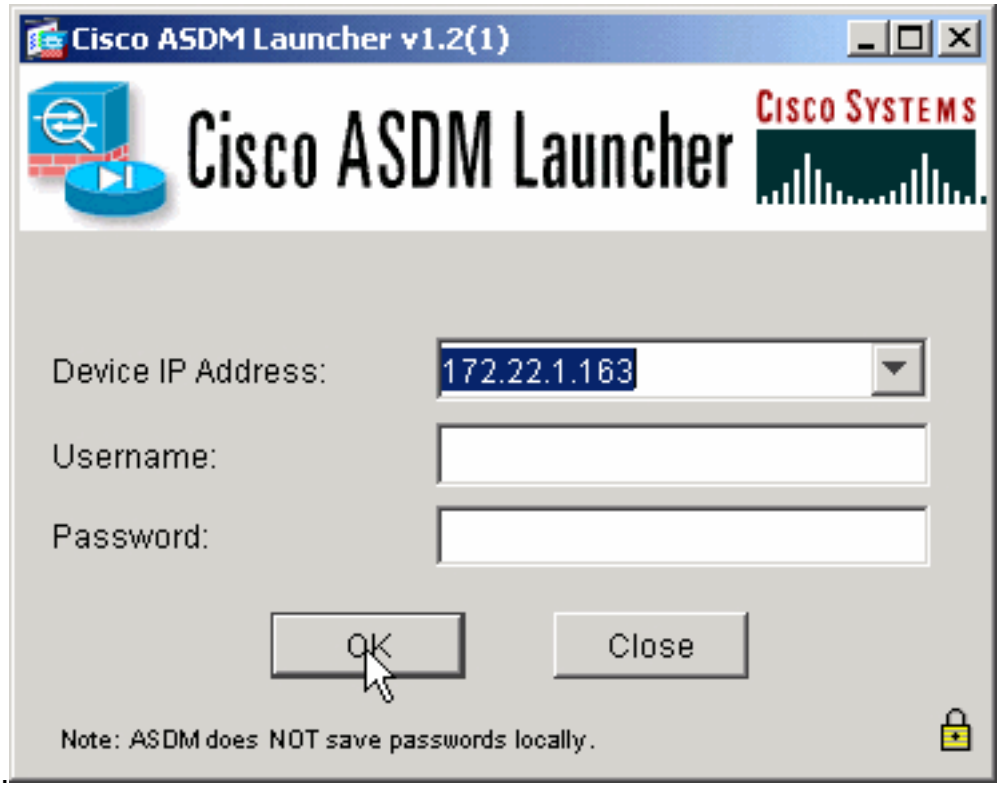
Настройка посредством ASDM

Выполните следующие действия:

1. Откройте свой браузер и введите **https://<Внутренний_IP-адрес_PIX>** для доступа к ASDM на PIX.Обязательно авторизуйте любые предупреждения, которые ваш браузер дает вам отнесенный подлинности сертификата SSL. По умолчанию имя пользователя и пароль являются пустыми.PIX представляет это окно для разрешения загрузки приложения ASDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение
   Java.

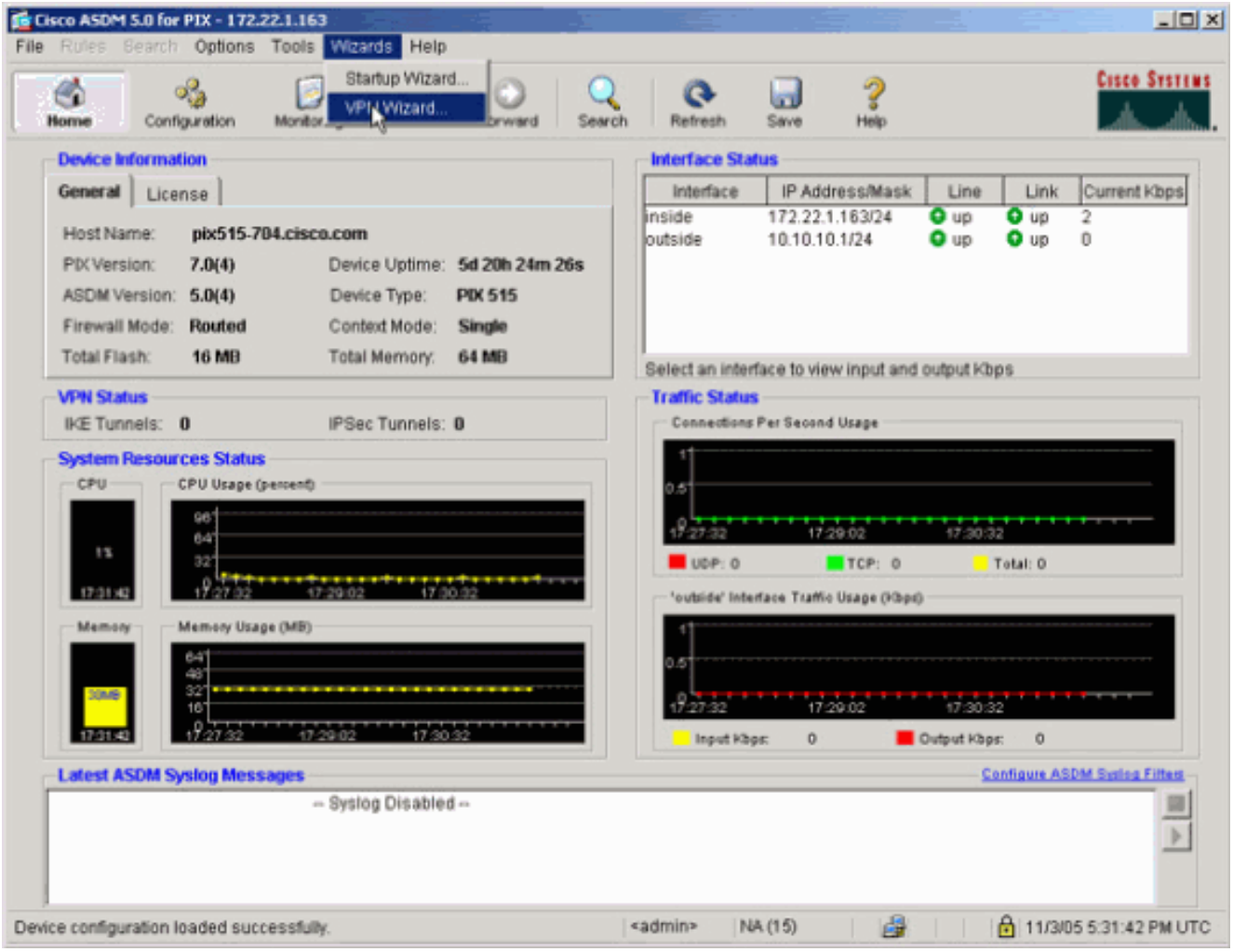


2. **Нажмите кнопку Download ASDM Launcher and Start ASDM** для загрузки установщика для приложения ASDM.
3. Как только Модуль запуска ASDM загружает, придерживайтесь приглашений, чтобы установить программное обеспечение и выполнить загрузчик Cisco ASDM.
4. **Введите в поле Device IP Address IP-адрес 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

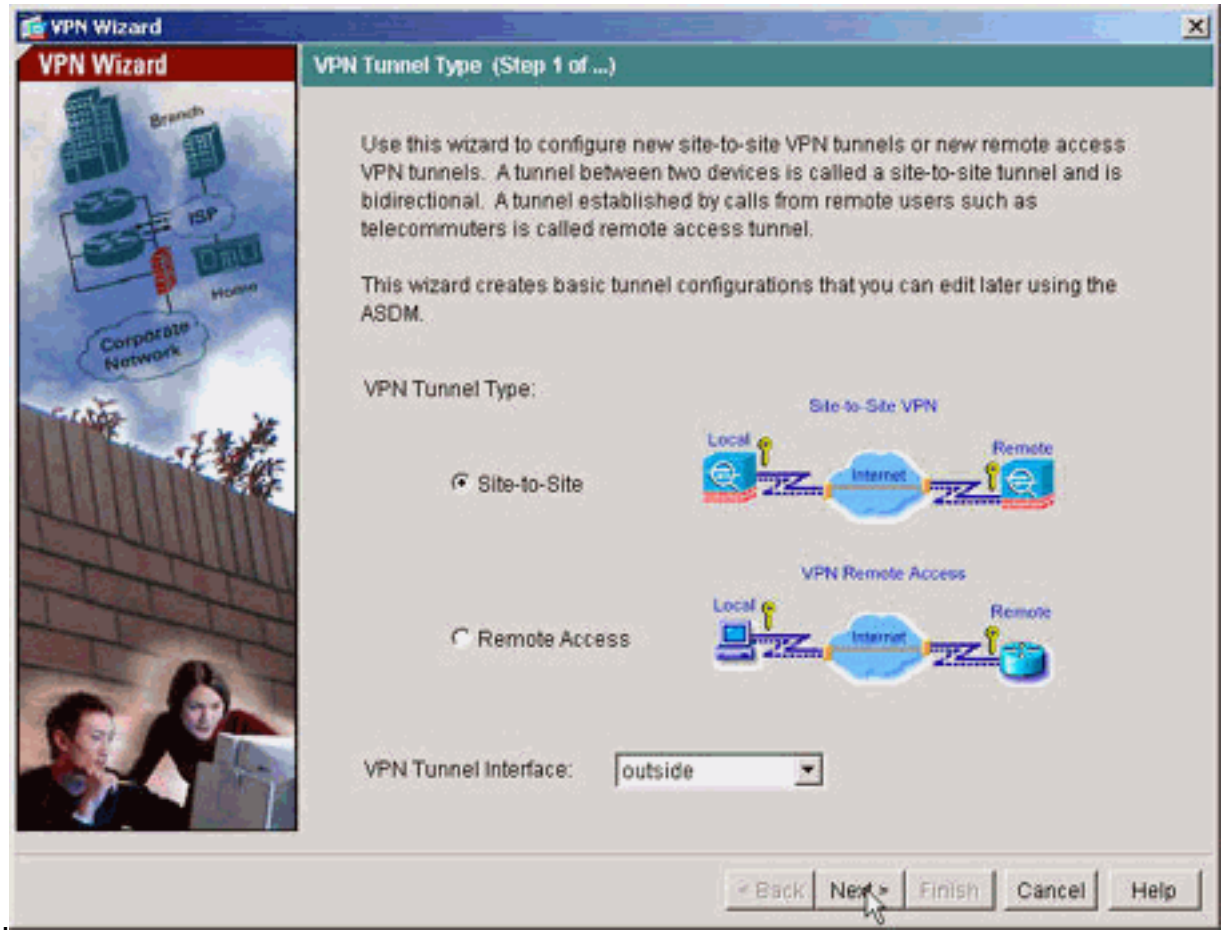


умолчанию.

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

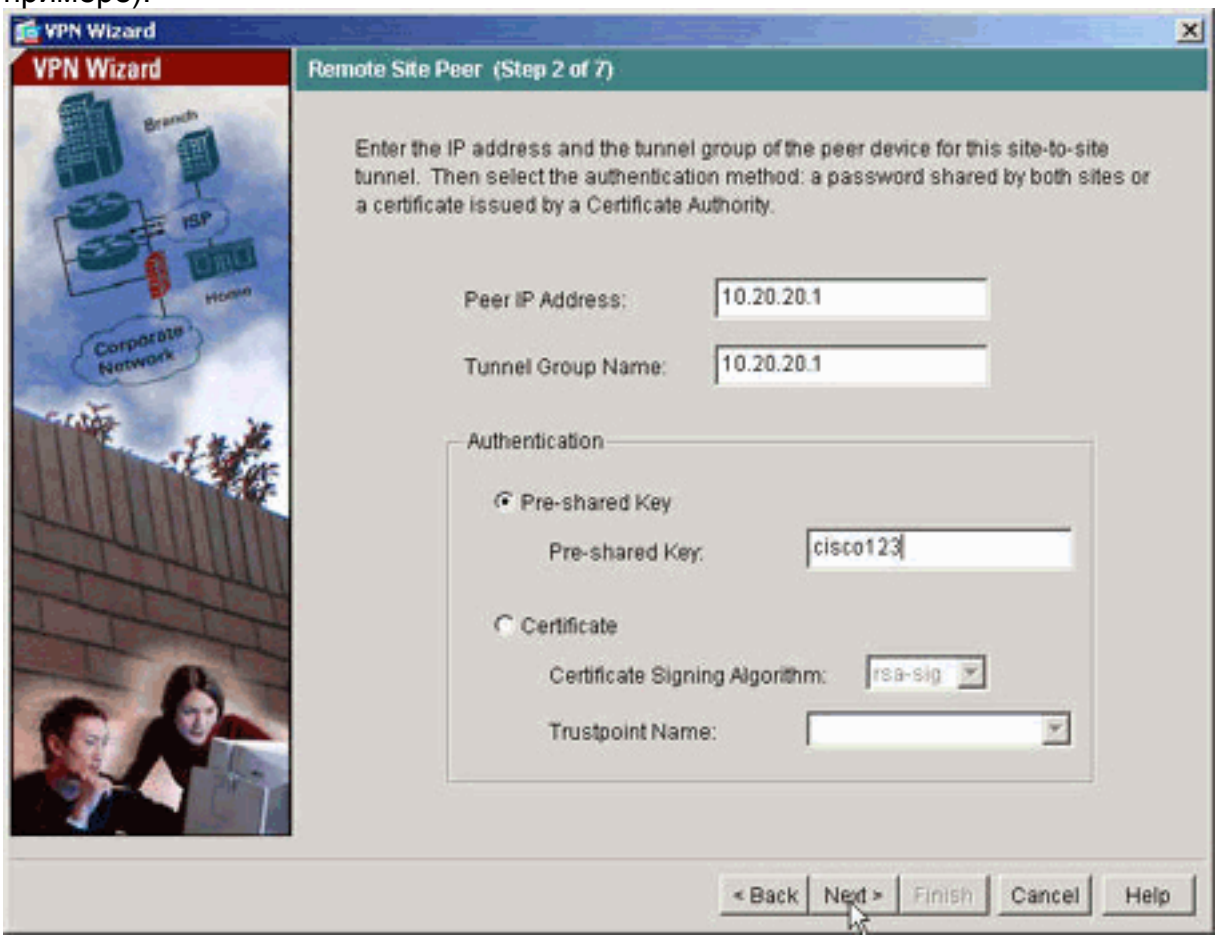


6. Выберите тип **Туннеля VPN типа «узел-**



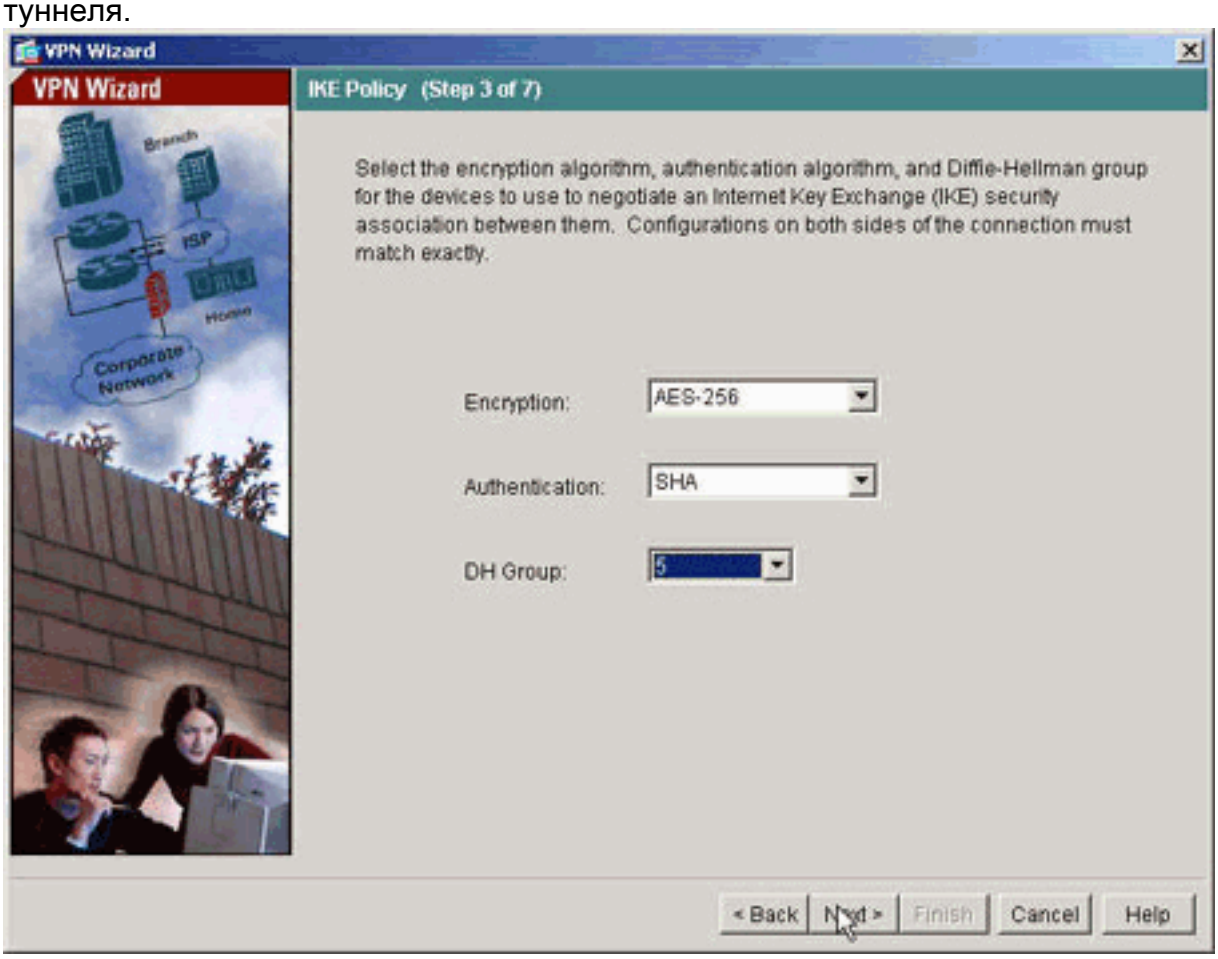
узел».

7. Укажите внешний IP-адрес удаленного узла. Введите информацию для аутентификации для использования (предварительный общий ключ в данном примере).

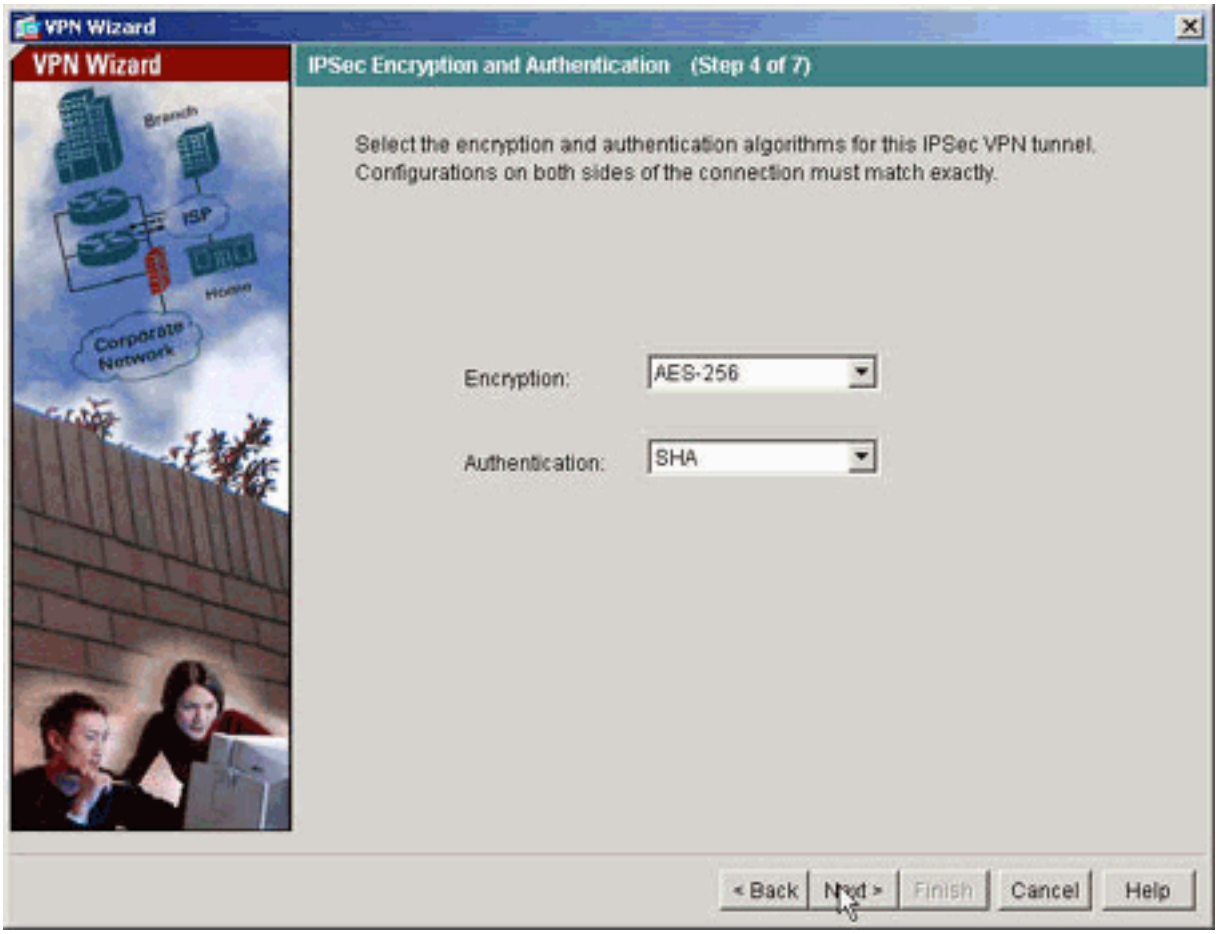


8. Задайте атрибуты для использования для IKE, также известного как "Фаза 1". Эти

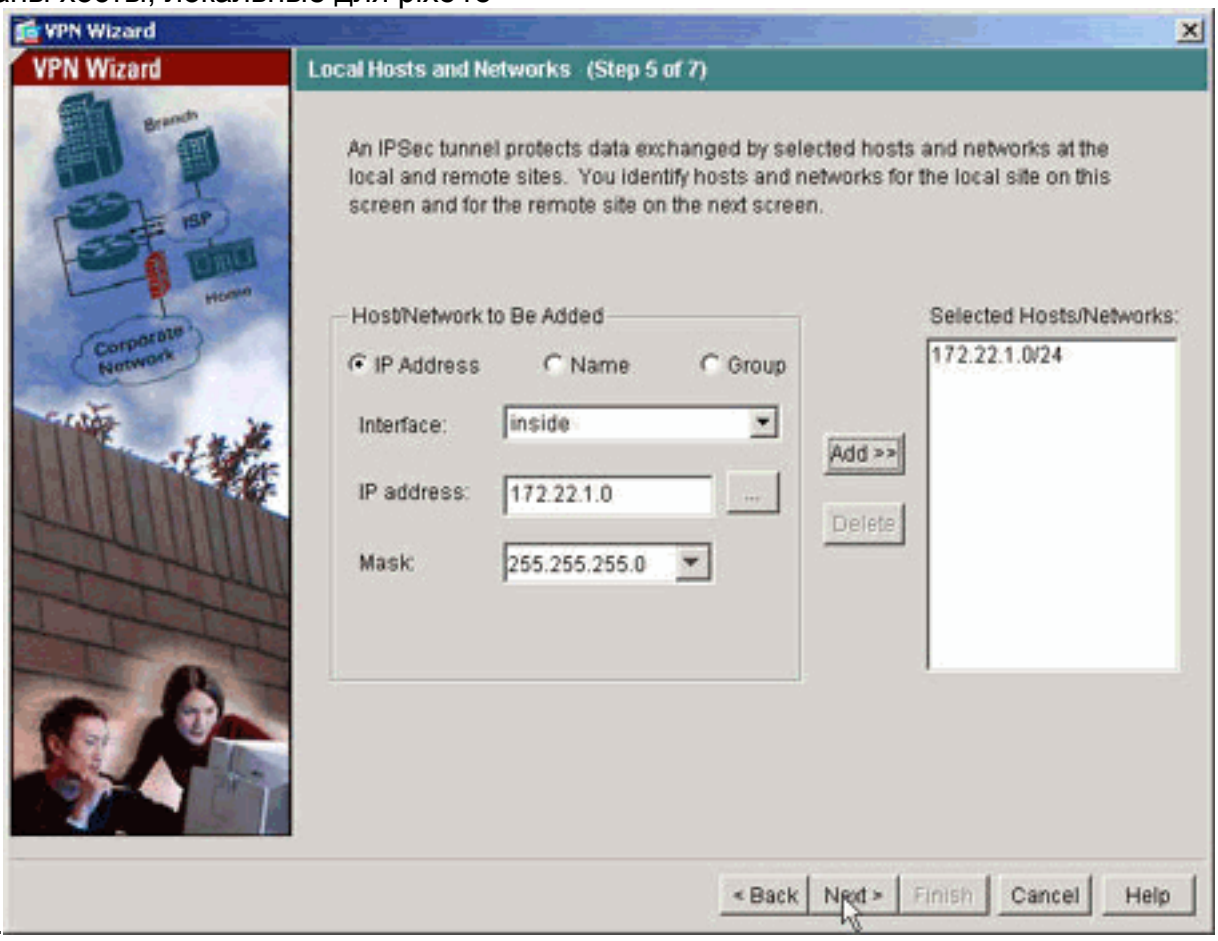
атрибуты должны быть тем же с обеих сторон
туннеля.



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

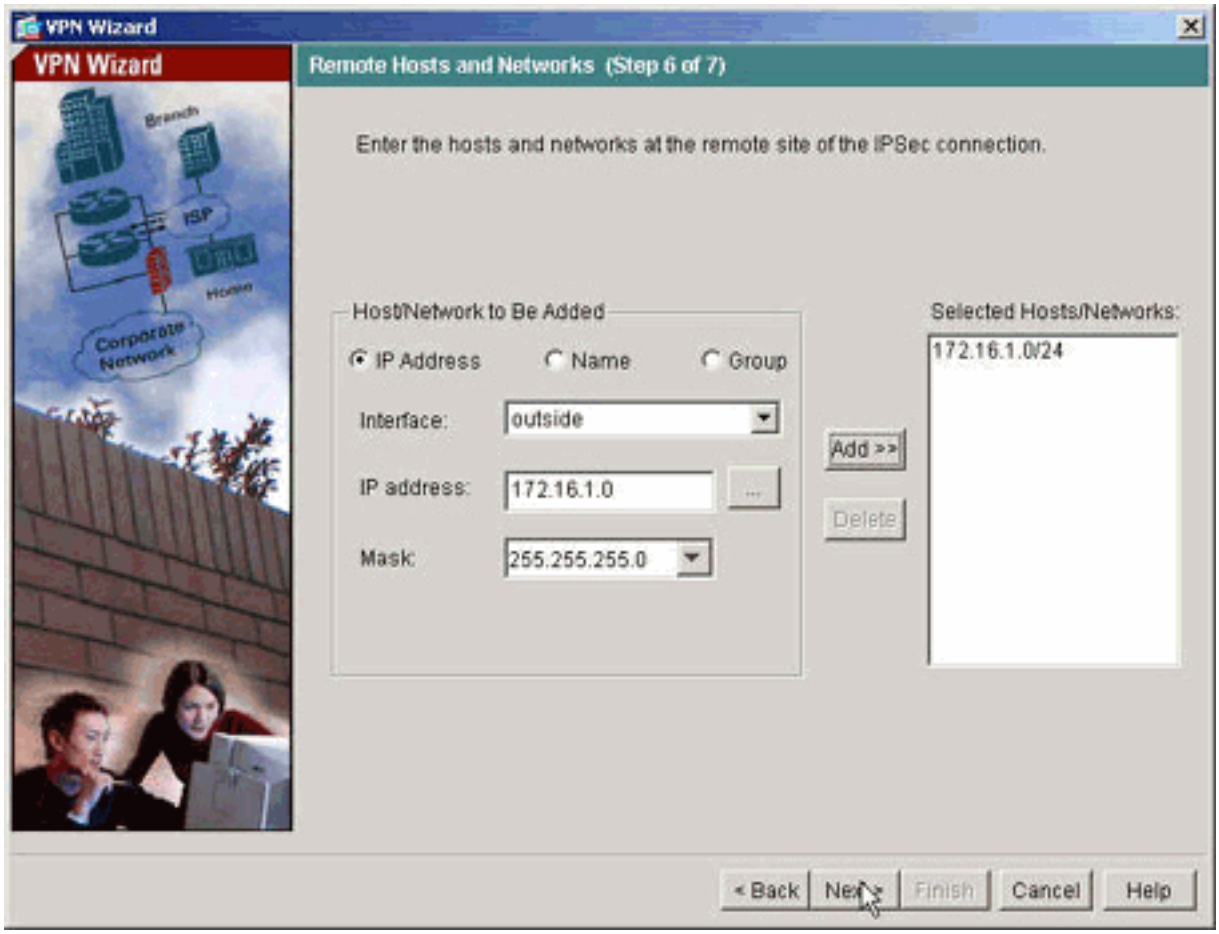


10. Укажите хосты, трафик которых будет разрешен через VPN-туннель. В этом шаге заданы хосты, локальные для pix515-

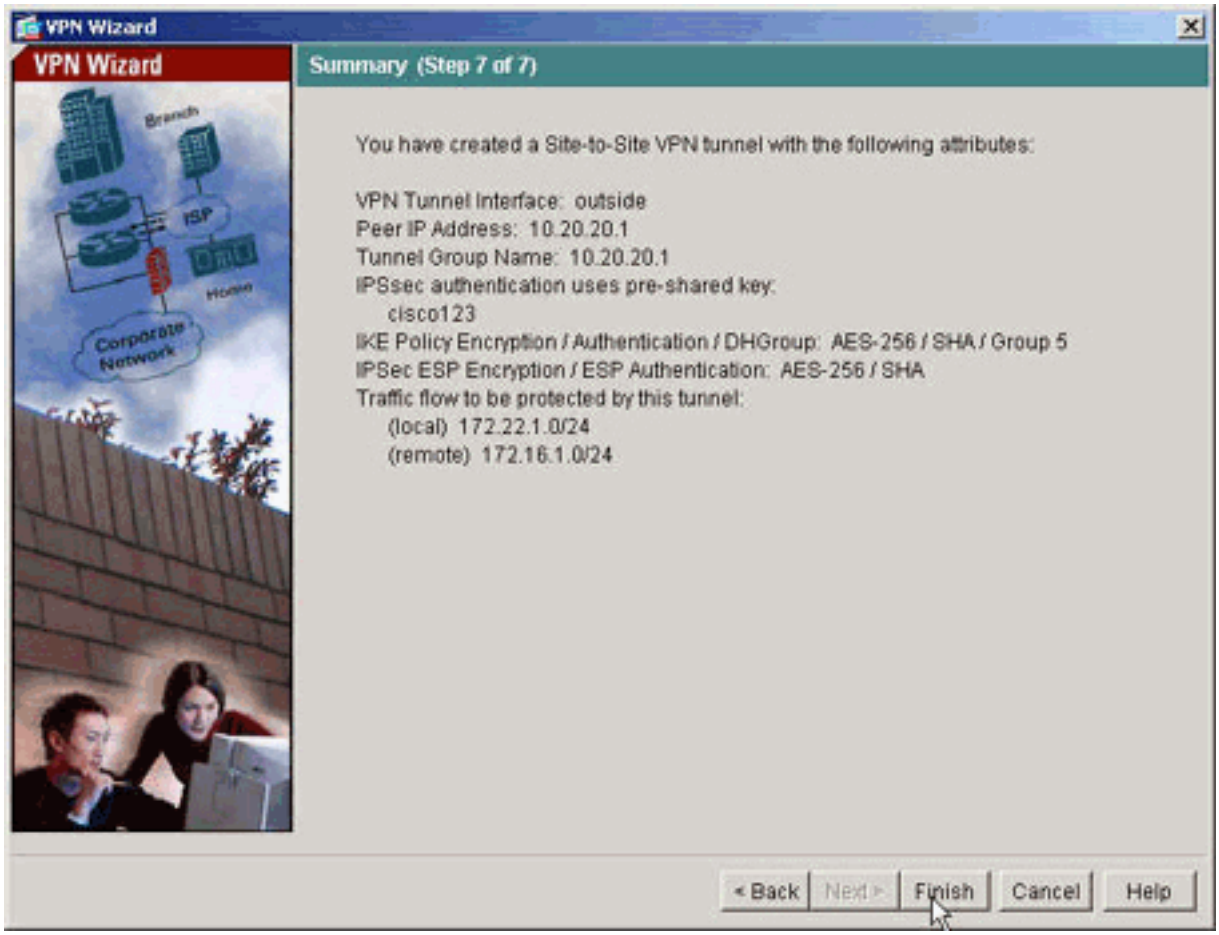


704.

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.**



Настройка PIX с помощью CLI

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#
```

Резервный туннель типа узел-узел

Для указания типа подключения для функции резервного соединения типа "узел-узел" данной записи криптографической карты используется команда crypto map set connection-type в режиме глобальной конфигурации. , `no`.

Синтаксис:

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

- **параметр answer-only указывает, что данный равноправный узел сначала только отвечает на входящие IKE-соединения во время первоначального частного обмена данными, чтобы определить соответствующий равноправный узел для подключения.**
- **параметр bidirectional указывает, что данный равноправный узел может принимать и инициировать соединения на основе данной записи криптографической карты.** Это - тип подключения по умолчанию для всех соединений узел-узел.
- **параметр originate-only указывает, что данный равноправный узел инициирует первый частный обмен данными, чтобы определить соответствующий равноправный узел для подключения.**

Команда crypto map set connection-type указывает типы подключения для функции резервирования соединения "LAN-LAN". Это позволяет узлам множественного резервирования быть заданными в одном конце соединения. Эта функция работает только между этими платформами:

- Два устройства безопасности серии 5500 Cisco ASA
- Устройство безопасности серии 5500 Cisco ASA и Cisco VPN 3000 Concentrator
- Устройство безопасности серии 5500 Cisco ASA и устройство безопасности, которое выполняет Версию программного обеспечения 7.0 Cisco PIX Security Appliance или

позже

Для настройки резервного прямого соединения локальных сетей Cisco рекомендует настроить один конец соединения как тип только источник с ключевым словом `originate-only` и конец с узлами множественного резервирования как тип только ответ с ключевым словом `answer-only`. **На конце типа "только источник" выполните команду crypto map set peer, чтобы упорядочить приоритет равноправных узлов**. Устройство безопасности типа только источник пытается выполнить согласование с первым узлом в списке. Если тот узел не отвечает, устройство безопасности прокладывает себе путь вниз список, пока или узел не отвечает или в списке больше нет узлов.

Когда настроено таким образом, узел типа только источник первоначально пытается установить составляющий собственность туннель и выполнить согласование с узлом. После того любой узел может установить обычное прямое соединение локальных сетей, и данные от любого конца могут инициировать туннельное соединение.

Примечание: При настройке VPN с IP-адресами множественных одноранговых телефонных соединений для крипто-записи VPN установлена с IP резервного узла, как только выключается основная адресуемая точка. Однако, как только основная адресуемая точка возвращается, VPN не вытесняет к основному IP - адресу. Необходимо вручную удалить существующий SA, чтобы повторно инициировать согласование VPN для переключения его на основной IP - адрес. Как заключение говорит, VPN вытесняют, не поддерживается в туннеле от узла к узлу.

Поддерживаемые типы резервных соединений LAN-LAN

Удаленная сторона	Главная сторона
`Originate-Only`	`Answer-Only`
`Bi-Directional`	`Answer-Only`
`Bi-Directional`	`Bi-Directional`

Пример

В данном примере осуществляется переход в режим глобальной конфигурации, выполняется команда crypto map mymap и задается тип подключения originate-only (только источник).

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

Очистка ассоциаций безопасности

В привилегированном режиме PIX используйте следующее команды:

- **clear [crypto] ipsec sa— удаляет все активные ассоциации безопасности IPSec.** *Ключевое слово crypto является необязательным.*
- **clear crypto isakmp sa— удаляет активные ассоциации безопасности IKE.** *Ключевое слово crypto является необязательным.*

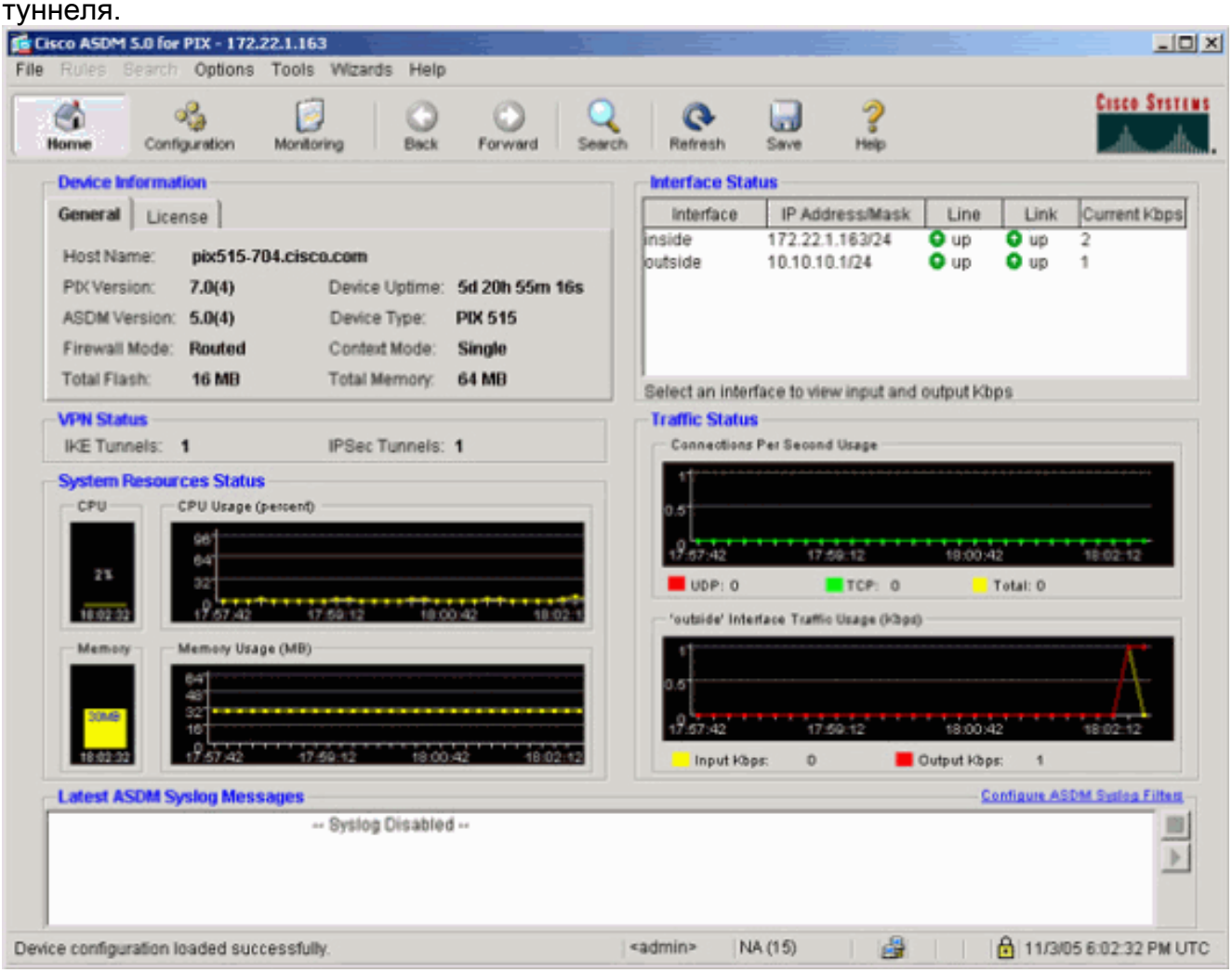
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

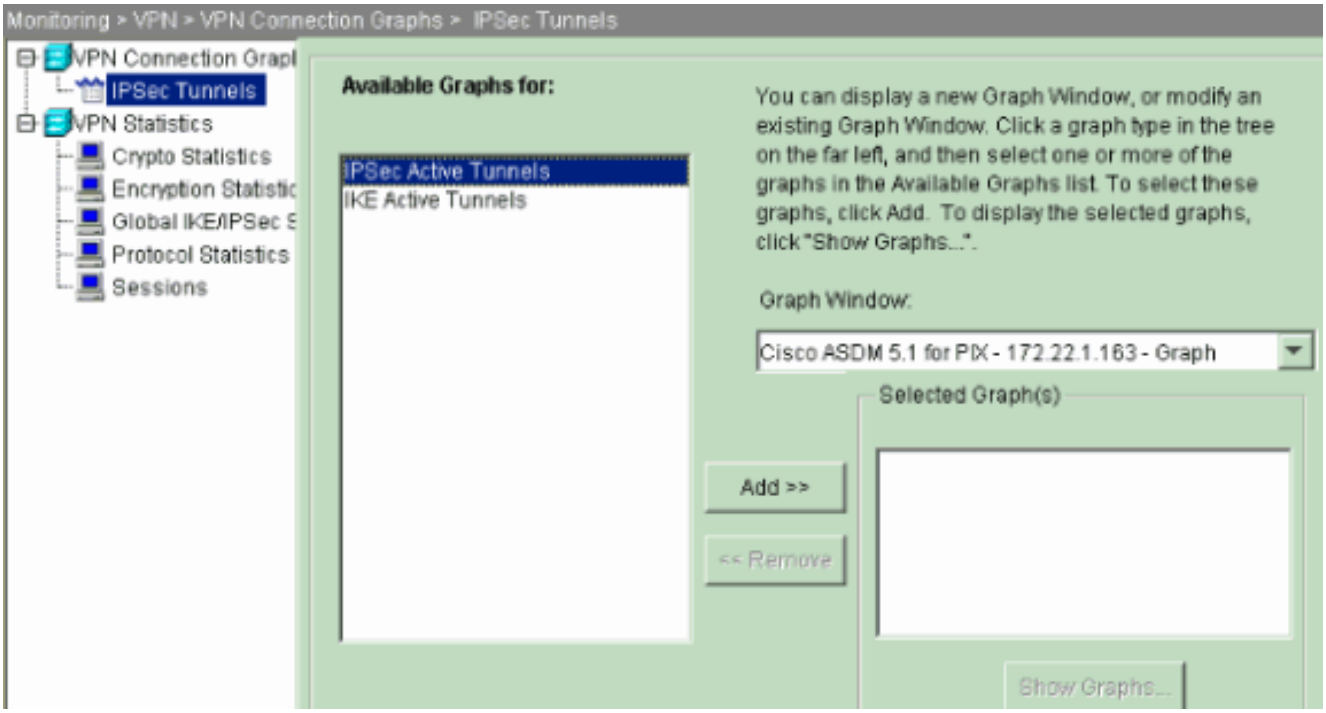
Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Если существует представляющий интерес трафик к узлу, туннель установлен между pix515-704 и PIX-02.

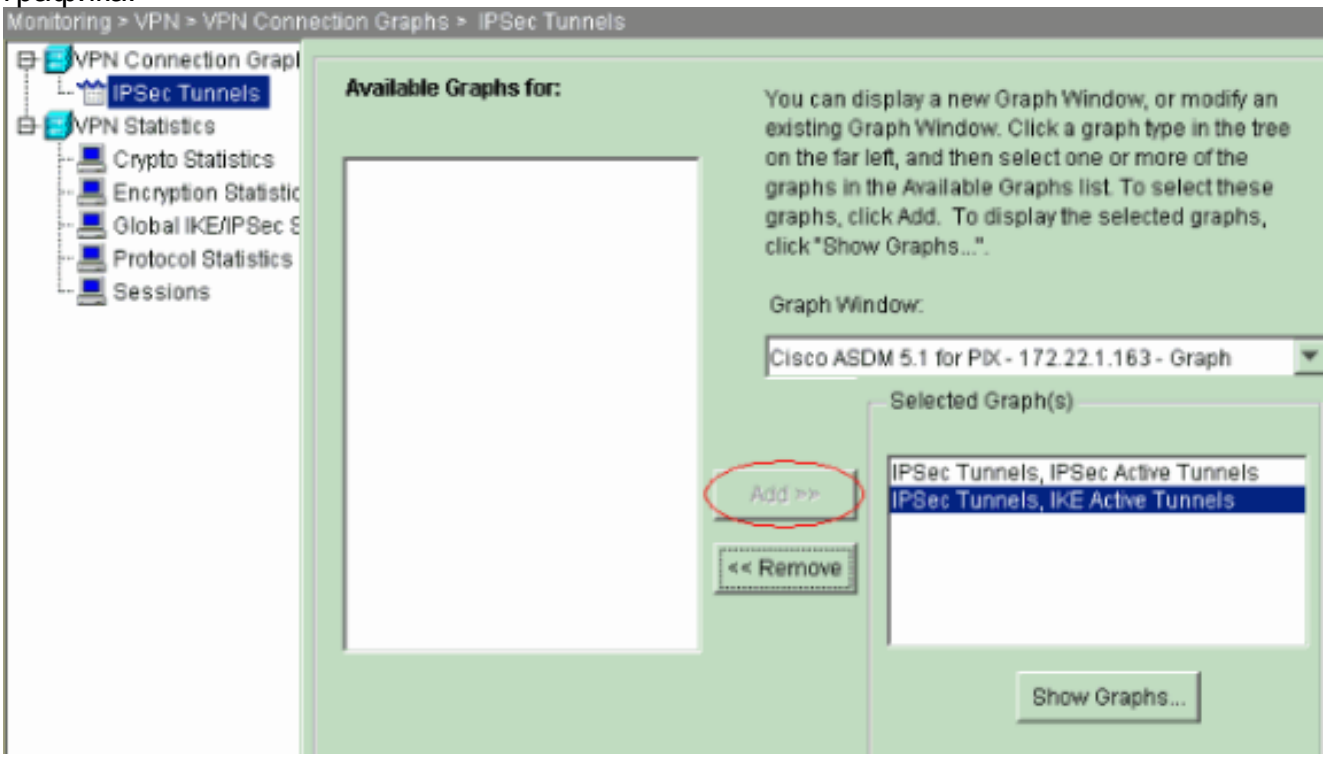
1. Просмотрите Состояние VPN под **Дом** в ASDM для проверки формирования туннеля.



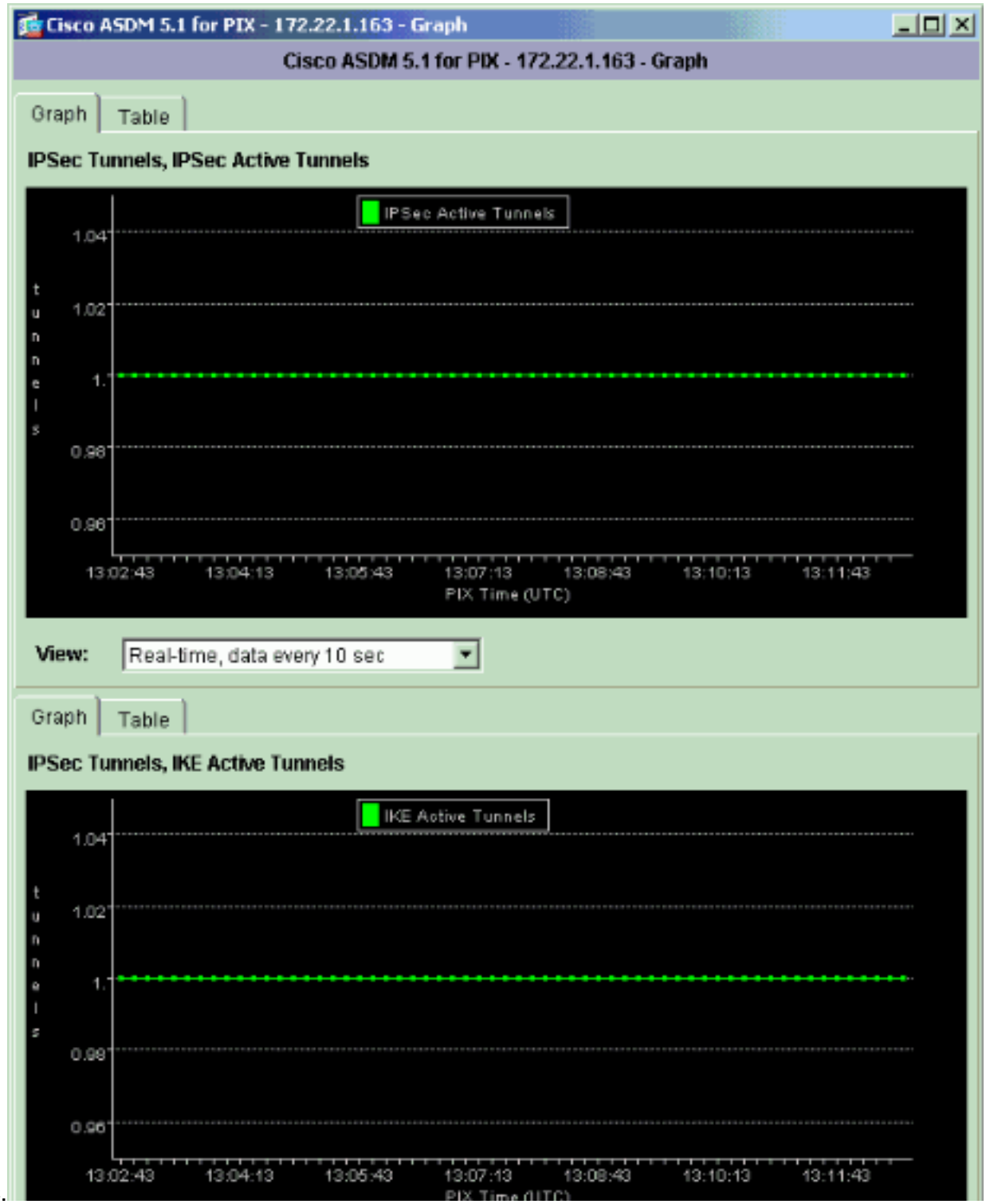
2. Выберите **Monitoring> VPN> VPN Connection Graphs> IPSec Tunnels** для проверки подробных данных об установке туннеля.



3. **Нажмите Add** для выбора графиков, доступных для просмотра в окне графика.

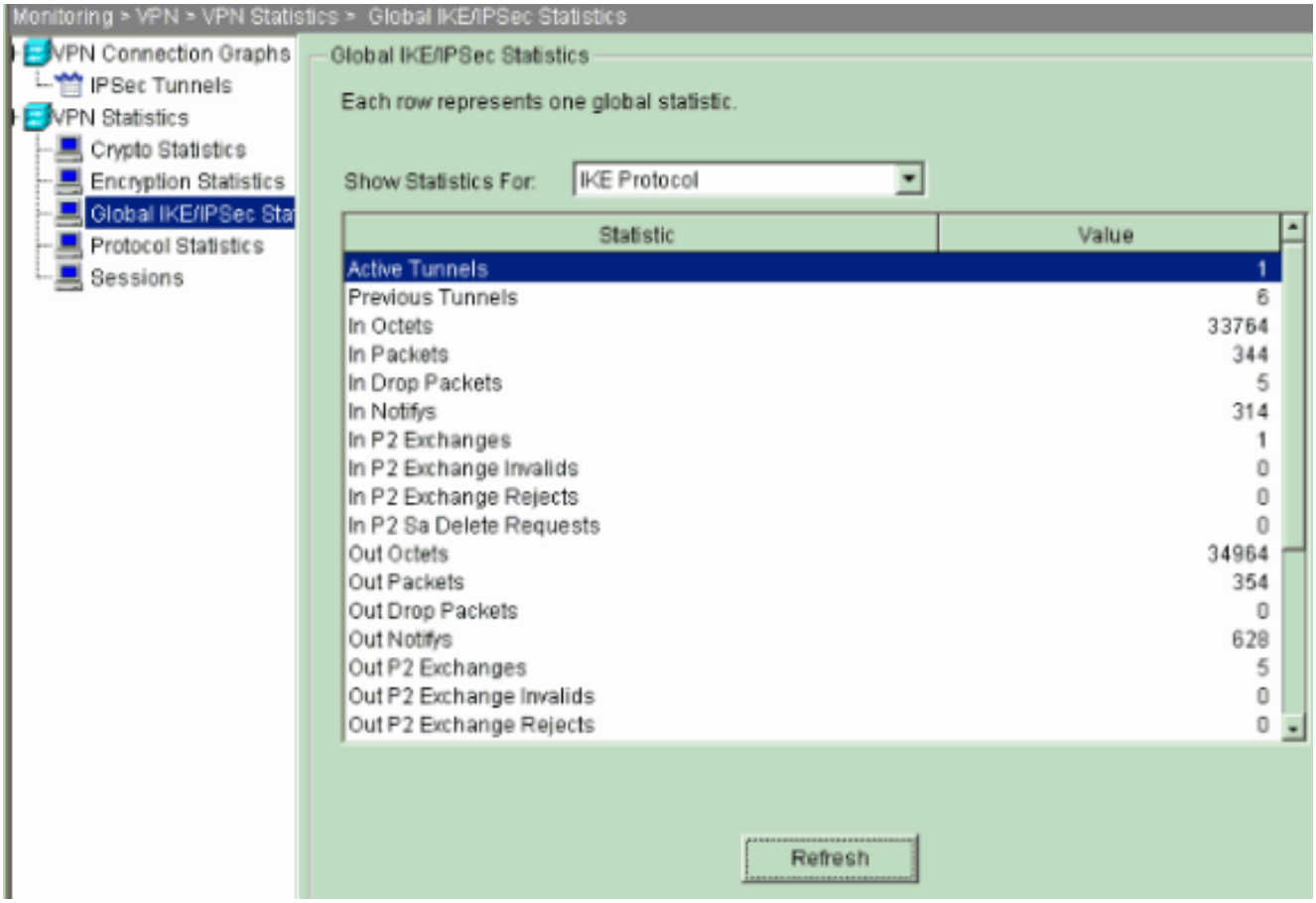


4. Нажмите **Show Graphs** для просмотра графиков обоих активных туннелей IKE и



IPsec.

5. Выберите **Monitoring> VPN> VPN Statistics> Global IKE/IPSec Statistics** для знания о статистической информации VPN-туннеля.



Можно также проверить формирование туннелей с помощью CLI. **Задайте команду show crypto isakmp sa, чтобы проверить формирование туннелей, и выполните команду show crypto ipsec sa, чтобы узнать количество инкапсулированных, шифрованных и т. д. пакетов.**

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
```

Устранение неполадок

БЕЗОПАСНАЯ ПЕРЕСЫЛКА (PFS)

При согласовании IPsec безопасная пересылка (PFS) позволяет гарантировать отсутствие связи нового ключа шифрования со всеми предыдущими ключами. Или включите или отключите безопасную пересылку (PFS) на обоих равноправные пользователи туннеля, иначе Туннель IPSec L2L не установлен в PIX/ASA.

По умолчанию безопасная пересылка (PFS)отключена. **Для включения PFS используйте команду pfs с ключевым словом enable в режиме настройки групповой политики.** *Чтобы отключить PFS, введите ключевое слово disable.*

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

Чтобы удалить атрибут PFS из текущей конфигурации, введите эту команду с ключом no. Групповая политика может наследовать значение для безопасной пересылки (PFS) от другой групповой политики. **Введите эту команду с ключом no, чтобы предотвратить наследование значения.**

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

Management-Access

В этом разделе описывается процесс устранения неполадок конфигурации.

Внутренний интерфейс PIX не может быть пропингован от другого конца туннеля, пока команда management-access не настроена в режиме глобальной конфигурации.

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

Команды "debug"

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

debug crypto isakmp– отображает данные отладки подключений IPsec и первый набор атрибутов, отклоняемых из-за несовместимости на обоих концах.

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 - отображаются данные отладки подключений 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
```

Дополнительные сведения

- Создание резервных туннелей между брандмауэрами с помощью PDM
- 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
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация