Пример Конфигурации "VPN между продуктами Sonicwall и Cisco Security Appliance

Содержание

Введение

В этом документе показано, как настроить туннель IPsec с предварительно разделенными ключами для обмена данными между двумя частными сетями, используя агрессивный и основной режимы. В этом примере частная сеть с адресным диапазоном 192.168.1.x находится за Cisco Security Appliance (PIX/ASA), а частная сеть с адресным диапазоном 172.22.1.x — за межсетевым экраном Sonicwall™ TZ170.

Предварительные условия

Требования

Рассматриваемая процедура настройки предполагает выполнение следующих условий:

Трафик из Cisco Security Appliance и из Sonicwall TZ170 должен быть направлен в Интернет (представленный здесь сетями 10.x.x.x networks) перед запуском этой конфигурации.

Пользователи должны быть знакомы с принципами согласования IPsec. Этот процесс можно разделить на пять этапов, включая два этапа обмена ключами в Интернете (IKE).

Туннель IPsec инициирован содержательным трафиком. Трафик считается содержательным при передаче между двумя одноранговыми узлами IPsec.

На первом этапе обмена ключами (IKE) одноранговые узлы IPSec согласуют установленную политику сопоставлений безопасности (SA) IKE. По завершении аутентификации одноранговых узлов создается защищенный туннель с применением протокола ISAKMP (Протокол управления ключами Ассоциации безопасности Интернет).

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.

Туннель IPsec создан, и данные передаются между узлами IPsec на основании параметров IPsec, настроенных в наборах преобразования IPsec.

Разъединение туннеля IPSec выполняется при удалении сопоставлений безопасности (IPSec SA) или по истечении срока их действия.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Cisco PIX 515E версия 6.3(5)

Cisco PIX 515 версия 7.0(2)

Sonicwall TZ170, SonicOS Standard 2.2.0.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

Родственные продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения.

Конфигурация PIX 6.3(5) может использоваться со всеми остальными продуктами межсетевого экрана Cisco PIX, работающими под управлением этой версии ПО (PIX 501, 506 и т.д.)

Конфигурация PIX/ASA 7.0(2) может использоваться только на устройствах, работающих под управлением последовательности версий ПО PIX 7.0 (кроме 501, 506 и, возможно, некоторых более старых 515s), а также Cisco 5500 серии ASA.

Условные обозначения

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

Настройка

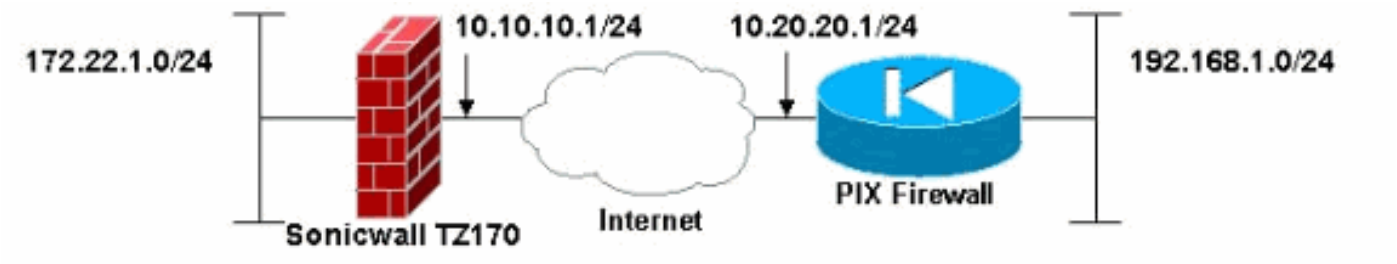
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание. Для поиска дополнительной информации о командах, приведенных в данном документе, используйте инструмент Средство поиска команд (только для зарегистрированных пользователей).

Примечание. В агрессивном режиме IPsec Sonicwall должен инициировать туннель IPsec для PIX. Это можно увидеть при анализе отладки этой конфигурации. Это является обязательным в случае работы в агрессивном режиме IPsec.

Схема сети

В настоящем документе используется следующая схема сети:



Настройка Sonicwall

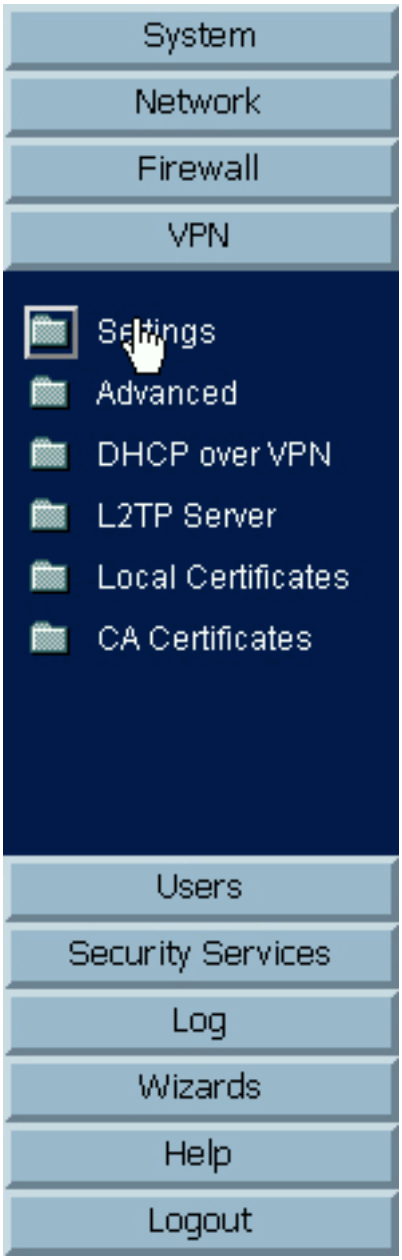
Настройка Sonicwall TZ170 выполняется через веб-интерфейс.

Выполните следующие действия:

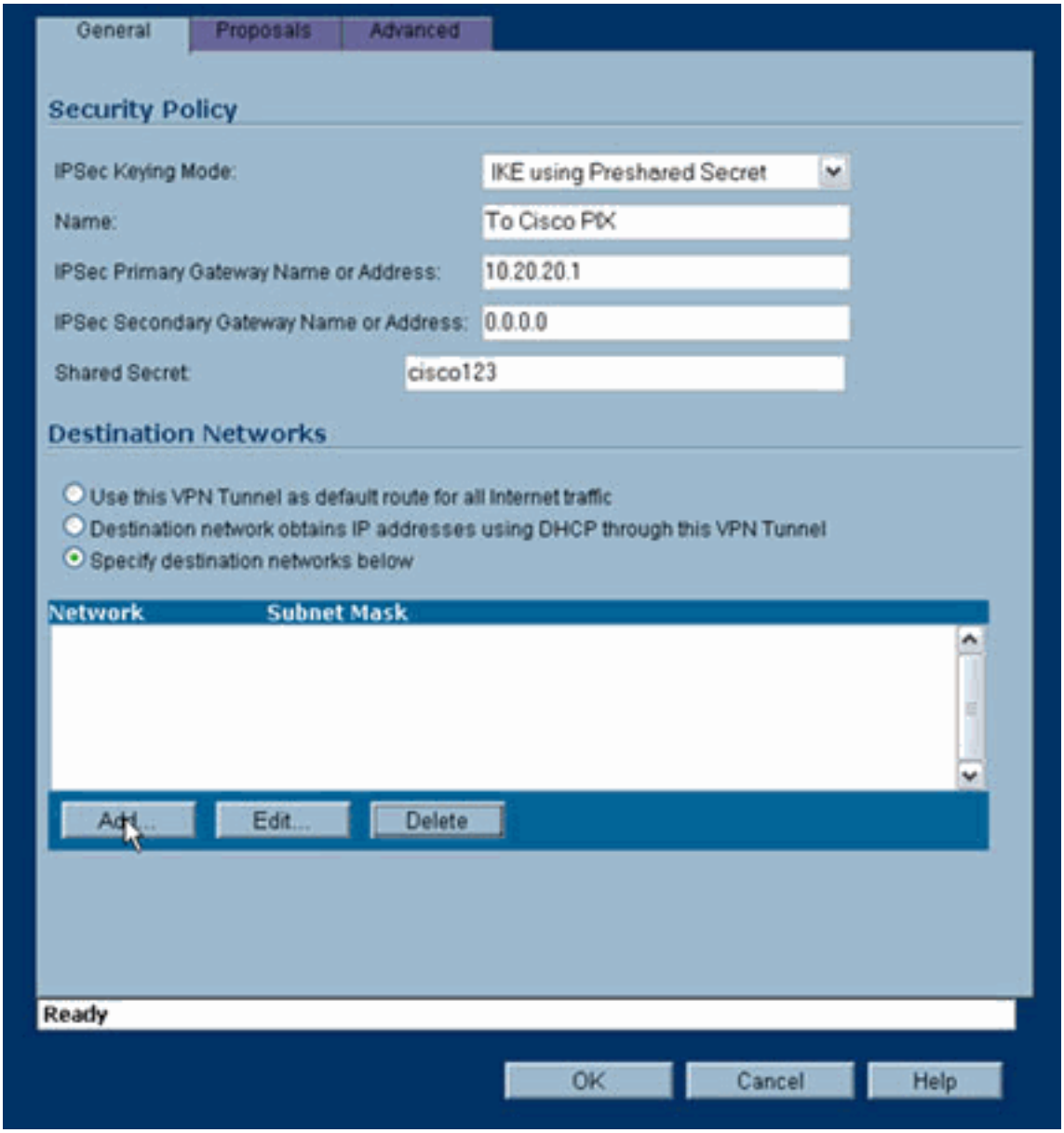
Подключитесь к IP-адресу маршрутизатора на одном из внутренних интерфейсов с помощью стандартного веб-браузера.

Появляется окно входа.

Войдите в устройство Sonicwall и выберите **VPN > Settings**.

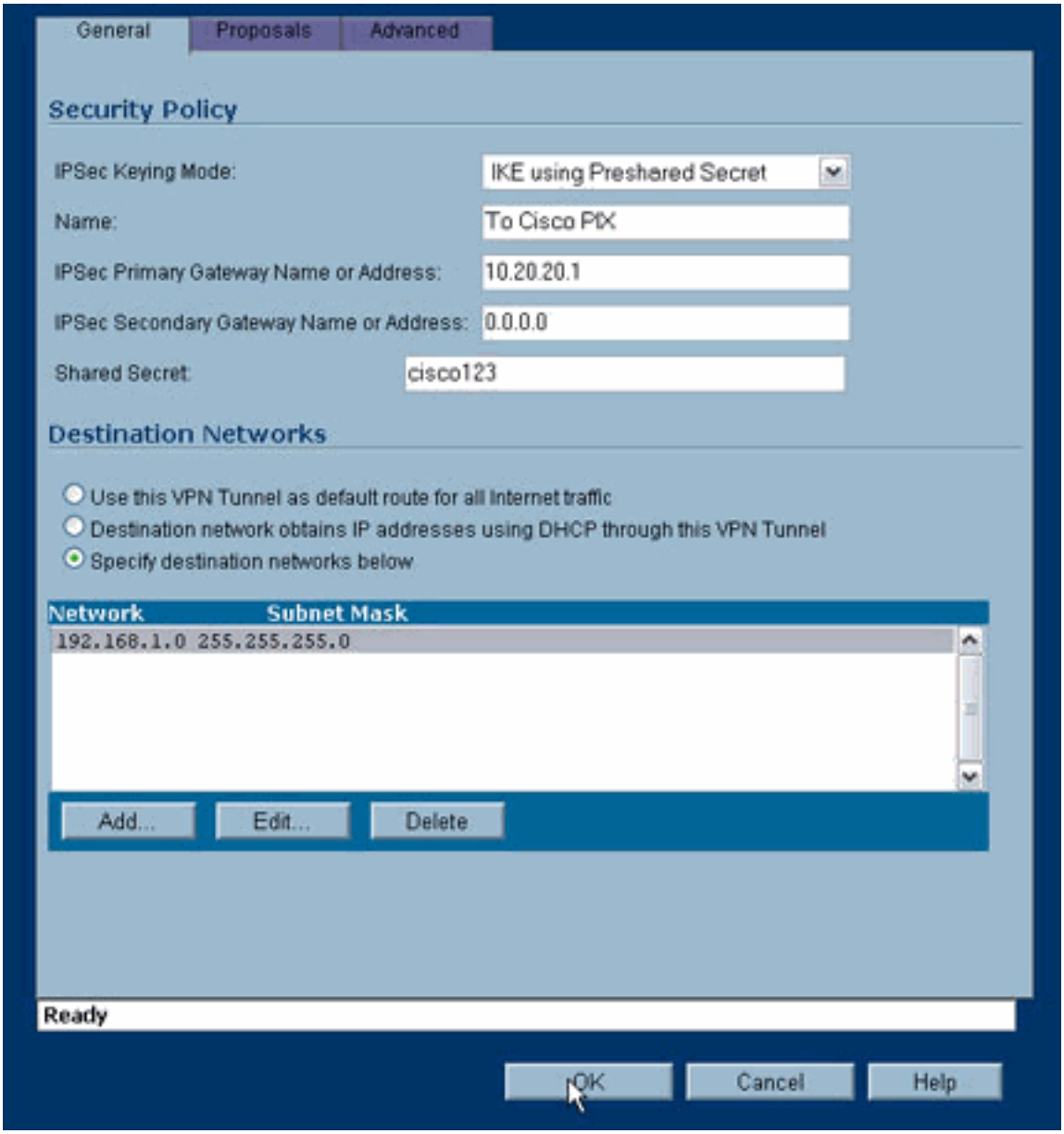


Введите IP-адрес узла VPN и общий ключ. Нажмите **Add** в пункте Destination Networks ("Сети назначения").



Введите сеть назначения.

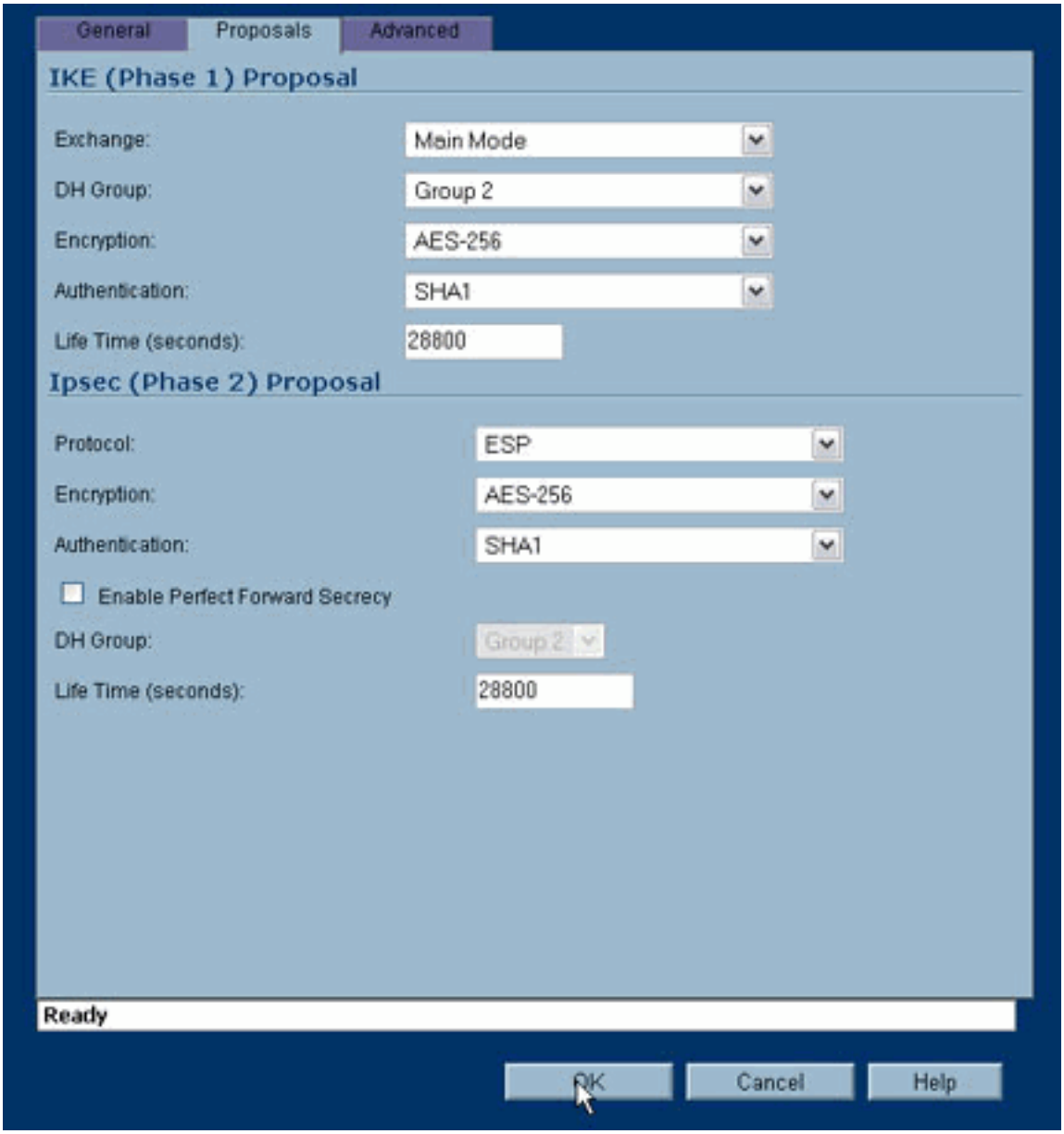
Отображается окно Settings ("Настройки") .



В верхней части окна настроек щелкните вкладку Proposals ("Предложения").

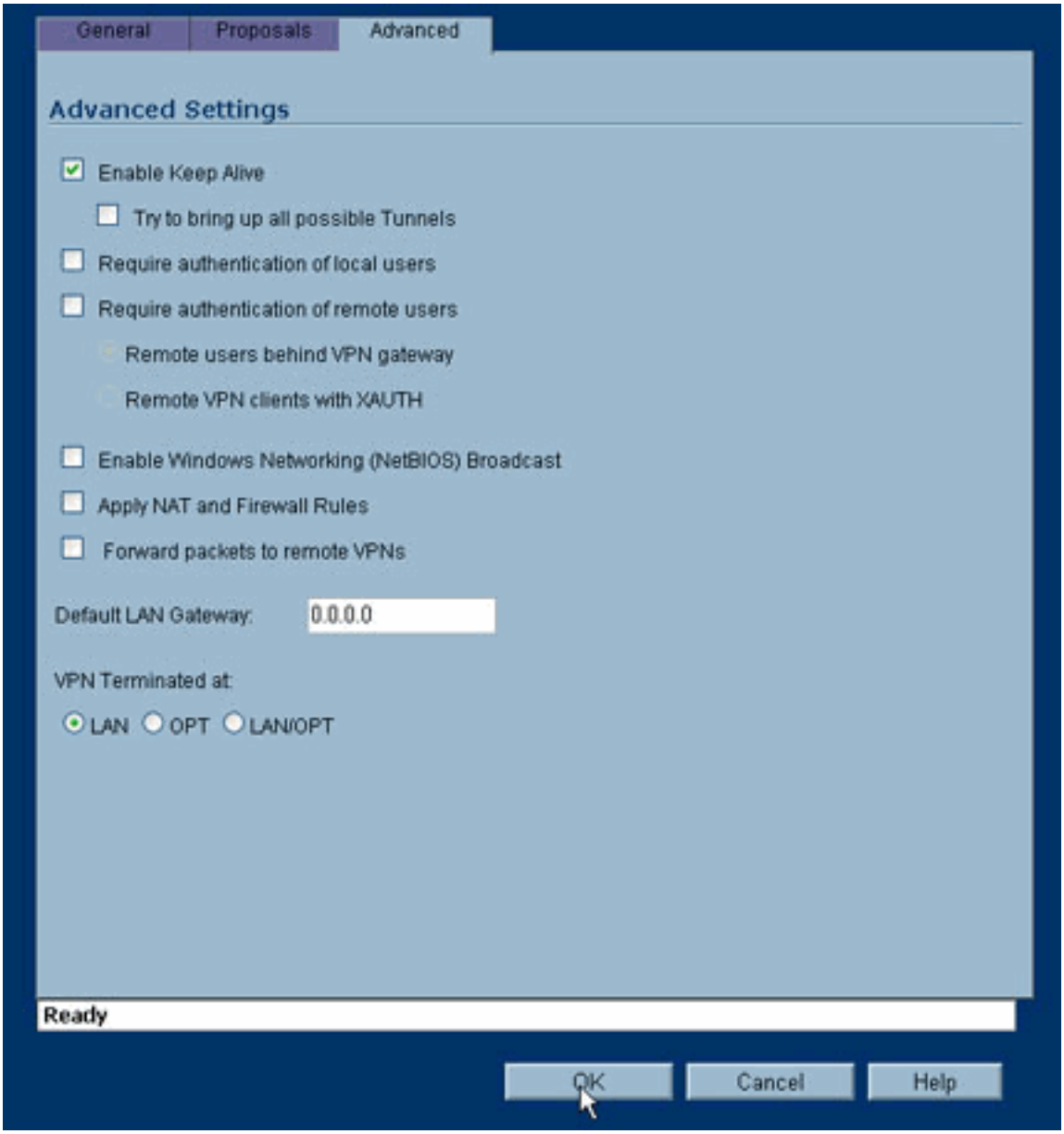
Выберите обмен, который планируется использовать для этой конфигурации (основной режим или агрессивный режим), а также остальные настройки первого и второго этапов.

В конфигурации примера используется шифрование AES-256 для обоих этапов, алгоритм хэширования SHA1 для аутентификации и 1024-битовый алгоритм Диффи-Хеллмана группы 2 для политики IKE.



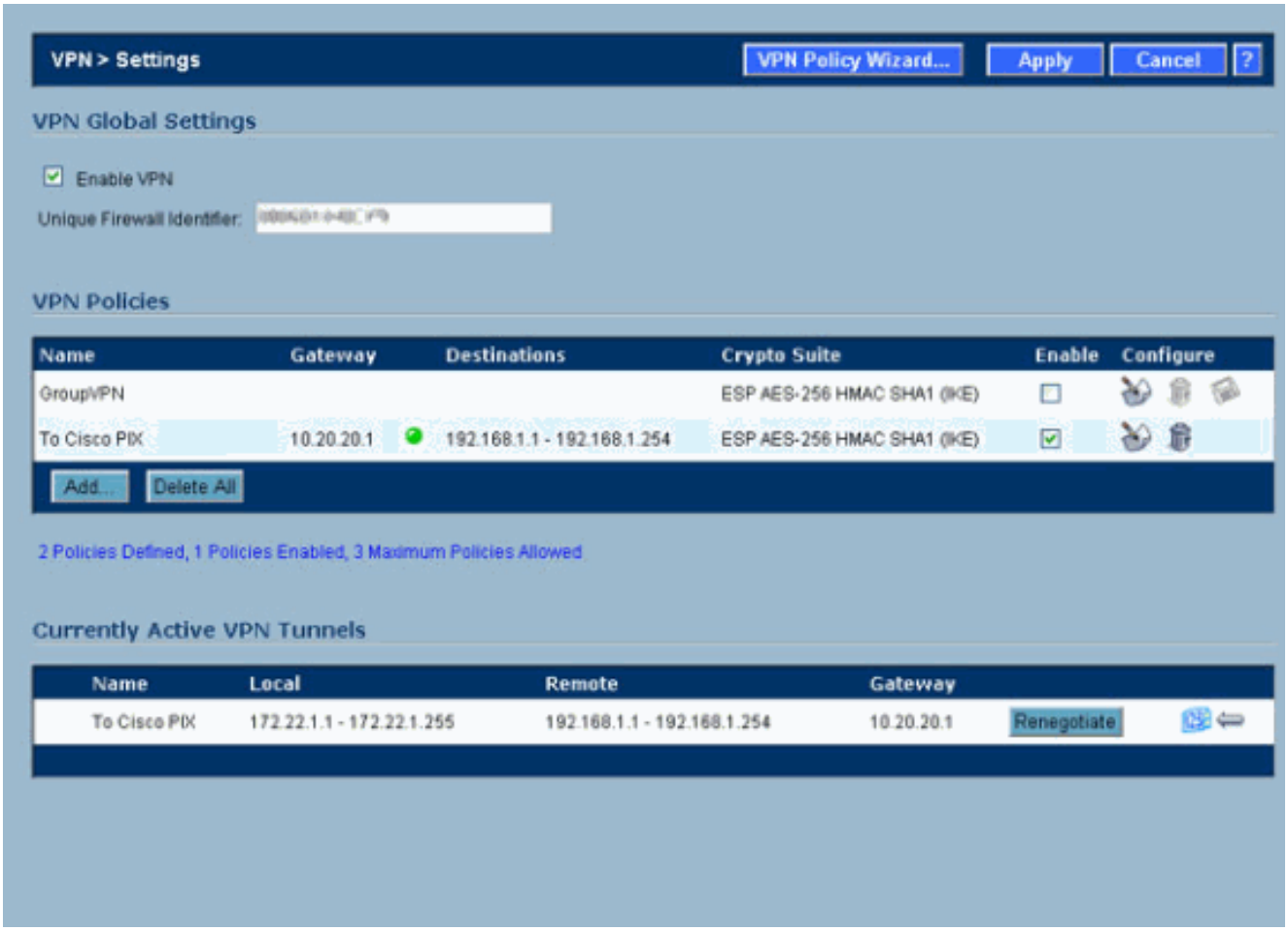
Щелкните вкладку Advanced ("Дополнительно").

На этой вкладке имеются дополнительные параметры, которые также можно настроить. Это настройки, используемые для данного примера конфигурации.



Нажмите кнопку **OK**.

После завершения этой настройки и настройки удаленного PIX окно Settings должно быть похоже на это окно примера.



Настройка основного режима IPsec

В этом разделе используются следующие конфигурации:

- Cisco PIX 515e версия 6.3(5)
- Cisco PIX 515 версия 7.0(2)

Cisco PIX 515e версия 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
fixup protocol dns maximum-length 512 fixup protocol ftp
21 fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol http 80 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol sip 5060 fixup
protocol sip udp 5060 fixup protocol skinny 2000 fixup
protocol smtp 25 fixup protocol sqlnet 1521 fixup
protocol tftp 69 names !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
```

```
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION: !--- Defines the transform set
for Phase 2 encryption and authentication. !---
Austinlab is the name of the transform set that uses
aes-256 encryption !--- as well as the SHA1 hash
algorithm for authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies IKE is used to establish the IPsec SAs
for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
map . crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map. crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Specifies the interface
to use for the IPsec tunnel.

isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used with the preshared key cisco123. isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
```

```
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 версия 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS®. !--- This output configures the IP
address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. 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 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies the ACL pixtosw to use with this map.
crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
```

```
!--- PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration !--- settings specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

Настройка агрессивного режима IPsec

В этом разделе используются следующие конфигурации:

- Cisco PIX 515e версия 6.3(5)
- Cisco PIX 515 версия 7.0(2)

Cisco PIX 515e версия 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
fixup protocol dns maximum-length 512 fixup protocol ftp
21 fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol http 80 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol sip 5060 fixup
protocol sip udp 5060 fixup protocol skinny 2000 fixup
protocol smtp 25 fixup protocol sqlnet 1521 fixup
protocol tftp 69 names !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
```

```
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
the name of the transform set that uses aes-256
encryption !--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map ciscopix for the transform
set. crypto dynamic-map ciscopix 1 set transform-set
austinlab !--- Specifies the IKE that should be used to
establish SAs !--- for the dynamic map. crypto map
dynmaptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
the settings above to the outside interface. crypto map
dynmaptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
.
isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used as the preshared key "cisco123". isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 версия 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
```

```
to Cisco IOS. !--- This output configures the IP
address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. 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 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map "ciscopix" for the defined
transform set. crypto dynamic-map ciscopix 1 set
transform-set austinlab !--- Specifies that IKE should
be used to establish SAs !--- for the defined dynamic
map. crypto map dynmaptosw 66 ipsec-isakmp dynamic
ciscopix !--- Applies the settings to the outside
interface. crypto map dynmaptosw interface outside !---
PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
```

```
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Интерпретатор выходных данных – OIT (только для зарегистрированных пользователей) поддерживает ряд команд **show**. Посредством OIT можно анализировать выходные данные команд **show**.

show crypto isakmp sa—отображает все текущие IKE SA на одноранговом узле.

show crypto ipsec sa — отображает настройки, используемые текущими SA.

В этих таблицах показаны выходные данные некоторых отладок для основного и агрессивного режимов в PIX 6.3(5) и PIX 7.0(2) после полной установки туннеля.

Примечание. Этих данных должно быть достаточно для установки туннеля IPsec между этими двумя типами оборудования. Если у вас имеются какие-либо комментарии, воспользуйтесь формой обратной связи в левой части этого документа.

Cisco PIX 515e версия 6.3(5) — основной режим

Cisco PIX 515 версия 7.0(2)- основной режим

Cisco PIX 515e версия 6.3(5) — агрессивный режим

Cisco PIX 515 версия 7.0(2) — агрессивный режим

Cisco PIX 515e версия 6.3(5) — основной режим

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src         state     pending
created
      10.10.10.1       10.20.20.1    QM_IDLE          0
1
pix515e-635#



pix515e-635#show crypto ipsec sa
```

```
          interface: outside
          Crypto map tag: maptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
          remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
          current_peer: 10.10.10.1:500
          PERMIT, flags={origin_is_acl,}
          #pkts encaps: 4, #pkts encrypt: 4, #pkts
digest 4
          #pkts decaps: 4, #pkts decrypt: 4, #pkts
verify 4
          #pkts compressed: 0, #pkts decompressed: 0
          #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
          #send errors 1, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
          path mtu 1500, ipsec overhead 72, media mtu
1500
          current outbound spi: ed0afa33

 inbound esp sas:
          spi: 0xac624692(2892121746)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 1, crypto map: maptosw
          sa timing: remaining key lifetime (k/sec):
(4607999/28718)
          IV size: 16 bytes
          replay detection support: Y


          inbound ah sas:


          inbound pcp sas:


          outbound esp sas:
          spi: 0xed0afa33(3976919603)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 2, crypto map: maptosw
          sa timing: remaining key lifetime (k/sec):
(4607999/28718)
          IV size: 16 bytes
          replay detection support: Y


          outbound ah sas:


          outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 версия 7.0(2) — основной режим

```
pix515-702#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: 10.10.10.1
           Type : L2L Role : initiator
           Rekey : no State : MM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
interface: outside
    Crypto map tag: maptosw, local addr: 10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: 2D006547

 inbound esp sas:
           spi: 0x309F7A33 (815757875)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28739)
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0x2D006547 (755000647)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28737)
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

Cisco PIX 515e версия 6.3(5) — агрессивный режим

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.20.20.1       10.10.10.1    QM_IDLE         0
1
```

```
pix515e-635#show crypto ipsec sa


           interface: outside
           Crypto map tag: dynmaptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={}
           #pkts encaps: 0, #pkts encrypt: 0, #pkts
digest 0
           #pkts decaps: 0, #pkts decrypt: 0, #pkts
verify 0
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
           #send errors 0, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
           path mtu 1500, ipsec overhead 72, media mtu
1500
           current outbound spi: efb1149d

 inbound esp sas:
           spi: 0x2ad2c13c(718455100)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 2, crypto map: dynmaptosw
           sa timing: remaining key lifetime (k/sec):
(4608000/28736)
           IV size: 16 bytes
           replay detection support: Y


           inbound ah sas:


           inbound pcp sas:


           outbound esp sas:
           spi: 0xefb1149d(4021359773)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 1, crypto map: dynmaptosw
           sa timing: remaining key lifetime (k/sec):
(4608000/28727)
           IV size: 16 bytes
           replay detection support: Y


           outbound ah sas:


           outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 версия 7.0(2) — агрессивный режим

```
pix515-702#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: 10.10.10.1
           Type : L2L Role : responder
           Rekey : no State : AM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
           interface: outside
           Crypto map tag: ciscopix, local addr:
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: D7E2F5FD

 inbound esp sas:
           spi: 0xDCBF6AD3 (3703532243)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28703
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0xD7E2F5FD (3621975549)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28701
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении неполадок.

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFCs)
- Cisco Systems – техническая поддержка и документация