PIX 6.x: Пример конфигурации динамических подключений IPsec между маршрутизатором PIX со статической адресацией и маршрутизатором IOS с NAT и динамической адресацией

Содержание

Введение

Этот документ предоставляет пример конфигурации, который позволяет PIX принимать динамичные IPsec соединения. При доступе из частной сети 10.1.1.x в Интернет удаленный маршрутизатор выполняет преобразование сетевых адресов (NAT). Трафик от 10.1.1.x до частной сети 192.168.1.x позади PIX исключен из процесса NAT. Маршрутизатор может инициировать соединения с PIX, но PIX не может инициировать соединения с маршрутизатором.

Эта конфигурация использует межсетевой экран PIX для создания динамического LAN-LAN IPsec (L2L) туннели с маршрутизатором Cisco IOS®, который получает динамические IP - адреса на их открытом интерфейсе (внешний интерфейс). Протокол DHCP (динамического конфигурирования узла) предоставляет механизм для выделения IP-адресов динамично от поставщика услуг (интернет-провайдер). При этом IP-адреса, переставшие быть востребованными для хостов, можно использовать повторно.

См. Соединение IPSec от динамического к статическому МАРШРУТИЗАТОРА К PIX с Примером Конфигурации NAT для получения дополнительной информации о сценарии, откуда маршрутизатор принимает динамические подключения IPsec Устройства безопасности PIX, которое выполняется 6. x.

Процедура, позволяющая разрешить устройству защиты PIX/ASA принимать динамические IPsec-подключения от маршрутизатора под управлением операционной системы Cisco IOS описана в документе Пример настройки протокола IPsec между статическим маршрутизатором под управлением ОС IOS и динамическим устройством PIX/ASA 7.x с трансляцией сетевых адресов.

Подробнее о том же сценарии, но с применением ПО версий 7.x и выше на устройстве защиты PIX/ASA, см. в документе Пример настройки IPsec с NAT между статическим устройством PIX/ASA 7.x и динамическим маршрутизатором IOS.

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 12.4
- Выпуск 6.3.1 программного обеспечения Cisco PIX Firewall
- Межсетевой экран Cisco Secure PIX 515E
- Маршрутизатор Cisco 7206

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.

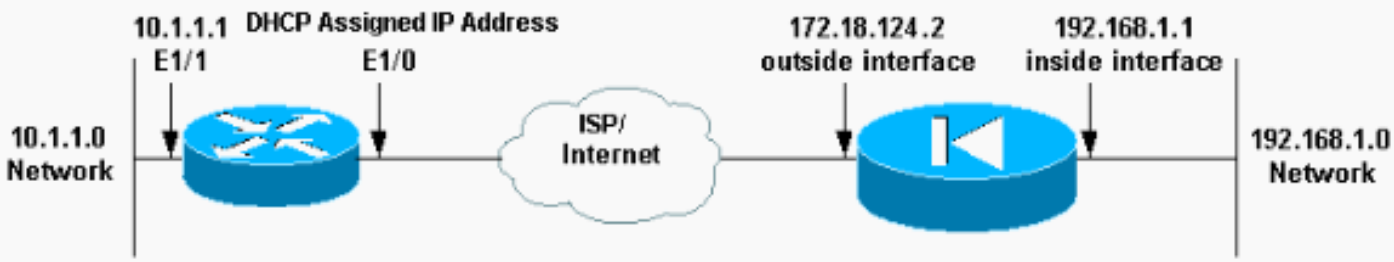
Настройка

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.



Конфигурации

Эти конфигурации используются в данном документе.

- Elf (PIX)
- Швабра (маршрутизатор Cisco 7204)

Elf (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access control list (ACL) to avoid NAT on the IPsec
packets. access-list nonat permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm history enable
```

```
arp timeout 14400
global (outside) 1 interface
!-- Binds ACL nonat to the NAT statement to avoid NAT on
the IPsec packets nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Permits Internet Control Message Protocol (ICMP)
traffic for testing. !--- Do not enable it in a live
network. conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 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 LOCAL protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPsec configuration crypto ipsec transform-set
router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *******. isakmp
key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
: end
[OK]
elf#
```

Швабра (маршрутизатор Cisco 7204)

```
mop#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
```

```
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) policies crypto isakmp
policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!
!--- IPsec policies crypto ipsec transform-set pix-set
esp-des esp-md5-hmac
!
crypto map pix 10 ipsec-isakmp
 set peer 172.18.124.2
 set transform-set pix-set
 match address 101
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!
!--- Except the private network from the NAT process. ip
nat inside source route-map nonat interface Ethernet1/0
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
```

```
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.**

Можно выполнить эти **команды показа** на PIX и на маршрутизаторе.

- **show crypto isakmp sa — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.**
- **show crypto ipsec sa– показывает настройки, используемые текущими ассоциациями безопасности IPSec.**
- **show crypto engine connections active— показывает текущие подключения и информацию о шифровании и расшифровке пакетов (только для маршрутизатора).**

Необходимо сбросить SA для обоих равноправных узлов.

- Команды PIX выполнены в режиме конфигурации.**clear crypto isakmp sa — удаляет SA фазы 1.clear crypto ipsec sa – удаляет SA фазы 2.**
- Команды маршрутизатора выполнены в режиме включения.**clear crypto isakmp** SA Фазы 1.**clear crypto sa** SA Фазы 2.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

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".

- **show crypto isakmp sa — отображает все текущие ассоциации безопасности (SA) IKE узла.**
- **show crypto ipsec sa– показывает настройки, используемые текущими ассоциациями безопасности IPSec.**
- **show crypto engine connections active— показывает текущие подключения и информацию о шифровании и расшифровке пакетов (только для маршрутизатора).**

Дополнительные сведения

- Страница технической поддержки протоколов согласования IPSec и IKE
- Устройства защиты PIX серии 500
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация