PIX/ASA 7.X : Добавление нового туннеля или предоставление удаленного доступа к существующему VPN-туннелю LAN-LAN.

Содержание

Введение

Данный документ пошагово описывает добавление нового VPN-туннеля или предоставление удаленного доступа VPN к существующей конфигурации VPN-туннеля LAN-LAN. Дополнительные сведения о создании первоначальных IPSec-туннелей в VPN, а также примеры конфигурации, см. в разделе Устройство адаптивной защиты серии Cisco ASA 5500 - Примеры конфигураций и технические примечания.

Предварительные условия

Требования

Перед применением данной конфигурации убедитесь, что текущий рабочий VPN-туннель IPSEC LAN-LAN настроен правильно.

Используемые компоненты

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

- Два устройства защиты ASA под управлением ПО 7.x
- Одно устройство защиты PIX под управлением ПО 7.x

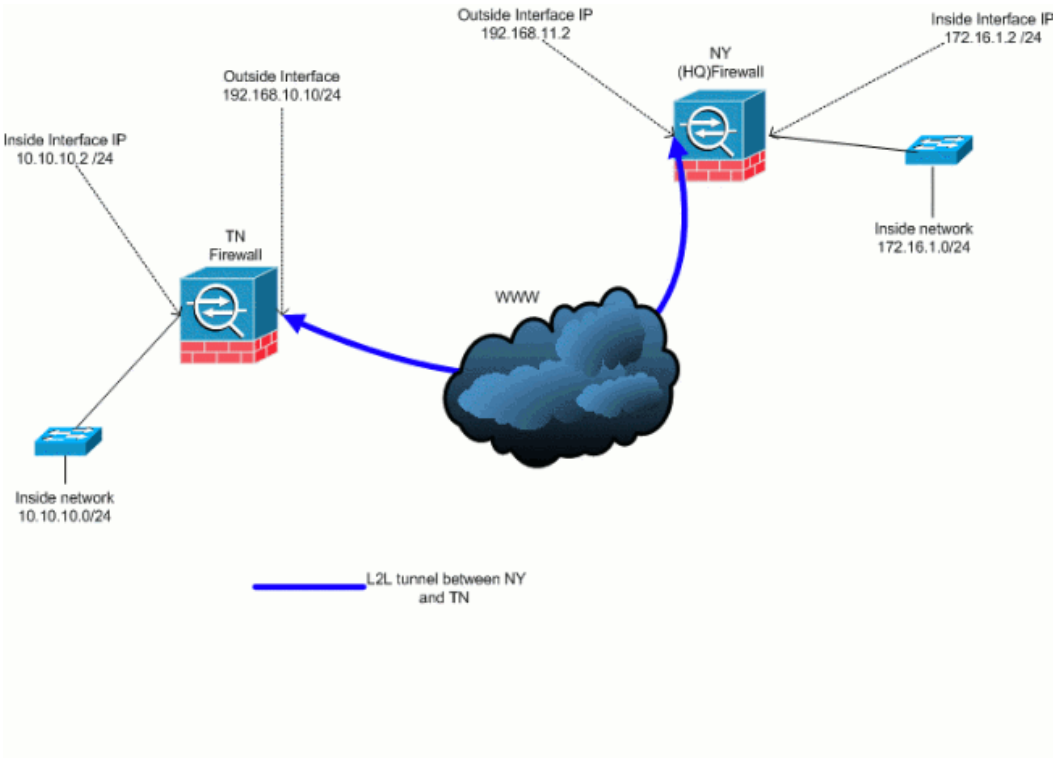
Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, были запущены с чистой (заданной по умолчанию) конфигурацией. Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Условные обозначения

Более подробные сведения о применяемых в документе обозначениях см. Условные обозначения, используемые в технической документации Cisco.

Сетевой график

В данном документе используется следующая настройка сети:



Нижеследующие выходные данные являются текущей рабочей конфигурацией устройства защиты, которое находится в Нью-Йорке (концентратор). В данной конфигурации, IPSec-туннель LAN-LAN настроен между Нью-Йорком (головной офис) и Теннеси.

Текущие конфигурации межсетевого экрана Нью-Йорка (головной офис)

```
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
shutdown
no nameif
no security-level
no ip address
!
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
access-list outside_20_cryptomap extended permit ip 172.16.1.0 255.255.255.0
10.10.10.0 255.255.255.0

!--- Выходные данные команды подавляются.


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
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 *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 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
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3
: end
```

```
ASA-NY-HQ#
```

Общие сведения

В данный момент, существующий туннель LAN-LAN настроен между офисами Нью-Йорка (головной офис) и Теннеси. Компания недавно открыла новый офис, который располагается в Техасе. Новому офису необходимо подключиться к местным ресурсам, которые расположены в офисах Нью-Йорка и Теннеси. Кроме того, существует дополнительная потребность – предоставить сотрудникам возможность работать из дома, а также безопасный доступ к ресурсам, которые находятся в удаленной внутренней сети. В данном примере, новый VPN-туннель настроен так же, как и VPN-сервер удаленного доступа, находящийся в офисе в Нью-Йорке.

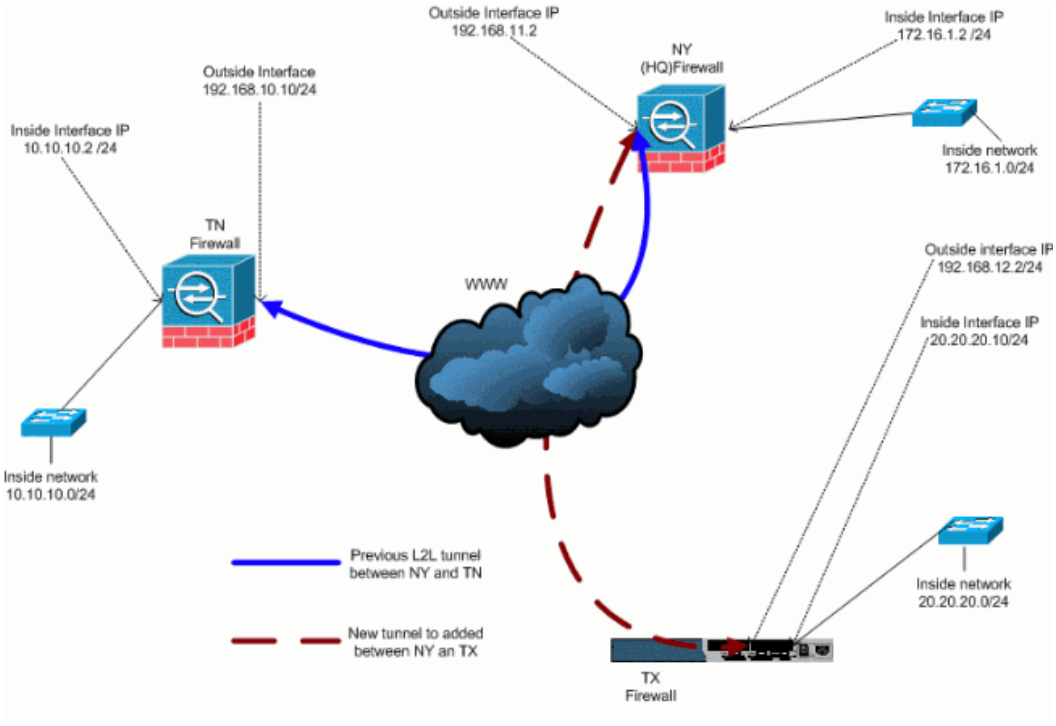
Чтобы разрешить связь между сетями VPN и определить трафик, который должен быть зашифрован или направлен через туннель, в данном примере используются две команды. Что позволяет получать доступ к Интернет, не отправляя трафик через VPN-туннель. Чтобы настроить эти два действия, задайте команды **split-tunnel** и **same-security-traffic**.

Раздельное туннелирование позволяет IPsec-клиентам, использующим удаленный доступ, условно направлять по туннелю IPsec в зашифрованном виде или напрямую пересылать пакеты интерфейсу сети в формате открытого текста. Благодаря раздельному туннелированию, пакеты, не сдерживаемые назначениями на другую сторону IPSec-туннеля, не обязательно должны быть вначале зашифрованными, отправлены через туннель, расшифрованы, а затем направлены в точку назначения. Данная команда применяет политику раздельного туннелирования к определенной сети. По умолчанию весь трафик направлен через туннель. Задайте команду **split-tunnel-policy** в режиме настройки групповой политики, чтобы установить политику раздельного туннелирования. Задайте данную команду со словом **no**, чтобы убрать split-tunneling-policy из настройки.

Устройство защиты включает в себя функцию, которая позволяет VPN-клиенту посылать трафик, защищенного IPSec другим пользователям VPN, путем разрешения передачи и приема трафика одного интерфейса. Данную функцию можно считать оконечным устройством VPN (клиент), который подключается через концентратор VPN (устройство защиты). Это называется возвратом. В другом приложении, данная функция может переадресовать входящий VPN-трафик обратно через тот же интерфейс, что и незашифрованный трафик. Применяется, например, к VPN клиентам, которые не имеют раздельного туннелирования, но имеют доступ к VPN и Интернет. Задайте команду **same-security-traffic** ***intra-interface*** в режиме глобального конфигурирования, чтобы настроить данную функцию.

Добавление дополнительного туннеля LAN-LAN к конфигурации

Схема сети для данной конфигурации:



Пошаговые инструкции

Данный раздел описывает процедуры, которые необходимо выполнить на концентраторе (межсетевой экран Нью-Йорка) устройства защиты. Дополнительную информацию о настройке клиентов оконечных устройств (межсетевой экран Техаса), см. PIX/ASA 7.x: пример простой настройки VPN-туннеля PIX-PIX.

Выполните следующие шаги:

1. Создайте два списка доступа, которые будут использоваться криптокартой, чтобы определить содержательный трафик:

   -
   ```
   ASA-NY-HQ(config)#access-list outside_30_cryptomap
      extended permit ip 172.16.1.0 255.255.255.0
      20.20.20.0 255.255.255.0
   ```

   -
   ```
   ASA-NY-HQ(config)#access-list outside_30_cryptomap
      extended permit ip 10.10.10.0 255.255.255.0
      20.20.20.0 255.255.255.0
   ```

    **Предупреждение:** Чтобы осуществить связь, другая сторона туннеля должна иметь противоположные записи списка контроля доступа (ACL) для определенной сети.

2. Введите эти данные для оператора no nat, чтобы исключить преобразование сетевых адресов между сетями:

   -
   ```
   ASA-NY-HQ(config)#access-list inside_nat0_outbound
      extended permit ip 172.16.1.0 255.255.255.0
      20.20.20.0 255.255.255.0
   ```

   -
   ```
   ASA-NY-HQ(config)#access-list inside_nat0_outbound
      extended permit ip 10.10.10.0 255.255.255.0
      20.20.20.0 255.255.255.0
   ```

   -
   ```
   ASA-NY-HQ(config)#access-list inside_nat0_outbound
      extended permit ip 20.20.20.0 255.255.255.0
      10.10.10.0 255.255.255.0
   ```

    **Предупреждение:** Чтобы осуществить связь, другая сторона туннеля должна иметь противоположные записи списка контроля доступа (ACL) для определенной сети.

3. Задайте данную команду, чтобы включить узел VPN-сети Техаса на получение доступа к VPN-туннелю Теннесси:

   -
   ```
   ASA-NY-HQ(config)#same-security-traffic permit
      intra-interface
   ```

   Это позволяет одноранговым узлам VPN иметь связь друг с другом.

4. Создайте настройку криптокарт для новых VPN-туннелей. Используйте набор преобразований, который использовался в первой настройки VPN, так как все настройки второй фазы похожи на первые.

   -
   ```
   ASA-NY-HQ(config)#crypto map outside_map 30 match
   ```

```
address outside_30_cryptomap
```

- ```
  ASA-NY-HQ(config)#crypto map outside_map 30 set
     peer 192.168.12.2
  ```

- ```
  ASA-NY-HQ(config)#crypto map outside_map 30 set
     transform-set
     ESP-3DES-SHA
  ```

5. Создайте туннельную группу для определенного туннеля с атрибутами необходимыми для подключения к удаленному узлу.

   - ```
     ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
        ipsec-l2l
     ```

   - ```
     ASA-NY-HQ(config)#tunnel-group 192.168.12.2
        ipsec-attributes
     ```

     - ```
       ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
          cisco123
       ```

     Примечание. Предварительно согласованный ключ должен соответствовать обеим сторонам туннеля.

6. Теперь, когда новый туннель был настроен, для включения его необходимо послать через туннель содержательный трафик. Чтобы осуществить это, задайте команду **source ping** для отправки эхо-запроса на хост внутренней сети удаленного туннеля.

   В данном примере, проверяется рабочая станция на другой стороне туннеля обладающая адресом 20.20.20.16. Это включает туннель между Нью Йорком и Техасом. Теперь существует два туннеля соединенных с головным офисом. Если нет доступа к системе в обход туннеля, см. Наиболее распространенные решения проблем с IPSec VPN, чтобы найти альтернативное решение, что касается использования команды `management-access`.

Пример конфигурации

Первый пример конфигурации

```
ASA-NY-HQ#show running-config

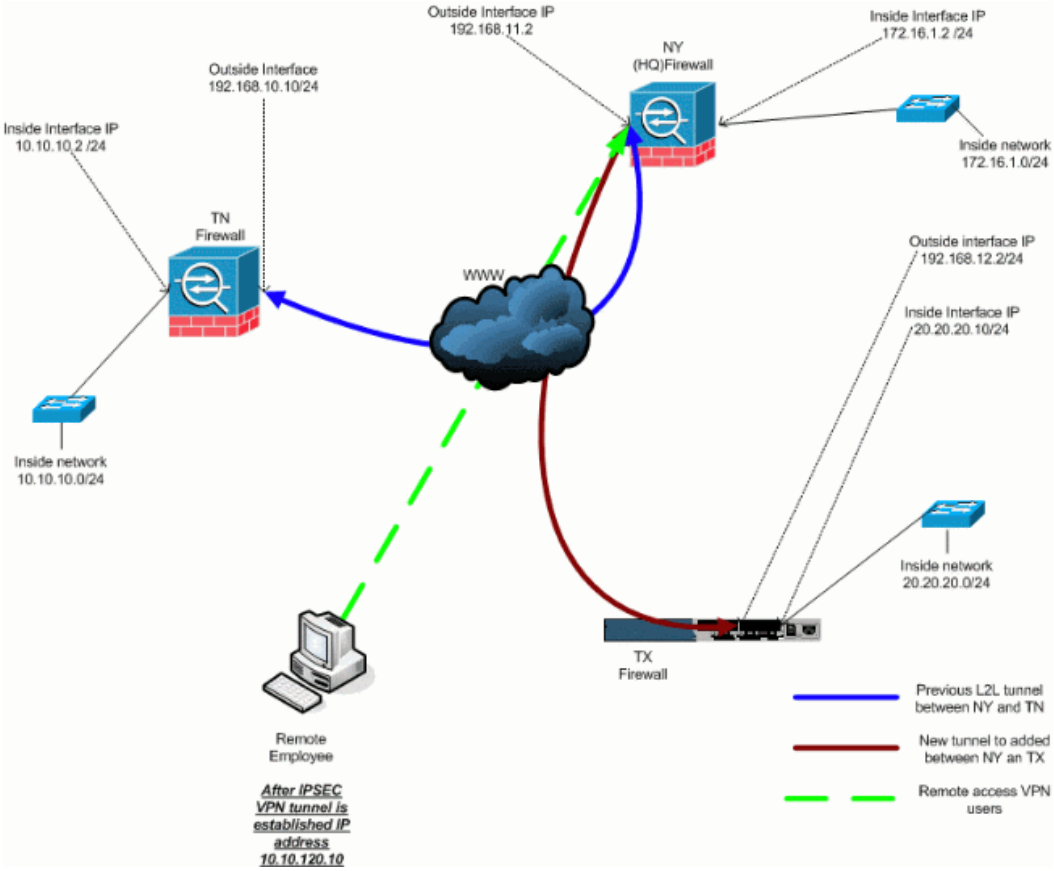
: Saved
:
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
shutdown
```
```

```
no nameif
no security-level
no ip address
!
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
same-security-traffic permit intra-interface
access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 20.20.20.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip 20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
username sidney password 3xsopMX9gN5Wnf1W encrypted privilege 15
aaa authentication telnet console LOCAL
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 30 match address outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.2
crypto map outside_map 30 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 *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
pre-shared-key *
```

```
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 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
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae
: end
ASA-NY-HQ#
```

Добавление удаленного доступа VPN к конфигурации

Схема сети для данной конфигурации:



Пошаговые инструкции

Данный раздел описывает необходимые процедуры по добавлению мощного удаленного доступа и разрешению удаленным пользователям получать доступа ко всем узлам. Дополнительную информацию о настройке серверов удаленного доступа и об ограничении доступа, см. PIX/ASA 7.x ASDM: Ограничение сетевого доступа для пользователей удаленного доступа VPN.

Выполните следующие шаги:

1. Создайте пул IP-адреса, который будет использоваться клиентами подключающимися посредством VPN-туннеля. Также, создайте базового пользователя для получения доступа к VPN после завершения настройки.

   - ```
     ASA-NY-HQ(config)#ip local pool Hill-V-IP
        10.10.120.10-10.10.120.100 mask 255.255.255.0
     ```

   - ```
     ASA-NY-HQ(config)#username cisco password
        cisco111
     ```

2. Освободите специальный трафик от преобразования.

   - ```
     ASA-NY-HQ(config)#access-list
        inside_nat0_outbound extended permit ip 172.16.1.0
        255.255.255.0 10.10.120.0 255.255.255.0
     ```

   - ```
     ASA-NY-HQ(config)#access-list
        inside_nat0_outbound extended permit ip 10.10.120.0
        255.255.255.0 10.10.10.0 255.255.255.0
     ```

   - ```
     ASA-NY-HQ(config)#access-list
        inside_nat0_outbound extended permit ip 10.10.120.0
        255.255.255.0 20.20.20.0 255.255.255.0
     ```

   Обратите внимание, что в данном примере освобождается преобразованная связь между VPN туннелями.

3. Разрешите связь между уже созданными туннелями LAN-LAN.

   - ```
     ASA-NY-HQ(config)#access-list
        outside_20_cryptomap extended permit ip 10.10.120.0
        255.255.255.0 10.10.10.0 255.255.255.0
     ```

   - ```
     ASA-NY-HQ(config)#access-list
        outside_30_cryptomap extended permit ip 10.10.120.0
        255.255.255.0 20.20.20.0 255.255.255.0
     ```

   Это дает возможность пользователям удаленного доступа связываться с сетями в обход определенного туннеля.

    **Предупреждение:** Чтобы осуществить связь, другая сторона туннеля должна иметь противоположные записи списка контроля доступа (ACL) для определенной сети.

4. Настройте трафик, который будет зашифрован и послан через VPN-туннель.

   -
     ```

```
ASA-NY-HQ(config)#access-list
   Hillvalley_splitunnel standard permit 172.16.1.0
   255.255.255.0
```

- ```
  ASA-NY-HQ(config)#access-list
     Hillvalley_splitunnel standard permit 10.10.10.0
     255.255.255.0
  ```

- ```
  ASA-NY-HQ(config)#access-list
     Hillvalley_splitunnel standard permit 20.20.20.0
     255.255.255.0
  ```

5. Настройте локальную проверку подлинности и информацию о политике для VPN-клиентов такие, как коды, dns и протоколы IPSec.

   - ```
     ASA-NY-HQ(config)#group-policy Hillvalley
        internal
     ```

   - ```
     ASA-NY-HQ(config)#group-policy Hillvalley
        attributes
     ```

     - ```
       ASA-NY-HQ(config-group-policy)#wins-server
          value 10.10.10.20
       ```

     - ```
       ASA-NY-HQ(config-group-policy)#dns-server value
          10.10.10.20
       ```

     - ```
       ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
          IPSec
       ```

6. Настройте IPSec и общие атрибуты, которые будут использованы VPN-туннелями Hillvalley такие, как предварительно согласованные ключи и пулы IP-адресов.

   - ```
     ASA-NY-HQ(config)#tunnel-group Hillvalley
        ipsec-attributes
     ```

     - ```
       ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
          cisco1234
       ```

   - ```
     ASA-NY-HQ(config)#tunnel-group Hillvalley
        general-attributes
     ```

     - ```
       ASA-NY-HQ(config-tunnel-general)#address-pool
          Hill-V-IP
       ```
       ```

```
ASA-NY-HQ(config-tunnel-general)#default-group-policy
   Hillvalley
```

7. Создайте политику раздельного туннеля, которая будет использовать ACL созданный в шаге №4, чтобы указать какой трафик будет зашифрован и пущен через туннель.

```
ASA-NY-HQ(config)#split-tunnel-policy
   tunnelspecified
```

```
ASA-NY-HQ(config)#split-tunnel-network-list value
   Hillvalley_splitunnel
```

8. Настройте необходимую для создания VPN-туннелей информацию криптокарт.

```
ASA-NY-HQ(config)#crypto ipsec transform-set
   Hill-trans esp-3des esp-sha-hmac
```

```
ASA-NY-HQ(config)#crypto dynamic-map
   outside_dyn_map 20 set transform-set
   Hill-trans
```

```
ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
   set reverse-route
```

```
ASA-NY-HQ(config)#crypto map outside_map 65535
   ipsec-isakmp dynamic
   outside_dyn_map
```

Пример конфигурации

Второй пример конфигурации

```
ASA-NY-HQ#show running-config

: Saved

hostname ASA-NY-HQ
ASA Version 7.2(2)

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
```

```
shutdown
no nameif
no security-level
no ip address
!
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
same-security-traffic permit intra-interface

!--- Необходимо для связи между одноранговыми узлами VPN.


access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.120.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip 10.10.120.0 255.255.255.0 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
access-list outside_20_cryptomap extended permit ip 20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list Hillvalley_splitunnel standard permit 172.16.1.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit 10.10.10.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit 20.20.20.0 255.255.255.0
access-list outside_30_cryptomap extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip 10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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
group-policy Hillvalley internal
group-policy Hillvalley attributes
wins-server value 10.10.10.20
dns-server value 10.10.10.20
vpn-tunnel-protocol IPSec
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Hillvalley_splitunnel
default-domain value corp.com
username cisco password dZBmhhbNIN5q6rGK encrypted
```

```
aaa authentication telnet console LOCAL
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 ipsec transform-set Hill-trans esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 20 set transform-set Hill-trans
crypto dynamic-map dyn_map 20 set reverse-route
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 30 match address outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.1
crypto map outside_map 30 set transform-set ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
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 *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
pre-shared-key *
tunnel-group Hillvalley type ipsec-ra
tunnel-group Hillvalley general-attributes
address-pool Hill-V-IP
default-group-policy Hillvalley
tunnel-group Hillvalley ipsec-attributes
pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 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
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48
ASA-NY-HQ#
```

Проверка

Используйте этот раздел для того, чтобы подтвердить, что ваша конфигурация работает правильно.

Средство Интерпретатор выходных данных (только для зарегистрированных клиентов) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитики выходных данных команды **show**.

- **ping inside x.x.x.x (IP-адрес хоста на противоположной стороне туннеля)** – Данная команда позволяет посылать трафик по туннелю, используя адрес источника внутреннего интерфейса.

Поиск и устранение неполадок

Данный раздел содержит сведения, которые можно использовать для устранения неполадок вашей конфигурации:

- Наиболее распространенные решения проблем с IPSec VPN
- Устранение неполадок IPSec – общие сведения и использование команд debug
- Устранение неполадок с подключениями через PIX и ASA

Дополнительные сведения

- **Введение в шифрование для обеспечения безопасности протокола IP (IPSec)**
- **Страница технической поддержки протоколов согласования IPSec и IKE**
- **Устройства адаптивной защиты Cisco серии ASA 5500 – Справочник по командам**
- **Cisco Systems – техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107646/addnetworkvpn.shtml