PIX/ASA 7.X : Добавление/удаление сети на существующем примере конфигурации VPN-туннеля L2L

Содержание

Введение

Этот документ предоставляет пример конфигурации для того, как добавить новую сеть к существующему VPN-туннелю.

Предварительные условия

Требования

Гарантируйте, что у вас есть Устройство безопасности PIX/ASA, которое выполняется 7.x код перед попыткой этой конфигурации.

Используемые компоненты

Сведения в этом документе основываются на двух устройствах Устройства безопасности Cisco 5500.

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.

Родственные продукты

Эта конфигурация может также использоваться с Устройством безопасности PIX 500.

Условные обозначения

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

Общие сведения

В настоящее время существует LAN-LAN (L2L) VPN-туннель, который является между NY и офисом TN. Офис NY просто добавил новую сеть, которая будет использоваться группой разработки CSI. Эта группа требует доступа к ресурсам, которые находятся в офисе TN. Задача под рукой состоит в том, чтобы добавить новую сеть к уже существующему VPN-туннелю.

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:

Добавление сети в туннель IPSec

В данном документе используется следующая конфигурация:

NY (HQ) Config межсетевого экрана

```
ASA-NY-HQ#show running-config : Saved : ASA Version
7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com enable
password WwXYvtKrnjXqGbu1 encrypted names ! interface
Ethernet0/0 nameif outside security-level 0 ip address
192.168.11.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 nameif Cisco
security-level 70 ip address 172.16.40.2 255.255.255.0 !
interface Ethernet0/3 shutdown no nameif no security-
level no ip address ! interface Management0/0 shutdown
no nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name corp2.com access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0 !--- You must be
```

```
sure that you configure the !--- opposite of these
access control lists !--- on the other end of the VPN
tunnel. access-list inside_nat0_outbound extended permit
ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0 !---
You must be sure that you configure the !--- opposite of
these access control lists !--- on the other end of the
VPN tunnel. access-list outside_20_cryptomap extended
permit ip 172.16.40.0 255.255.255.0 10.10.10.0
255.255.255.0 !--- Output is suppressed. nat-control
global (outside) 1 interface nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 172.16.1.0
255.255.255.0 !--- The new network is also required to
have access to the Internet. !--- So enter an entry into
the NAT statement for this new network. nat (inside) 1
172.16.40.0 255.255.255.0 route outside 0.0.0.0 0.0.0.0
192.168.11.100 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart crypto ipsec
transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10 crypto
map outside_map 20 set transform-set ESP-3DES-SHA crypto
map outside_map interface outside crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp nat-traversal 20 tunnel-group 192.168.10.10 type
ipsec-l2l tunnel-group 192.168.10.10 ipsec-attributes
pre-shared-key * !--- Output is suppressed. : end ASA-
NY-HQ#
```

Удаление сети из туннеля IPSec

Используйте это шагает для удаления сети из конфигурации Туннеля IPSec. Здесь, полагайте, что сеть 172.16.40.0/24 была удалена из NY (HQ) Конфигурация устройства Secuirty.

1. Прежде удаляют сеть из туннеля, разъединяют IP - безопасное соединение, которое также очищает сопоставления безопасности, отнесенные к фазе 2.
   ASA-NY-HQ# clear crypto ipsec sa Очищает сопоставления безопасности, отнесенные к фазе 1 следующим образом
   ASA-NY-HQ# clear crypto isakmp sa
2. Удалите ACL представляющего интерес трафика для Туннеля IPSec.
   ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
3. Удалите ACL (inside_nat0_outbound), так как трафик исключен из nat.
   ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
4. Очистите преобразование NAT как показано
   ASA-NY-HQ# clear xlate
5. Когда когда-либо вы модифицируете конфигурацию туннеля, удаляете и повторно применяете это крипто-команды для взятия последней конфигурации во внешнем

интерфейсе
```
ASA-NY-HQ(config)# crypto map outside_map interface outside ASA-NY-HQ(config)# crypto
isakmp enable outside
```
6. Сохраните активную конфигурацию к флэш-памяти **"write memory"**.
7. Выполните ту же процедуру для другого конца - Устройство безопасности TN для удаления конфигураций.
8. Initate Туннель IPSec и проверяют соединение.

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.**

- **пропингуйте в 172.16.40.20**
- **show crypto isakmp sa**
- **show crypto ipsec sa**

Устранение неполадок

См. эти документы для большего количества сведений об устранении проблем:

- Решения для устранения проблем IPSec VPN
- Понимание и Использование команд отладки
- Поиск и устранение неполадок соединений через PIX и ASA

Дополнительные сведения

- **Введение в шифрование IPSec**
- **Страница поддержки IPsec Negotiation/IKE**
- **Справочник по командам устройства безопасности**
- **Configuring IP Access Lists**
- **Cisco Systems – техническая поддержка и документация**