PIX/ASA 7.X : Добавьте новый туннель или удаленный доступ к существующему VPN L2L

Содержание

Введение

Этот документ указывает пошаговую последовательность действий для добавления нового VPN-туннеля или VPN-сети удаленного доступа в существующую конфигурацию VPN L2L. Сведения о создании начальных туннелей IPSEC VPN и разнообразные примеры настроек можно найти в примерах конфигурации и технических примечаниях для устройств адаптивной защиты Cisco ASA серии 5500.

Предварительные условия

Требования

Гарантируйте корректную настройку VPN-туннеля IPSec L2L, который в настоящее время в рабочем состоянии перед попыткой этой конфигурации.

Используемые компоненты

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

- Два Устройства обеспечения безопасности ASA, которые работают 7.x код
- Одно устройство безопасности PIX, которое выполняется 7.x код

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.

Схема сети

В настоящем документе используется следующая схема сети:

Эти выходные данные являются текущей рабочей конфигурацией NY (КОНЦЕНТРАТОР) устройство безопасности. В этой конфигурации существует туннель L2L IPSec, настроенный между NY (HQ) и TN.

Текущий NY (HQ) конфигурация 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 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 !--- 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 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 настоящее время существует существующий туннель L2L, установленный между NY (HQ) офис и офисом TN. Ваша компания недавно открыла новый офис, который расположен в TX. Этот новый офис требует подключения к локальным ресурсам, которые расположены в NY и офисах TN. Кроме того, существует дополнительное требование, чтобы позволить сотрудникам возможность работать из дома и надежно обратиться к ресурсам, которые расположены на внутренней сети удаленно. В данном примере новый VPN-туннель настроен, а также сервер VPN для удаленного доступа, который расположен в офис NY.

В данном примере используются две команды, чтобы позволить связь между сетями VPN и определить трафик, который должен быть туннелирован или зашифрован. Это позволяет вам иметь доступ к Интернету, не имея необходимость передавать тот трафик через VPN-туннель. **Чтобы настроить эти два действия, задайте команды split-tunnel и same-security-traffic.**

Разделенное туннелирование позволяет Клиенту IPSEC удаленного доступа условно прямым пакетам по Туннелю IPSec в зашифрованной форме, или к сетевому интерфейсу в форме открытого текста. С включенным разделенным туннелированием пакеты, не направляющиеся в назначения с другой стороны Туннеля IPSec, не должны быть зашифрованы, переданы через туннель, дешифровали, и затем маршрутизировали к конечному назначению. Эта команда применяет эту политику разделенного туннелирования к указанной сети. По умолчанию должен туннелировать весь трафик. **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 безопасности включает функцию, которая позволяет клиенту VPN передавать ТРАФИК С ЗАЩИТОЙ ПО ПРОТОКОЛУ IPSEC другим пользователям VPN путем разрешения такому трафику войти и из того же интерфейса. Также названный прикреплением, эта функция может считаться лучами VPN (клиенты), которые соединяются через концентратор VPN (устройство безопасности). В другом приложении эта функция может перенаправить входящий трафик VPN, отступают через тот же интерфейс как незашифрованный трафик. Это полезно, например, клиенту VPN, который не имеет разделенного туннелирования, но должен и обратиться к VPN и просмотреть веб-сайты. *Задайте команду same-security-traffic intra-interface в режиме глобального конфигурирования, чтобы настроить данную функцию.*

Добавьте дополнительный туннель L2L к конфигурации

Это - схема сети для этой конфигурации:

Пошаговые инструкции

Этот раздел предоставляет требуемые процедуры, которые должны быть выполнены на КОНЦЕНТРАТОРЕ (Межсетевой экран NY) устройство безопасности. См. PIX/ASA 7. x: Пример простой настройки VPN-туннеля PIX-PIX.

Выполните следующие действия:

1. Создайте эти два новых списка доступа, которые будут использоваться криптокартой, для определения представляющего интерес трафика:`ASA-NY-HQ(config)#access-list outside_30_cryptomap extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-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`**% Warning:** Для связи для имения место другая сторона туннеля должна иметь противоположность этой записи списка контроля доступа (ACL) для той индивидуальной сети.
2. Добавьте эти записи ни в какое выражение NAT для освобождения преобразовывания посредством NAT между этими сетями:`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0ASA-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`**% Warning:** Для связи для имения место другая сторона туннеля должна иметь противоположность этой записи ACL для той индивидуальной сети.
3. Выполните эту команду, чтобы позволить хосту на сети VPN TX иметь доступ к VPN-туннелю TN:`ASA-NY-HQ(config)#same-security-traffic permit intra-interface`Это позволяет узлам VPN говорить друг между другом.
4. Создайте конфигурацию криптокарты для нового VPN-туннеля. Используйте тот же набор преобразований, который использовался в первой конфигурации VPN, поскольку все параметры настройки фазы 2 являются тем же.`ASA-NY-HQ(config)#crypto map outside_map 30 match address outside_30_cryptomapASA-NY-HQ(config)#crypto map outside_map 30 set peer 192.168.12.2ASA-NY-HQ(config)#crypto map outside_map 30 set transform-set ESP-3DES-SHA`
5. Создайте туннельную группу, которая задана для этого туннеля наряду с атрибутами, должен был соединиться с удаленным хостом.`ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type ipsec-l2lASA-NY-HQ(config)#tunnel-group 192.168.12.2 ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key cisco123`**Примечание:** Предварительный общий ключ должен совпасть точно с обеих сторон туннеля.
6. Теперь, когда вы настроили новый туннель, необходимо передать представляющий интерес трафик через туннель для внедрения его. **Чтобы осуществить это, задайте команду source ping для отправки эхо-запроса на хост внутренней сети удаленного туннеля.**В данном примере пропингована рабочая станция с другой стороны туннеля с адресом 20.20.20.16. Это переводит туннель в рабочее состояние между NY и TX.

Теперь, существует два туннеля, связанные с офисом HQ. Если у вас нет доступа к системе позади туннеля, обратитесь к Наиболее распространенным Решениям для Устранения проблем IPSEC VPN найти альтернативное решение относительно использования `management-access`.

Пример конфигурации

Пример конфигурации 1

```
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#
```

Добавьте VPN для удаленного доступа к конфигурации

Это - схема сети для этой конфигурации:

Пошаговые инструкции

Этот раздел предоставляет требуемые процедуры, чтобы добавить возможность удаленного доступа и позволить удаленным пользователям обращаться ко всем узлам. См. PIX/ASA 7.x ASDM: Ограничение сетевого доступа для пользователей удаленного доступа VPN.

Выполните следующие действия:

1. Создайте пул IP-адреса, который будет использоваться для клиентов, которые соединяются через VPN-туннель. Кроме того, создайте рядового пользователя для доступа к VPN, как только завершена конфигурация.`ASA-NY-HQ(config)#ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask 255.255.255.0ASA-NY-HQ(config)#username cisco password cisco111`
2. Освободите определенный трафик от того, чтобы быть преобразованным посредством NAT.`ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 10.10.120.0 255.255.255.0ASA-NY-HQ(config)#access-list inside_nat0_outbound extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0 255.255.255.0ASA-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`Заметьте, что туземная связь между VPN-туннелями освобождена в данном примере.
3. Позвольте связь между туннелями L2L, которые уже созданы.`ASA-NY-HQ(config)#access-list outside_20_cryptomap extended permit ip 10.10.120.0 255.255.255.0 10.10.10.0 255.255.255.0ASA-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 позволяет пользователям удаленного доступа способность связаться с сетями позади указанных туннелей.**% Warning:** Для

связи для имения место другая сторона туннеля должна иметь противоположность этой записи ACL для той индивидуальной сети.

4. Настройте трафик, который будет зашифрован и передан через VPN-туннель.
```
ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 172.16.1.0
    255.255.255.0ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 10.10.10.0
    255.255.255.0ASA-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, такую как wins, dns и Протоколы IPSec, для клиентов VPN.
```
ASA-NY-HQ(config)#group-policy Hillvalley
 internalASA-NY-HQ(config)#group-policy Hillvalley
 attributesASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```
6. IPSec набора и общие атрибуты, такие как предварительные общие ключи и пулы IP-адреса, которые будут использоваться VPN-туннелем Hillvalley.
```
ASA-NY-HQ(config)#tunnel-group Hillvalley
 ipsec-attributesASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234ASA-NY-HQ(config)#tunnel-group Hillvalley
 general-attributesASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IPASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```
7. Создайте политику раздельных туннелей, которая будет использовать ACL, созданный в шаге 4 для определения, какой трафик будет зашифрован и пройдется туннель.
```
ASA-NY-HQ(config)#split-tunnel-policy
 tunnelspecifiedASA-NY-HQ(config)#split-tunnel-network-list value
 Hillvalley_splitunnel
```
8. Настройте cryto сведения о сопоставлении, требуемые к созданию VPN-туннеля.
```
ASA-NY-HQ(config)#crypto ipsec transform-set
 Hill-trans esp-3des esp-sha-hmacASA-NY-HQ(config)#crypto dynamic-map
 outside_dyn_map 20 set transform-set
 Hill-transASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
 set reverse-routeASA-NY-HQ(config)#crypto map outside_map 65535
 ipsec-isakmp dynamic
 outside_dyn_map
```

Пример конфигурации

Пример конфигурации 2

```
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 !--- This is
required for communication between VPN peers. 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

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.**

- **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.**

Устранение неполадок

См. эти документы для получения информации можно использовать для устранения проблем конфигурации:

- Наиболее распространенные решения для устранения проблем IPSEC VPN
- Устранение проблем IPSec — общие сведения и использование команд debug
- Устранение неполадок в подключениях через PIX и ASA

Дополнительные сведения

- Введение в шифрование IPSec
- Страница технической поддержки протоколов согласования IPSec и IKE
- Справочники по командам устройств адаптивной защиты Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация