ASA/PIX: Пример настройки туннеля IPSec между устройством обеспечения безопасности и маршрутизатором IOS по локальной сети

Содержание

Введение

В данном документе описан способ настройки туннеля IPsec между PIX Security Appliance начиная с версии 7.x или Adaptive Security Appliance (ASA) с одной внутренней сетью и маршрутизатором 2611, в котором работает криптографический образ. Для упрощения используются статические маршруты.

Дополнительные сведения о настройке туннеля "ЛВС-ЛВС" между маршрутизатором и PIX см. в документе Настройка IPsec - между маршрутизатором и PIX.

Дополнительные сведения о настройке туннеля "ЛВС-ЛВС" между брандмауэром PIX и концентратором Cisco VPN 3000 см. в документе Пример настройки туннеля IPsec "ЛВС-ЛВС" между концентратором Cisco VPN 3000 и брандмауэром PIX.

Дополнительные сведения о настройке туннеля "ЛВС-ЛВС" между PIX и концентратором VPN см. в документе Пример настройки туннеля IPsec между PIX и концентратором VPN.

Дополнительные сведения о туннелях LAN-LAN между устройствами PIX, которые позволяют клиентам VPN получать доступ к промежуточным PIX через концентратор PIX, см. документ Пример настройки усовершенствованной связи оконечных PIX/ASA 7.x с

клиентами через VPN с использованием аутентификации TACACS+.

См. SDM: VPN Защищенного взаимодействия между сетями Site-to-Site IPsec Между ASA/PIX и Примером конфигурации Маршрутизатора IOS для узнавания больше о том же сценарии, где Устройство безопасности PIX/ASA работает под управлением ПО версии 8. x.

См. Профессионала Конфигурации: VPN Защищенного взаимодействия между сетями Site-to-Site IPsec Между ASA/PIX и Примером конфигурации Маршрутизатора IOS для узнавания больше о том же сценарии, где связанную с ASA конфигурацию показывают с помощью GUI ASDM и связанной с маршрутизатором конфигурации, показывают с помощью GUI CP Cisco.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- PIX-525 с программным обеспечением PIX версии 7.0
- Маршрутизатор Cisco 2611 под управлением операционной системы Cisco IOS® Release 12.2(15)T13

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.

Условные обозначения

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

Общие сведения

В PIX команды access-list и nat 0 работают совместно. Когда пользователь в сети 10.1.1.0 получает доступ к сети 10.2.2.0, используется список доступа для разрешения шифрования трафика сети 10.1.1.0 без преобразования сетевых адресов (NAT). **В маршрутизаторе команды route-map и access-list используются для разрешения шифрования трафика сети 10.2.2.0 без NAT.** Однако когда те же самые пользователи направляются в любое другое место, их адрес преобразуется в 172.17.63.230 посредством преобразования адресов портов (PAT).

Ниже приведены команды конфигурации, требуемые для устройства защиты PIX, чтобы для трафика туннеля не использовался режим PAT, а для трафика в Интернет режим PAT использовался

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

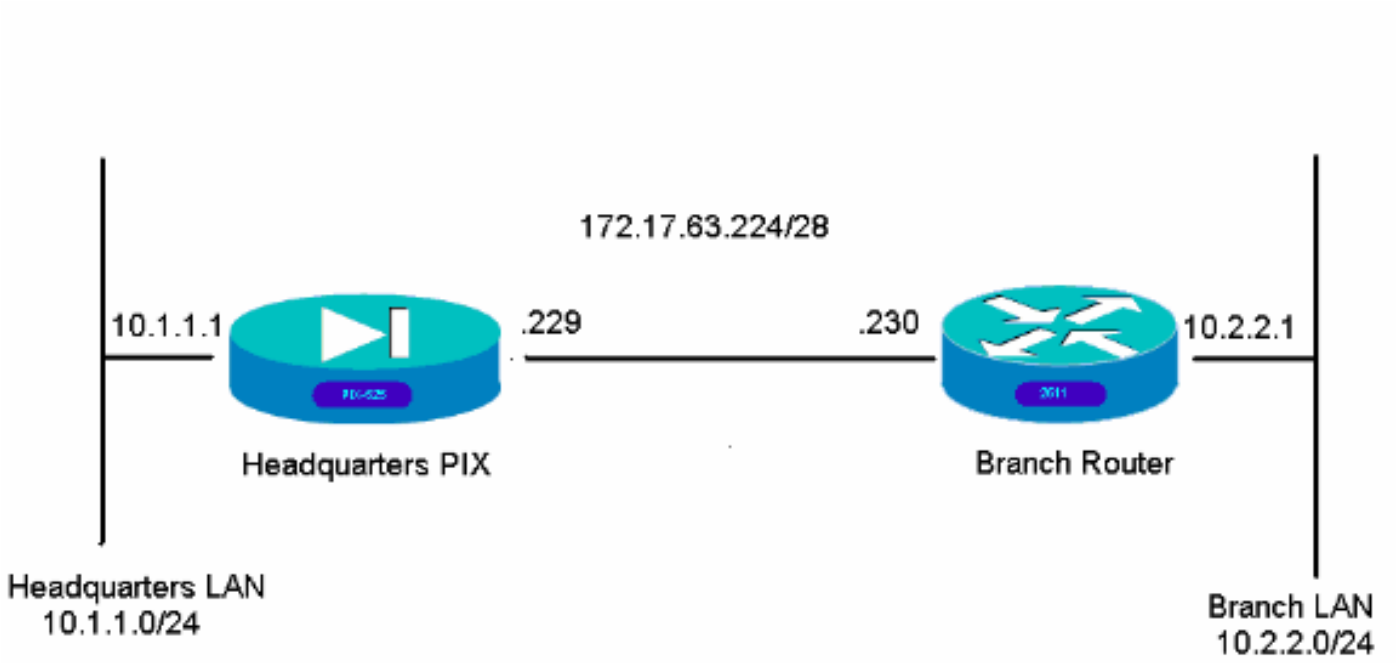
Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Данные примеры настройки приведены для интерфейса командной строки. Если вы предпочитаете выполнять настройку при помощи ASDM, см. раздел Настройка с помощью Adaptive Security Device Manager (ASDM) данного документа.

- Центральные PIX
- Маршрутизатор подразделения

Центральные PIX
HQPIX(config)#**show run** PIX Version 7.0(0)102 names ! **interface Ethernet0 description WAN interface nameif outside security-level 0 ip address 172.17.63.229**

```
255.255.255.240 ! interface Ethernet1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
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
HQPIX domain-name cisco.com ftp mode passive clock
timezone AEST 10 access-list Ipsec-conn extended permit
ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 access-
list nonat extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0 pager lines 24 logging enable
logging buffered debugging mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside asdm image flash:/asdmfile.50073 no
asdm history enable arp timeout 14400 nat-control global
(outside) 1 interface nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 access-group 100
in interface inside route outside 0.0.0.0 0.0.0.0
172.17.63.230 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout
uauth 0:05:00 absolute aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
partner protocol tacacs+ username cisco password
3USUcOPFUiMCO4Jk encrypted http server enable http
10.1.1.2 255.255.255.255 inside no snmp-server location
no snmp-server contact snmp-server community public
snmp-server enable traps snmp crypto ipsec transform-set
avalanche esp-des esp-md5-hmac crypto ipsec security-
association lifetime seconds 3600 crypto ipsec df-bit
clear-df outside crypto map forsberg 21 match address
Ipsec-conn crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside isakmp identity
address isakmp enable outside isakmp policy 1
authentication pre-share isakmp policy 1 encryption 3des
isakmp policy 1 hash sha isakmp policy 1 group 2 isakmp
policy 1 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 telnet
timeout 5 ssh timeout 5 console timeout 0 tunnel-group
172.17.63.230 type ipsec-l2l tunnel-group 172.17.63.230
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map asa_global_fw_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
inspect http ! service-policy asa_global_fw_policy
global Cryptochecksum:3a5851f7310d14e82bdf17e64d638738 :
end SV-2-8#
```

Маршрутизатор подразделения

```
BranchRouter#show run Building configuration... Current
configuration : 1719 bytes ! ! Last configuration change
at 13:03:25 AEST Tue Apr 5 2005 ! NVRAM config last
updated at 13:03:44 AEST Tue Apr 5 2005 ! version 12.2
service timestamps debug datetime msec service
```

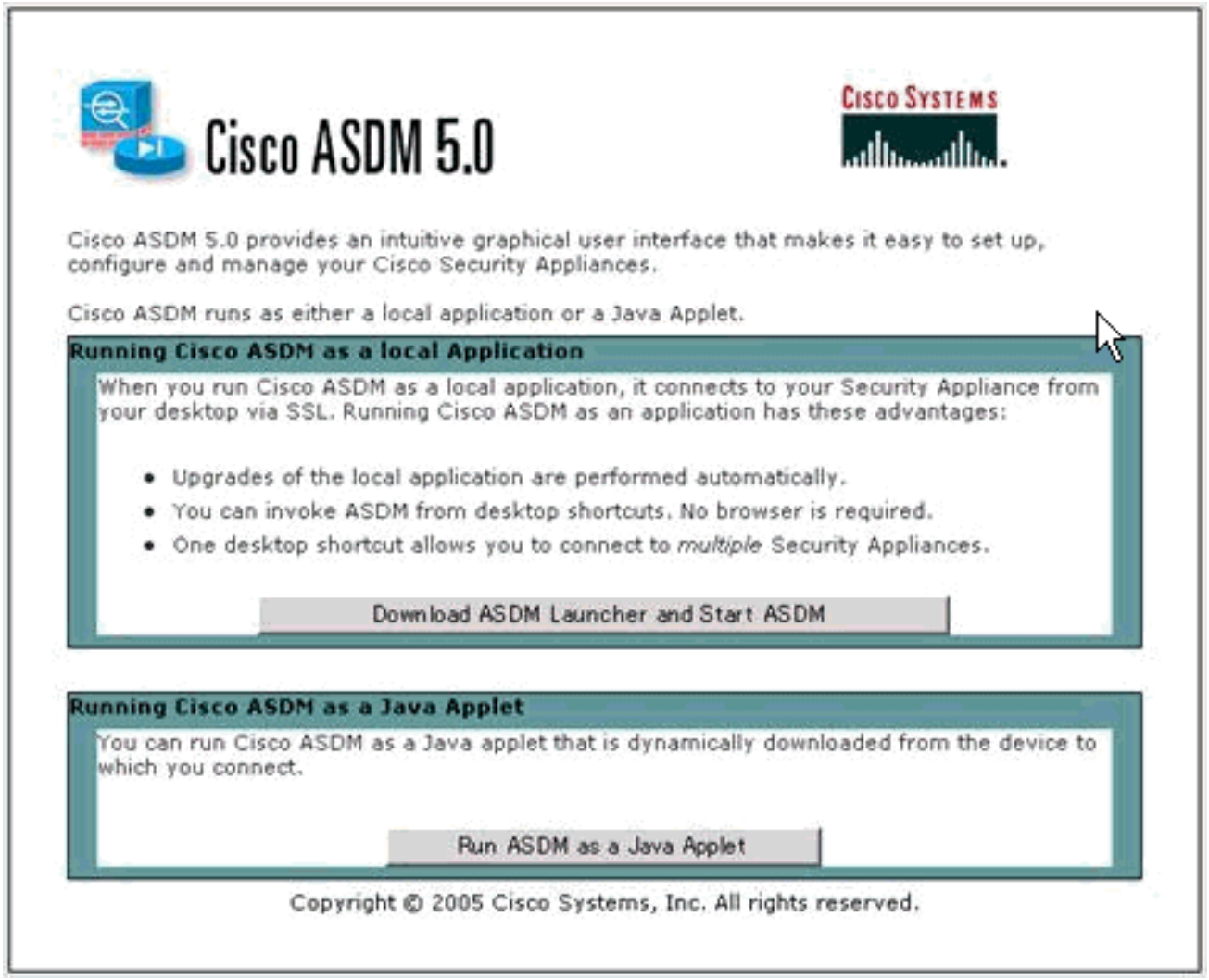
```
timestamps log uptime no service password-encryption !
hostname BranchRouter ! logging queue-limit 100 logging
buffered 4096 debugging ! username cisco privilege 15
password 0 cisco memory-size iomem 15 clock timezone
AEST 10 ip subnet-zero ! ! ! ip audit notify log ip
audit po max-events 100 ! ! ! crypto isakmp policy 11
encr 3des authentication pre-share group 2 crypto isakmp
key cisco123 address 172.17.63.229 ! ! crypto ipsec
transform-set sharks esp-des esp-md5-hmac ! crypto map
nolan 11 ipsec-isakmp set peer 172.17.63.229 set
transform-set sharks match address 120 ! ! ! ! ! ! ! ! !
! no voice hpi capture buffer no voice hpi capture
destination ! ! mta receive maximum-recipients 0 ! ! ! !
interface Ethernet0/0 ip address 172.17.63.230
255.255.255.240 ip nat outside no ip route-cache no ip
mroute-cache half-duplex crypto map nolan ! interface
Ethernet0/1 ip address 10.2.2.1 255.255.255.0 ip nat
inside half-duplex ! ip nat pool branch 172.17.63.230
172.17.63.230 netmask 255.255.255.0 ip nat inside source
route-map nonat pool branch overload no ip http server
no ip http secure-server ip classless ip route 10.1.1.0
255.255.255.0 172.17.63.229 ! ! ! access-list 120 permit
ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 130
deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-
list 130 permit ip 10.2.2.0 0.0.0.255 any ! route-map
nonat permit 10 match ip address 130 ! call rsvp-sync !
! mgcp profile default ! dial-peer cor custom ! ! ! ! !
line con 0 line aux 0 line vty 0 4 login ! ! end
```

Настройка с помощью ASDM

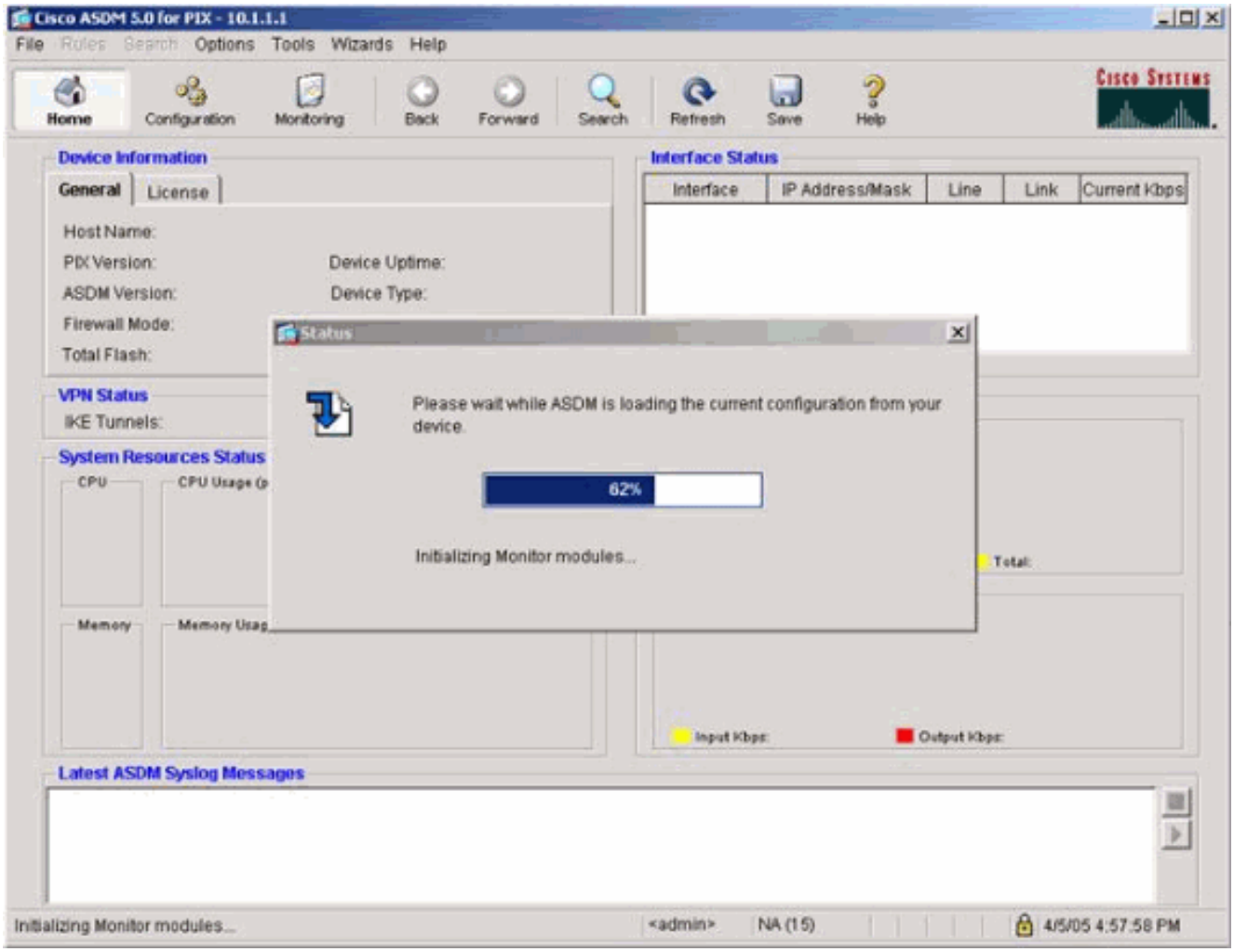
В этом примере конфигурации показан способ настройки PIX с использованием графического интерфейса пользователя ASDM. ПК с Интернет-браузером и IP-адресом 10.1.1.2 подключен к внутреннему интерфейсу PIX e1. Проверьте, чтобы в PIX был включен http.

В данной процедуре демонстрируется настройка центрального PIX при помощи ASDM.

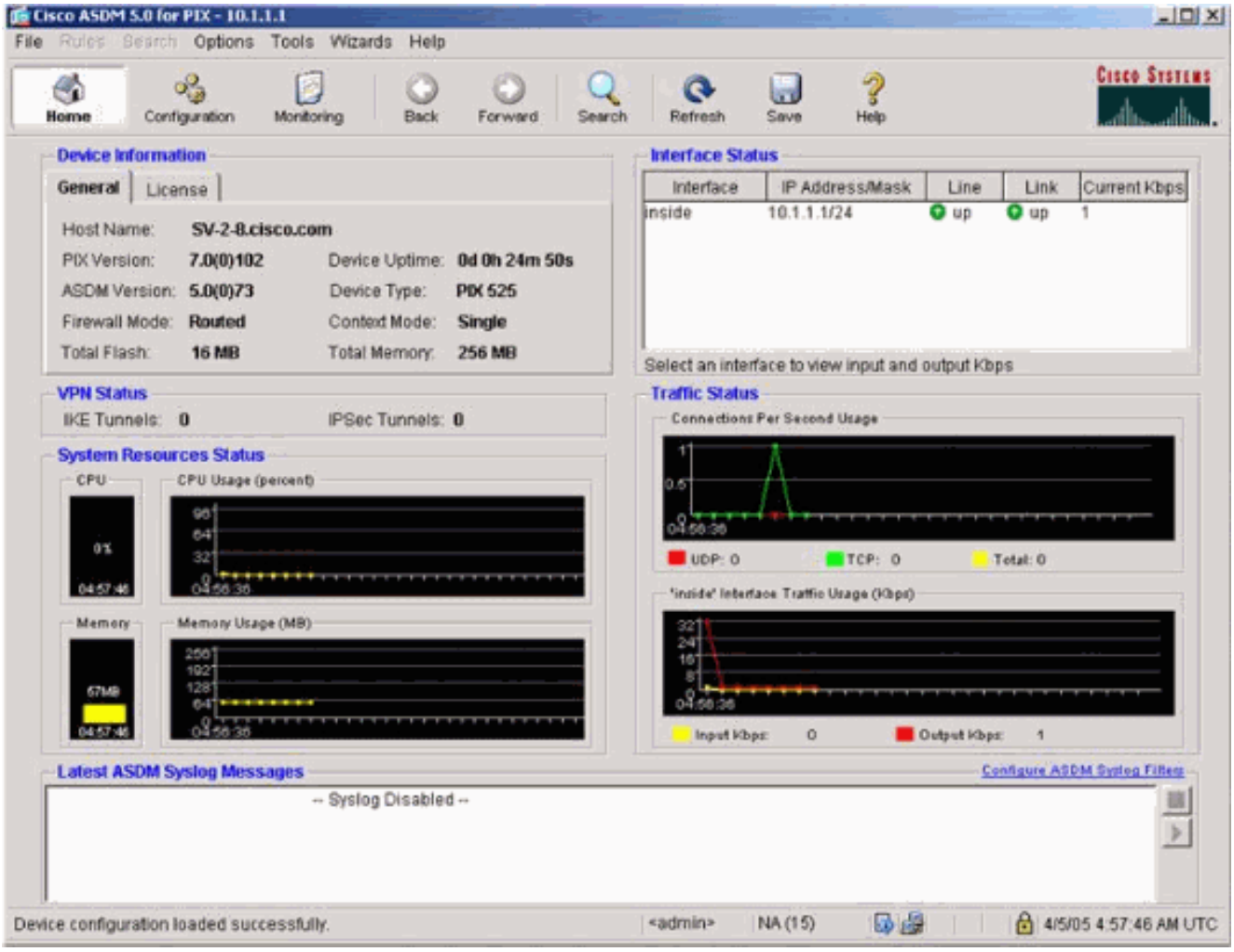
1. Подключите ПК к PIX и выберите способ загрузки.



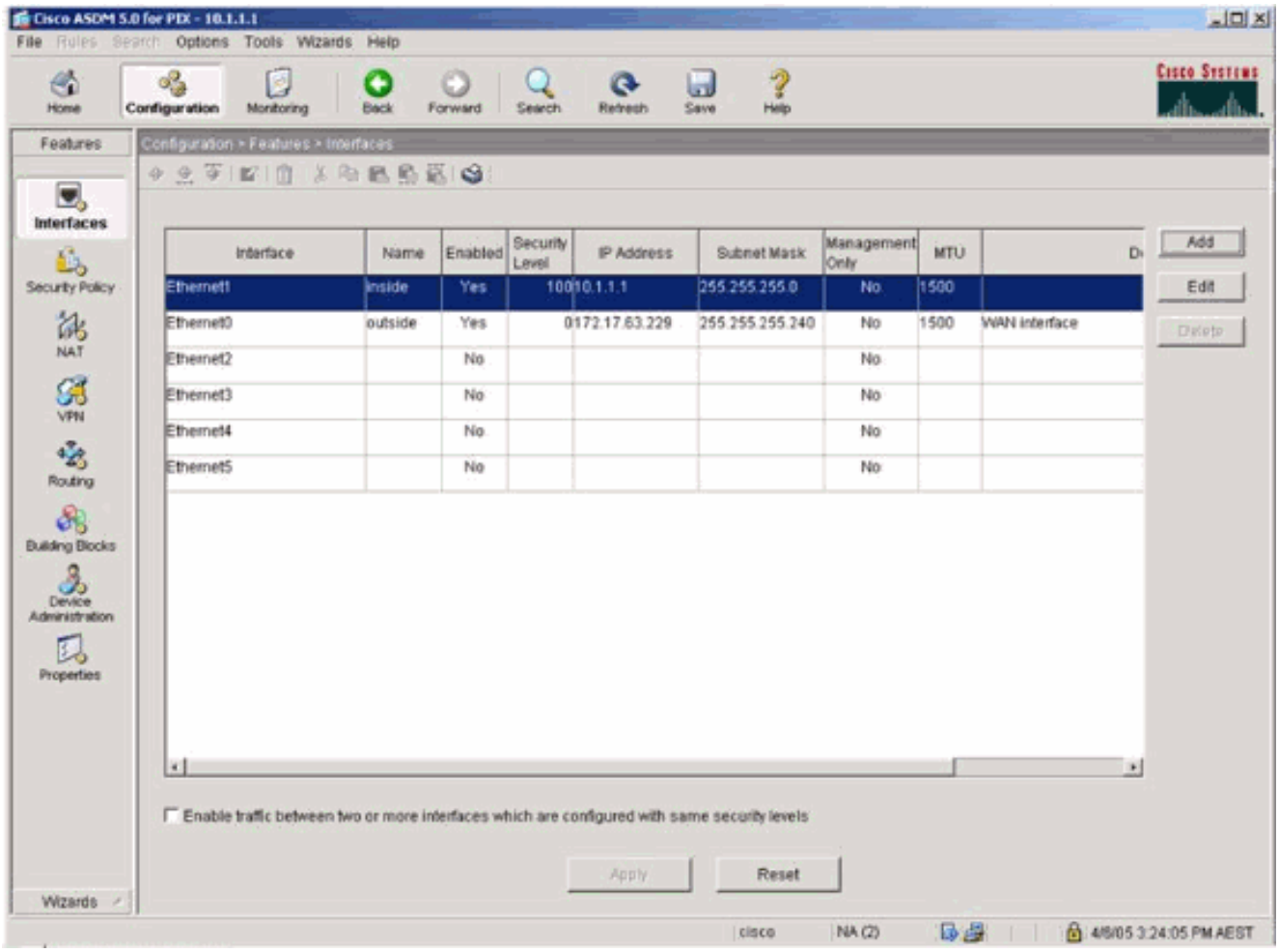
ASDM загружает с PIX существующую конфигурацию.



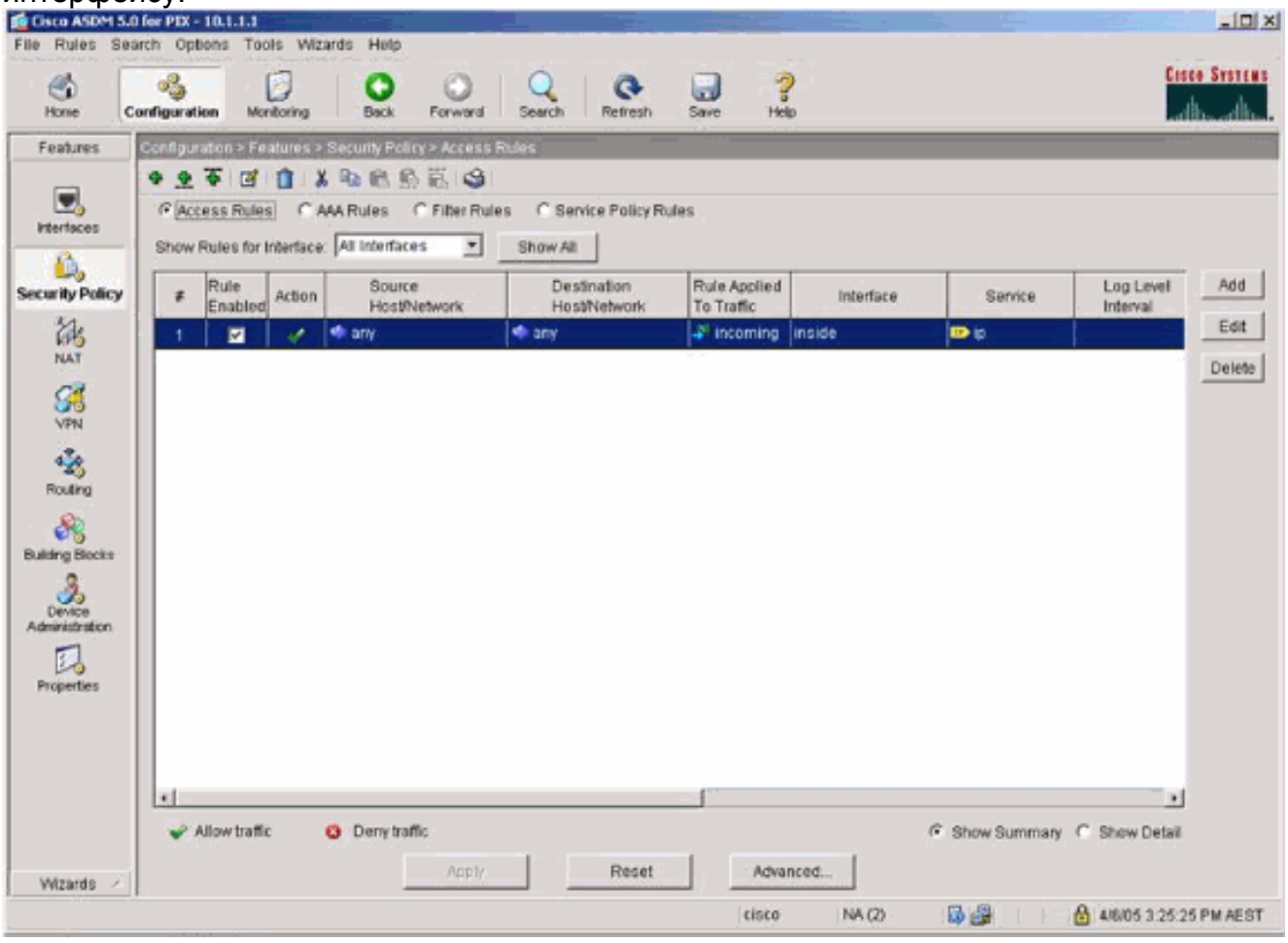
В окне приведен инструментарий для мониторинга и меню.



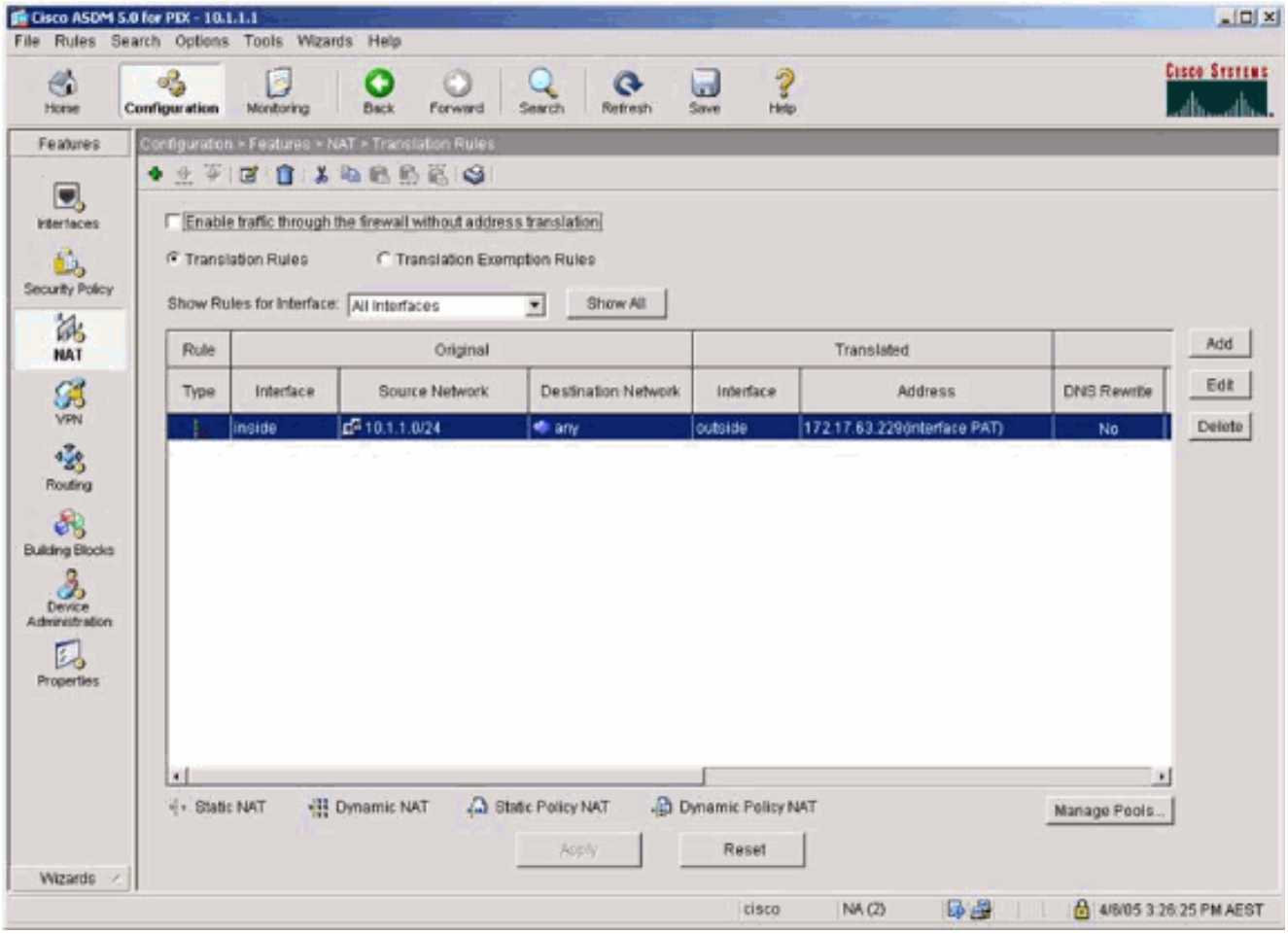
2. Выберите **Configuration> Features> Interfaces** и выберите **Add** для новых интерфейсов или **Отредактируйте** для существующей конфигурации.



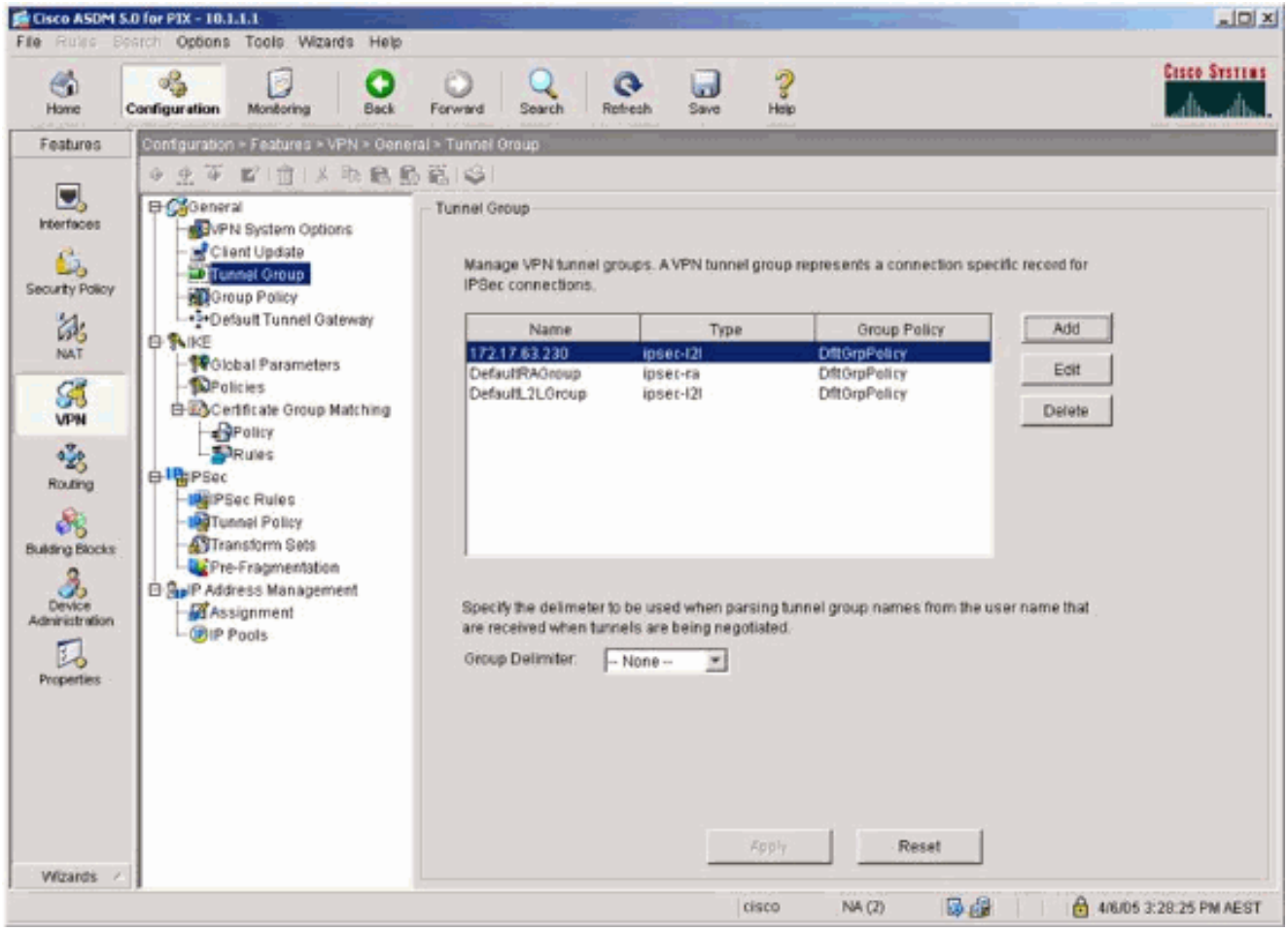
3. Примените параметры безопасности ко внутреннему интерфейсу.



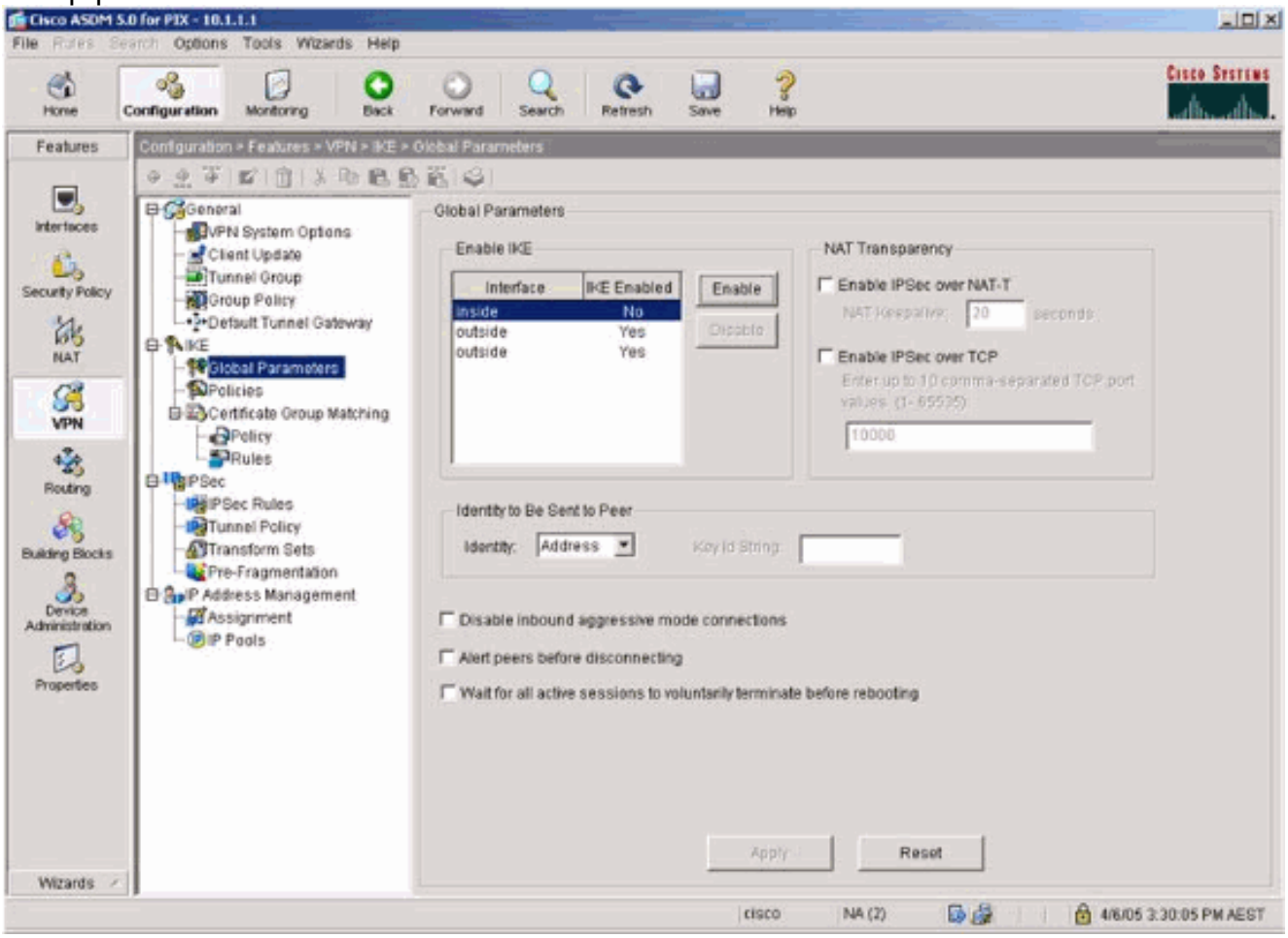
4. В окне настройки NAT зашифрованный трафик исключен для NAT, а для всего остального трафика, идущего на внешний интерфейс, используется NAT/PAT.



5. Выберите **VPN> General> Tunnel Group** и включите Туннельную группу

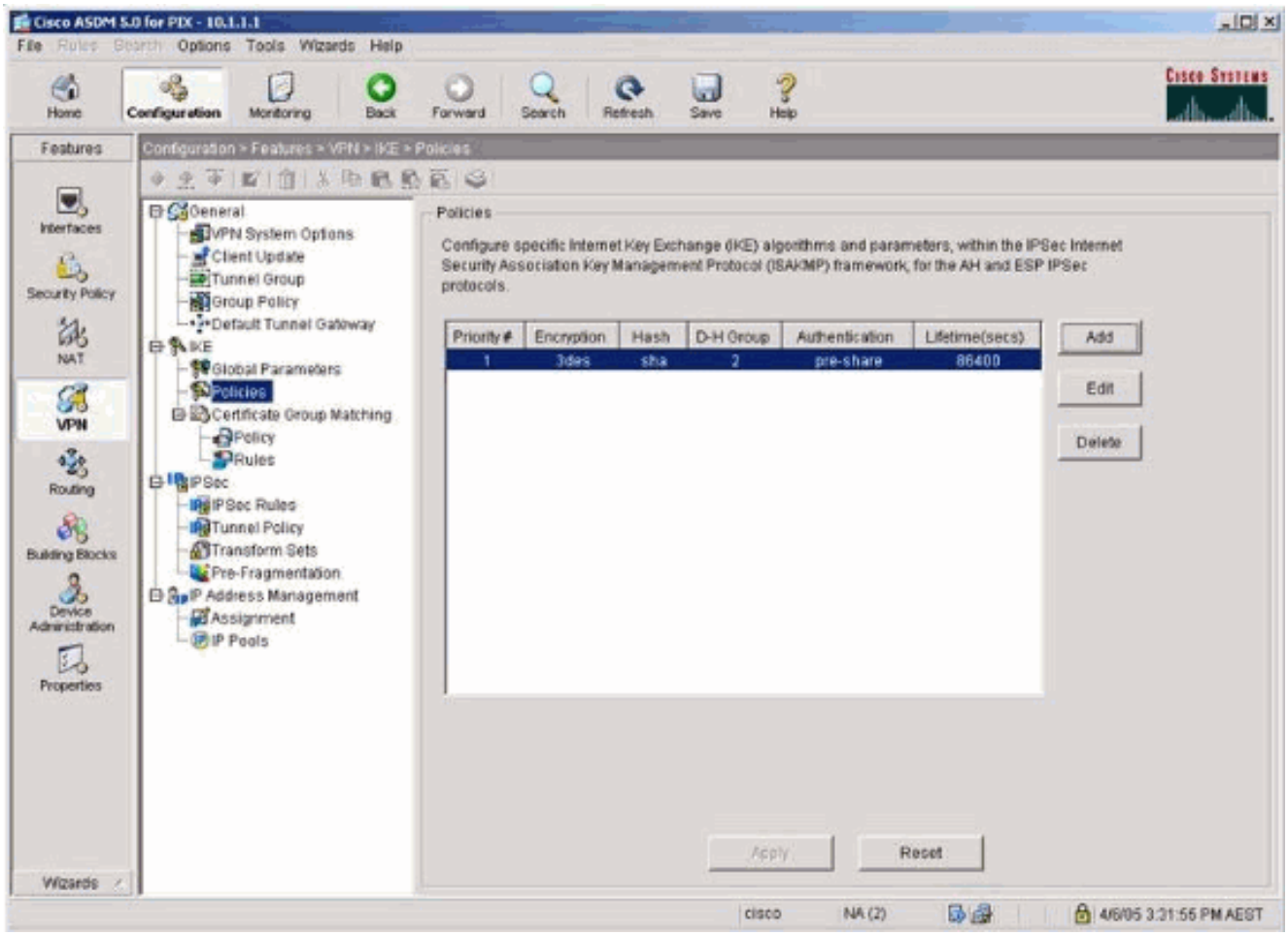


6. Выберите **VPN> IKE> Global Parameters** и включите IKE на внешнем интерфейсе.

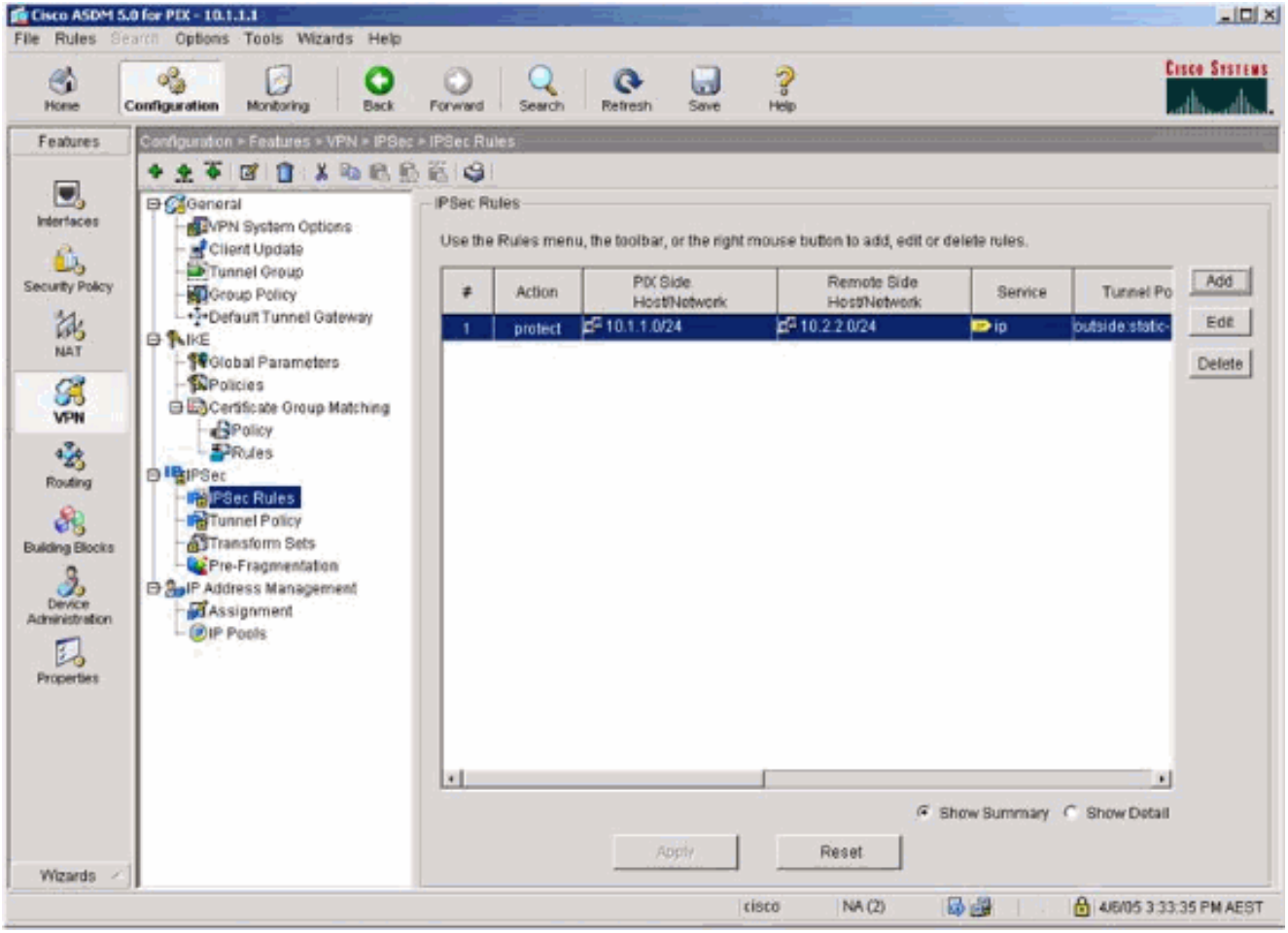


7. Выберите **VPN> IKE> Policies** и выберите Наборы правил

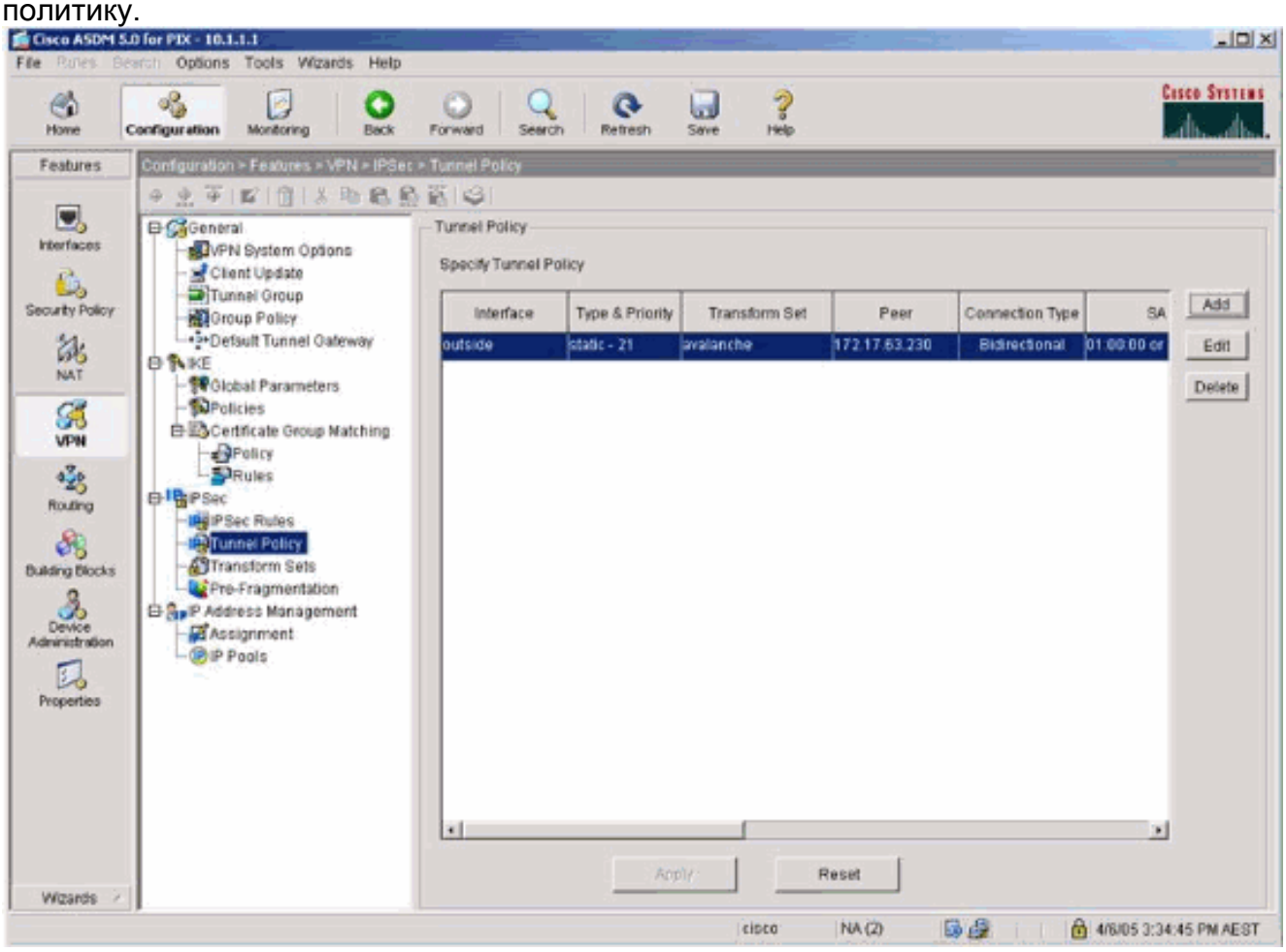
IKE.



8. Выберите **VPN> IPsec> IPsec Rules** и выберите **IPsec** для локального туннеля и удаленной
адресации.

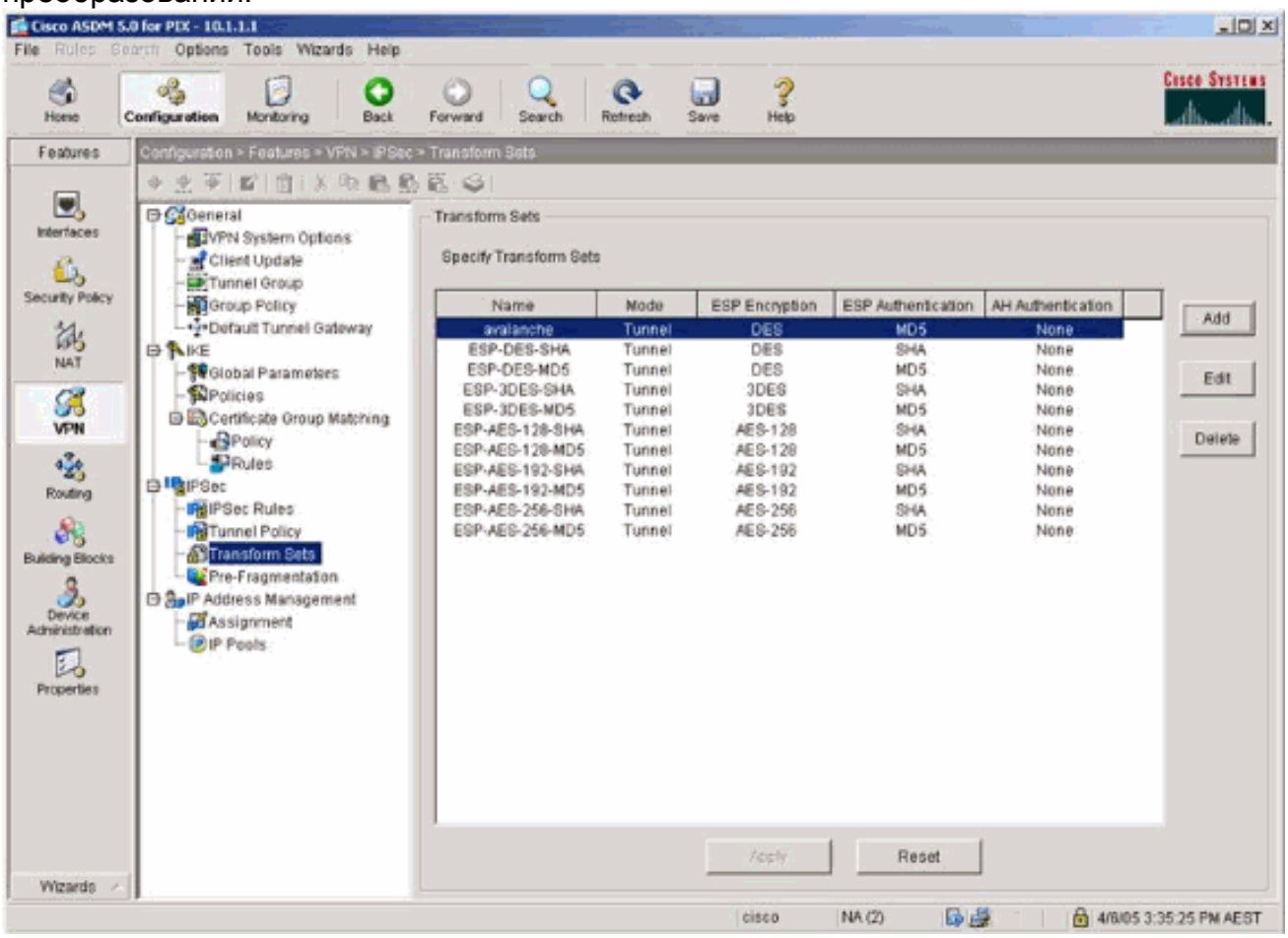


9. Выберите **VPN> IPsec> Tunnel Policy** и выберите туннельную политику.

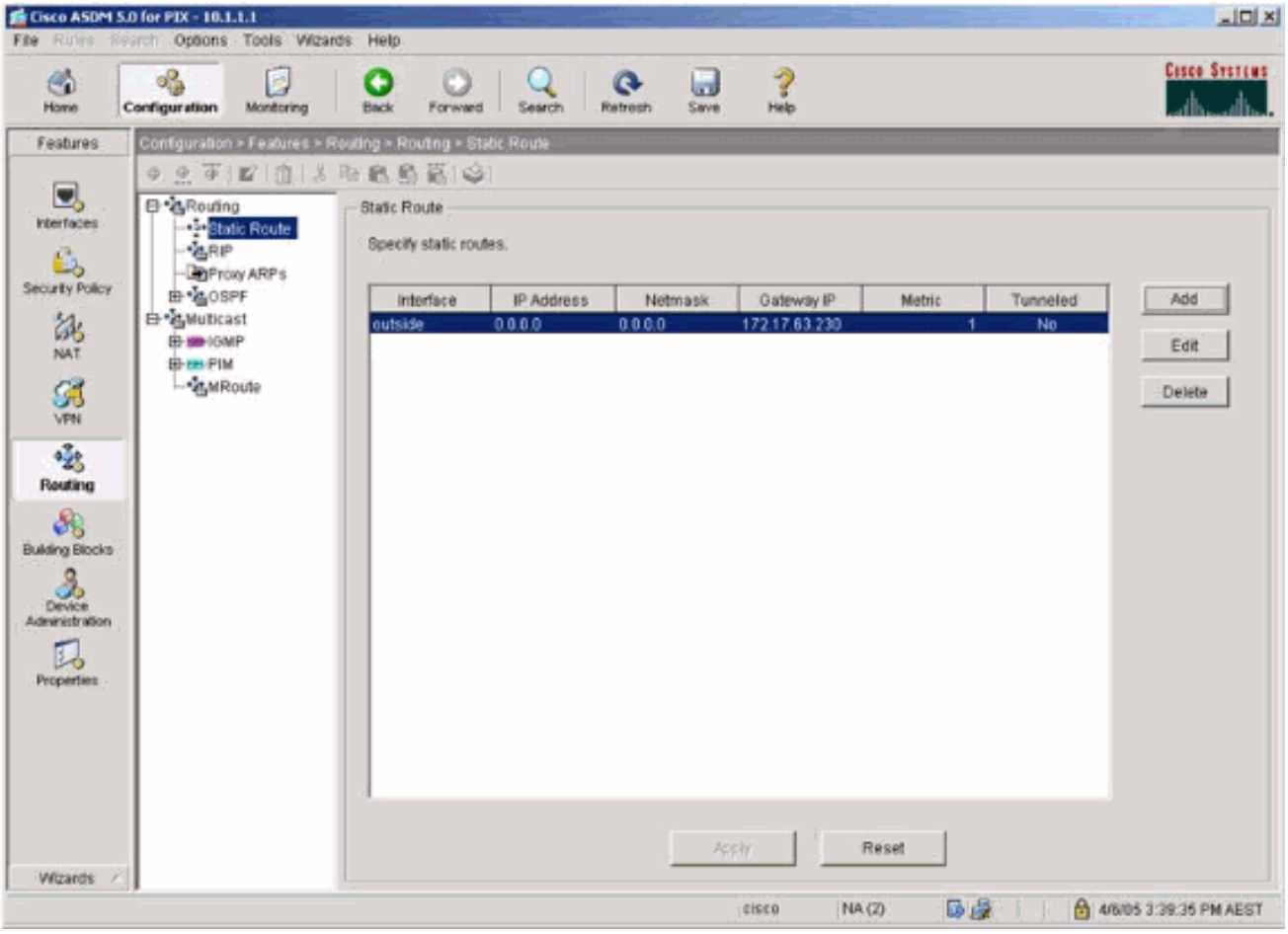


10. Выберите **VPN> IPsec> Transform Sets** и выберите Набор

преобразований.



11. Выберите **Routing> Routing> Static Route** и выберите статический маршрут к маршрутизатор/шлюзу. В данном примере для упрощения статический маршрут указывает на удаленный равноправный узел
VPN.



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.**

- **команда show crypto ipsec sa – отображает связи безопасности, соответствующие второму этапу.**
- **команда show crypto isakmp sa вЂ отображает сопоставления безопасности, соответствующие первому этапу.**

Устранение неполадок

ASDM можно использовать для включения регистрации, а также для просмотра журналов.

- Выберите **Configuration> Properties> Logging> Logging Setup**, выберите **Enable Logging** и нажмите **Apply** к enable logging.
- Выберите **Monitoring> Logging> Log Buffer> On Logging Level**, выберите **Logging Buffer** и нажмите **View** для просмотра журналов.

Команды для устранения неполадок

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

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- команда debug crypto ipsec отображает согласование IPSec на втором этапе.
- debug crypto isakmp – вывод данных о согласовании ISAKMP в фазе 1.
- "debug crypto engine" - отображается зашифрованный трафик.
- clear crypto isakmp– удаляет ассоциации безопасности, соответствующие первому этапу.
- clear crypto sa– удаляет ассоциации безопасности, соответствующие второму этапу.
- debug icmp trace— данная команда показывает, достигают ли устройства PIX запросы ICMP, отправляемые хостами. Для выполнения этой отладки добавьте команду access-list, чтобы разрешить ICMP в вашей конфигурации.
- logging buffer debugging – отображает установленные соединения и отказы в подключении к узлам, которые используют PIX. Информация хранится в буфере журнала PIX. Его можно просмотреть при помощи команды show log.

Дополнительные сведения

- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Cisco PIX Firewall Software
- 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