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

Содержание

Введение

Этот документ предоставляет пример конфигурации, который показывает вам, как позволить маршрутизатору IOS® принять динамические подключения IPsec от Межсетевого экрана PIX. Если частная сеть 10.0.0.x обращается к Интернету, удаленный маршрутизатор выполняет Технологию NAT. Трафик от 10.0.0.x до частной сети 10.1.0.x позади PIX исключен из процесса NAT. Межсетевой экран PIX может инициировать соединения с маршрутизатором, но маршрутизатор не может инициировать соединения с PIX.

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

См. документ PIX 6.x: Динамический IPsec Между Статически Обращенным Межсетевым экраном PIX и Динамично Обращенным Маршрутизатором IOS с Примером Конфигурации NAT для получения дополнительной информации о сценарии, где PIX принимает динамические подключения IPsec от маршрутизатора.

См. PIX/ASA 7.x и позже: Динамический IPsec Между Статически Обращенным PIX и Динамично Обращенным Маршрутизатором IOS с Примером Конфигурации NAT, чтобы позволить Устройству безопасности PIX/ASA принять динамические подключения IPsec от маршрутизатора IOS.

См. PIX/ASA 7.x и позже: Динамический IPsec Между Статически Обращенным Маршрутизатором IOS и Динамично Обращенным PIX с Примером Конфигурации NAT для узнавания больше о том же сценарии, где Устройство безопасности PIX/ASA работает под управлением ПО версии 7.x и позже.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск 12.4 программного обеспечения Cisco IOS
- Выпуск 6.3.4 программного обеспечения Cisco PIX Firewall
- Межсетевой экран Cisco Secure PIX 515E
- Маршрутизатор Cisco 2811

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:

- PIX-515 E
- R2 (маршрутизатор Cisco 2811)

PIX-515 E

```
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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

!--- The access control list (ACL) to avoid NAT on the
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
!--- The ACL to apply on crypto map. !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
!--- ISP will providthe the Outside IP address.
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 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 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
sysopt connection permit-ipsec

!--- IPsec configuration, Phase 2. crypto ipsec
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
*******.

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
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
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2 (маршрутизатор Cisco 2811)

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
```

```
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!--- ISAKMP policy, Phase 1. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
!--- IPsec policy, Phase 2. crypto ipsec transform-set
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
!--- Except the private network from the NAT process. ip
nat inside source list 102 interface FastEthernet0/0
overload
!
!--- Include the private-network-to-private-network !---
```

```
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

!--- Except the private network from the NAT process.
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
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.

- 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.

Выполните эти команды PIX в режиме конфигурации.

- clear crypto isakmp sa — удаляет SA фазы 1.
- clear crypto ipsec sa – удаляет SA фазы 2.

Выполните эти команды маршрутизатора в режиме включения.

- clear crypto isakmp SA Фазы 1.
- clear crypto sa SA Фазы 2.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей 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** все текущие SA IKE в узле.
- **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

- 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)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация