PIX 6.x: Пример конфигурации прохода туннеля IPsec через брандмауэр PIX Firewall с использованием Списка доступа и с NAT

Содержание

Введение

В этом документе приводится пример конфигурации для туннеля IPSec через межсетевой экран, который производит трансляцию сетевых адресов (NAT). **Эта конфигурация не будет работать с трансляцией адресов портов (PAT), если используются релизы программного обеспечения Cisco IOS®, предшествующие 12.2(13)T.** Этот вид настройки может быть использован для туннелирования IP-трафика. Его нельзя использовать для шифрования трафика, который не идет через межсетевой экран, такого как IPX или обновления маршрутизации. Для этого вида настройки подходит общая инкапсуляция маршрутов (GRE). В этом примере маршрутизаторы Cisco 2621 и 3660 являются конечными точками туннеля IPSec, соединяющими две частные сети с кондуитами или списками управления доступом (ACL) на PIX между ними для обеспечения трафика IPSec.

Примечание: NAT является трансляцией адресов один к одному, чтобы не быть перепутанным с PAT, который является многими (в межсетевом экране)-to-one трансляция. Дополнительные сведения об устранении неисправностей NAT см. в документации "Проверка работы NAT и основные способы устранения неполадок NAT" или "Работа NAT".

Примечание: IPSec с PAT может работать неправильно, поскольку внешнее оконечное устройство туннеля не может управлять несколькими туннелями с одного IP-адреса. Свяжитесь со своим поставщиком для выяснения, работают ли оконечные устройства туннеля с PAT. Кроме того, в релизах 12.2(13)T и более поздних для PAT также можно использовать функцию NAT Transparency (прозрачность). Подробнее см. Прозрачность

IPSec NAT. Подробнее о данных функциях в версиях 12.2(13)T и более поздних см. "Поддержка IPSec ESP через NAT". Прежде чем обратиться в TAC, посмотрите документ "Ответы на вопросы по NAT", где есть ответы на многие общие вопросы.

См. Туннель IPSec Проходят через Устройство безопасности С использованием Списка доступа и MPF с Примером Конфигурации NAT для получения дополнительной информации о том, как настроить Туннель IPSec через межсетевой экран с NAT на версии 7 PIX/ASA. x.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco IOS Software Release 12.0. 7. T [до, но не включая 12.2 (13) T]См. Прозрачность NAT IPSec для более свежих версий.
- Маршрутизатор Cisco 2621, который выполняет Cisco IOS Software Release 12.4
- Маршрутизатор Cisco 3660, который выполняет Cisco IOS Software Release 12.4
- Межсетевой экран Cisco PIX, который выполняется 6. x

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

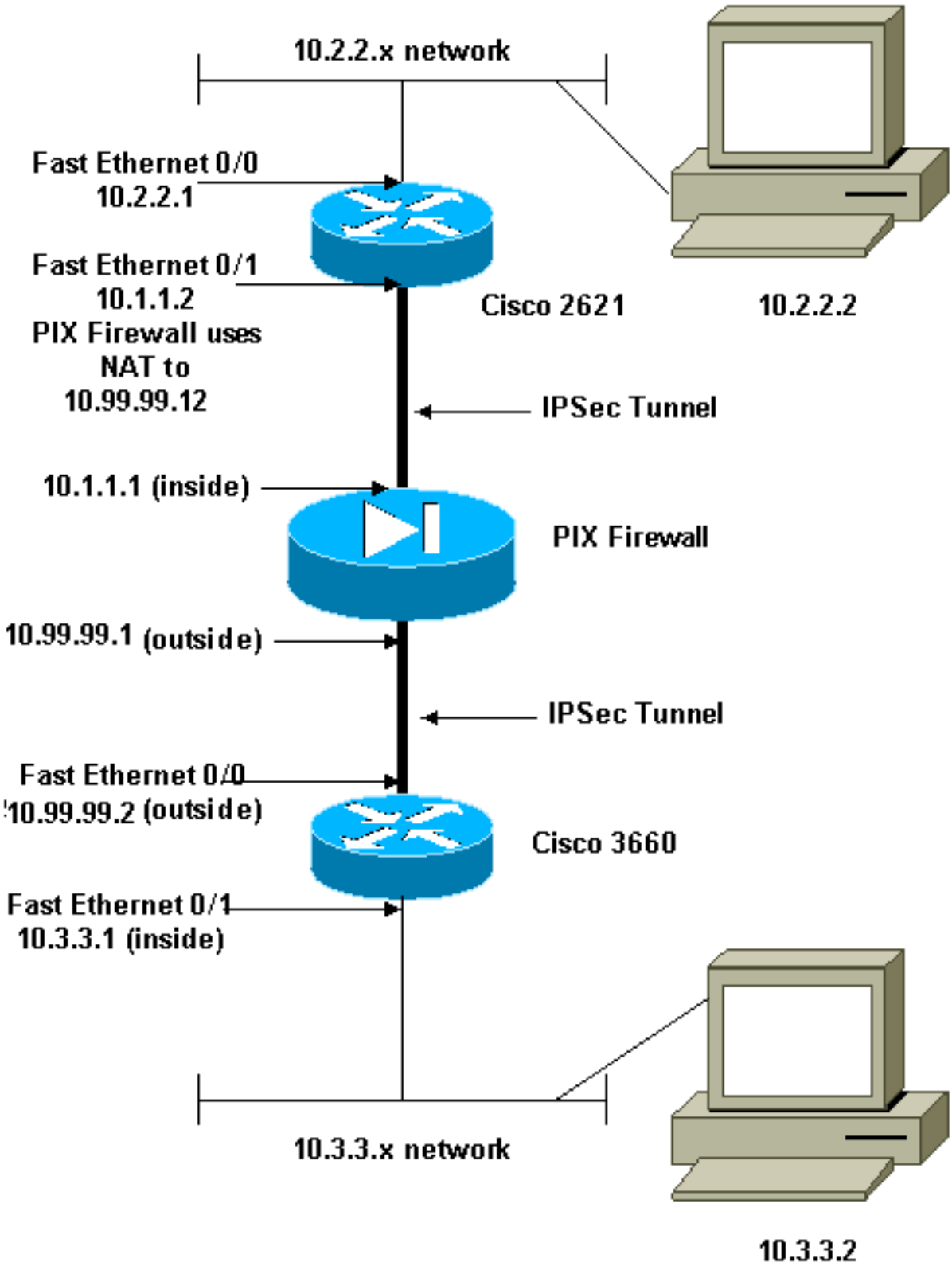
Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация Cisco 2621
- Частичная конфигурация межсетевого экрана Cisco PIX

- Конфигурация Cisco 3660

Конфигурация Cisco 2621

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.2
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/1
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
 end
```

Частичная конфигурация межсетевого экрана Cisco PIX

```
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
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. nat (inside) 1 0.0.0.0 0.0.0.0 0 0
 static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

Примечание: Команда fixup protocol esp-ike отключена по умолчанию. Если **команда fixup protocol esp-ike** выполнена, устройство включено, и Межсетевой экран PIX сохраняет исходный порт Протокола IKE. Это также создает трансляцию PAT для трафика ESP. Кроме того, если устройство ike ESP работает, Протокол ISAKMP не может быть включен ни на каком интерфейсе.

Конфигурация Cisco 3660

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !
```

```
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.12
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/0
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.12
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 interface FastEthernet0/0
  ip address 10.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
 !
 interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
 !
 interface Ethernet3/1
  no ip address
  no ip directed-broadcast
 interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
 !
 !--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
 !--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.99.99.1
 no ip http server
 !
```

```
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 end
```

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.**
- **show crypto engine connection active** — Использование для наблюдения зашифрованных и расшифрованных пакетов.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Команды для устранения неполадок

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

- **"debug crypto engine" - отображается зашифрованный трафик.**
- **debug crypto ipsec — используйте для просмотра сеансов согласования протокола IPSec в фазе 2.**
- **debug crypto isakmp — используйте для вывода данных о согласовании ISAKMP в фазе 1.**

Очистка сопоставлений безопасности

- **clear crypto isakmp** сопоставления безопасности IKE.

- clear crypto ipsec sa – удаление сопоставлений безопасности IPSec.

Дополнительные сведения

- Cisco PIX 500 Series Security Appliances
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Страница поддержки NAT
- Запрос на комментарии (RFC)
- Cisco Systems – техническая поддержка и документация