

Динамический узел к узлу VPN-туннель IKEv2 между двумя примерами конфигурации ASA

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Схема сети](#)

[Настройка](#)

[Решение 1 - использование DefaultL2LGroup](#)

[Статическая конфигурация ASA](#)

[Динамический ASA](#)

[Решение 2 - создает определяемую пользователем туннельную группу](#)

[Статическая конфигурация ASA](#)

[Динамическая конфигурация ASA](#)

[Проверка](#)

[На статическом ASA](#)

[На динамическом ASA](#)

[Устранение неполадок](#)

Введение

Этот документ описывает, как настроить VPN-туннель второй версии протокола Internet Key Exchange (IKEv2) от узла к узлу между двумя Устройствами адаптивной безопасности (ASA), где один ASA имеет динамический IP - адрес, и другой имеет статический IP - адрес.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Версия ASA 5505
- Версия ASA 9.1 (5)

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.

Общие сведения

Существует два способа, которыми может быть установлена эта конфигурация:

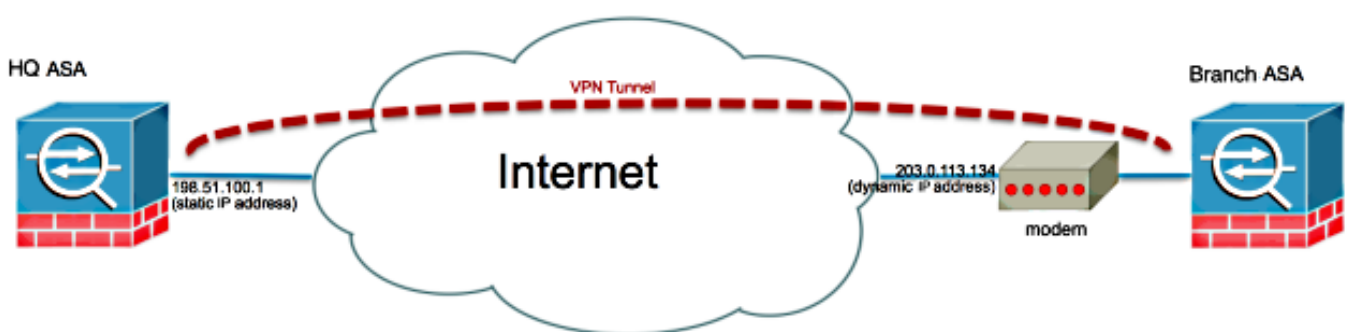
- С туннельной группой DefaultL2LGroup
- С именованной туннельной группой

Самое большое различие в настройке между этими двумя сценариями является ID Протокола ISAKMP, используемым удаленным ASA. Когда DefaultL2LGroup используется на статическом ASA, ID ISAKMP узла должен быть адресом. Однако, если именованная туннельная группа используется, ID ISAKMP узла должен быть тем же имя группы туннелей с помощью этой команды:

```
crypto isakmp identity key-id <tunnel-group_name>
```

Преимущество использования именованных туннельных групп на статическом ASA состоит в том, что то, когда DefaultL2LGroup используется, конфигурация на удаленных динамических ASA, которая включает предварительные общие ключи, должно быть идентичным, и это не обеспечивает много глубины детализации с настройкой политики.

Схема сети



Настройка

В этом разделе описываются конфигурацию на каждом ASA, в зависимости от которого решения вы решаете использовать.

Решение 1 - использование DefaultL2LGroup

Когда один ASA получает свой адрес динамично, это - самый простой способ настроить LAN-LAN (L2L) туннель между двумя ASA. DefaultL2L Group является предварительно сконфигурированной туннельной группой на ASA и всех соединениях, которые явно не совпадают ни с каким падением группы конкретного туннеля на этом соединении. Так как Динамический ASA не имеет постоянного предопределенного IP-адреса, это означает, что admin не может настроить ASA Statis для разрешения соединения на определенной туннельной группе. В этой ситуации DefaultL2L Group может использоваться для разрешения динамических соединений.

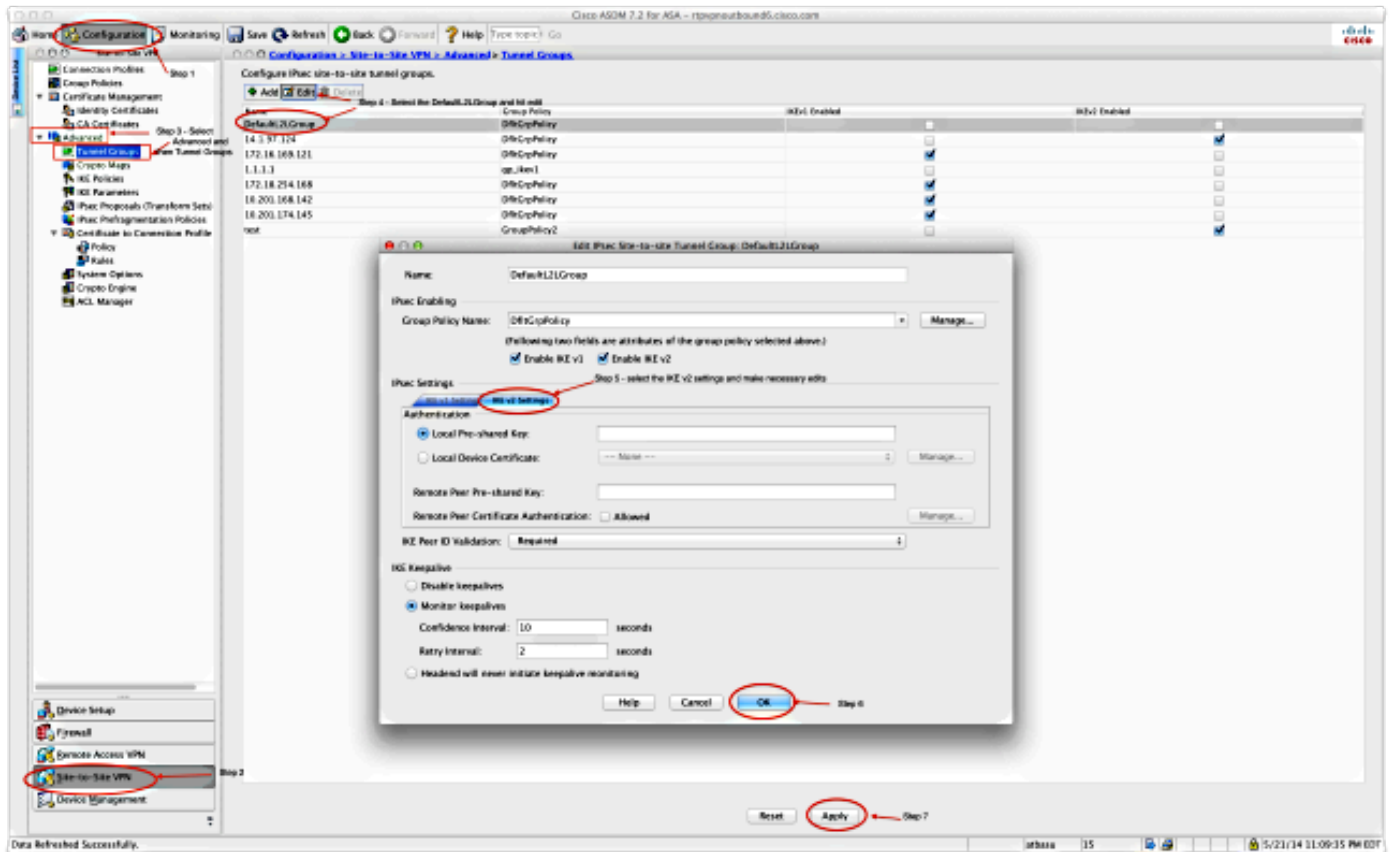
Совет: С этим методом обратная сторона - то, что все узлы будут иметь тот же предварительный общий ключ, так как только один предварительный общий ключ может быть определен на туннельную группу, и все узлы соединятся с той же туннельной группой DefaultL2LGroup.

Статическая конфигурация ASA

```
interface Ethernet0/0
 nameif inside
 security-level 100
 IP address 172.30.2.6 255.255.255.0
!
interface Ethernet0/3
 nameif Outside
 security-level 0
 IP address 207.30.43.15 255.255.255.128
!
boot system disk0:/asa915-k8.bin
crypto ipsec IKEv2 ipsec-proposal Site2Site
 protocol esp encryption aes-256
 protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 10 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-
256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set IKEv2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map Outside_map interface Outside
crypto IKEv2 policy 2
 encryption aes-256
```

```
integrity sha512
group 24
prf sha512
lifetime seconds 86400
crypto IKEv2 policy 3
  encryption aes-256
  integrity sha group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 40
  encryption des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 enable inside client-services port 443
crypto IKEv2 enable Outside client-services port 443
group-policy Site2Site internal
group-policy Site2Site attributes
  vpn-idle-timeout none
  vpn-session-timeout none
  vpn-filter none
  vpn-tunnel-protocol IKEv2
tunnel-group DefaultL2LGroup general-attributes
  default-group-policy Site2Site
tunnel-group DefaultL2LGroup ipsec-attributes
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****
```

На Менеджере устройств адаптивной безопасности (ASDM) (ASDM) можно настроить DefaultL2LGroup как показано здесь:



Динамический ASA

```

interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif inside
  security-level 100
  IP address 172.16.1.1 255.255.255.224
!
interface Vlan2
  nameif outside
  security-level 0
  IP address dhcp setroute
!
ftp mode passive
object network NETWORK_OBJ_172.16.1.0_24
  subnet 172.16.1.0 255.255.255.0
object-group network DM_INLINE_NETWORK_1
  network-object object 10.0.0.0

```

```
network-object object 172.0.0.0
access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
object-group DM_INLINE_NETWORK_1
nat (inside,outside) source static NETWORK_OBJ_172.16.1.0_24 NETWORK_OBJ_
172.16.1.0_24 destination static DM_INLINE_NETWORK_1 DM_INLINE_NETWORK_1
nat (inside,outside) source dynamic any interface
crypto ipsec IKEv2 ipsec-proposal Site2Site
  protocol esp encryption aes-256
  protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal DES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs group5
crypto map outside_map 1 set peer 198.51.100.1
crypto map outside_map 1 set ikev1 phase1-mode aggressive group5
crypto map outside_map 1 set IKEv2 ipsec-proposal Site2Site
crypto map outside_map interface outside
crypto IKEv2 policy 2
  encryption aes-256
  integrity sha512
  group 24
  prf sha512
  lifetime seconds 86400
crypto IKEv2 policy 3
  encryption aes-256
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
crypto IKEv2 policy 40
  encryption des
  integrity sha
```

```

group 5 2
prf sha
lifetime seconds 86400
crypto IKEv2 enable outside
management-access inside
group-policy GroupPolicy_198.51.100.1 internal
group-policy GroupPolicy_198.51.100.1 attributes
  vpn-tunnel-protocol IKEv2
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 general-attributes
  default-group-policy GroupPolicy_198.51.100.1
tunnel-group 198.51.100.1 ipsec-attributes
  ikev1 pre-shared-key *****
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****

```

На ASDM можно использовать типичного мастера для устанавливания соответствующего профиля подключения, или можно просто добавить новое соединение и выполнить стандартную процедуру.

Решение 2 - создает определяемую пользователем туннельную группу

Этот метод требует немного большего количества конфигурации, но это обеспечивает больше глубины детализации. Каждый узел может иметь свою собственную отдельную политику и предварительный общий ключ. Однако, здесь важно изменить ID ISAKMP на динамическом узле так, чтобы это использовало название вместо IP-адреса. Это позволяет статическому ASA совпадать с входящим запросом инициализации ISAKMP к правильной туннельной группе и использовать правильную политику.

Статическая конфигурация ASA

```

interface Ethernet0/0
  nameif inside
  security-level 100
  IP address 172.16.0.1 255.255.255.0
!
interface Ethernet0/3
  nameif Outside
  security-level 0
  IP address 198.51.100.1 255.255.255.128
!
boot system disk0:/asa915-k8.bin
object-group network DM_INLINE_NETWORK_1
  network-object object 10.0.0.0
  network-object object 172.0.0.0

access-list Outside_cryptomap_1 extended permit IP object-group DM_INLINE_NETWORK_
1 172.16.1.0 255.255.255.0

crypto ipsec IKEv2 ipsec-proposal Site2Site
  protocol esp encryption aes-256
  protocol esp integrity sha-1
crypto ipsec IKEv2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5

```

```
crypto ipsec IKEv2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal 3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec IKEv2 ipsec-proposal DES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
crypto engine large-mod-accel
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-
SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set IKEv2 ipsec-proposal
AES256 AES192 AES 3DES DES
crypto dynamic-map DynamicSite2Site1 4 match address Outside_cryptomap_1
crypto dynamic-map DynamicSite2Site1 4 set IKEv2 ipsec-proposal Site2Site
crypto map Outside_map 65534 ipsec-isakmp dynamic DynamicSite2Site1
crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map Outside_map interface Outside
```

```
crypto IKEv2 policy 2
  encryption aes-256
  integrity sha512
  group 24
  prf sha512
  lifetime seconds 86400
```

```
crypto IKEv2 policy 3
  encryption aes-256
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
```

```
crypto IKEv2 policy 10
  encryption aes-192
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
```

```
crypto IKEv2 policy 20
  encryption aes
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
```

```
crypto IKEv2 policy 30
  encryption 3des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
```

```
crypto IKEv2 policy 40
  encryption des
  integrity sha
  group 5 2
  prf sha
  lifetime seconds 86400
```

```
crypto IKEv2 enable Outside client-services port 443
management-access inside
```

```
group-policy GroupPolicy4 internal
group-policy GroupPolicy4 attributes
  vpn-tunnel-protocol IKEv2
```

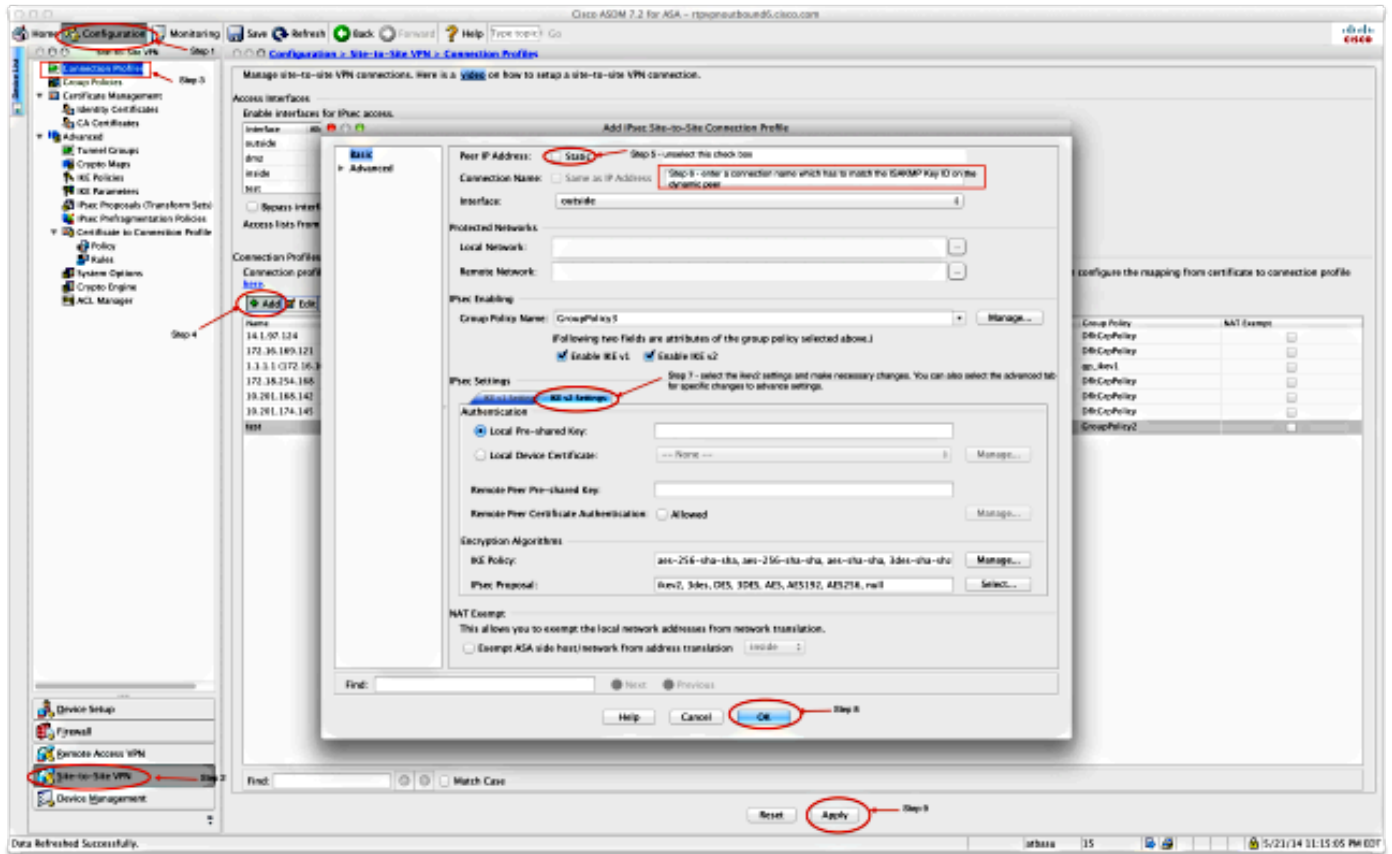


```

tunnel-group DynamicSite2Site1 type ipsec-l2l
tunnel-group DynamicSite2Site1 general-attributes
  default-group-policy GroupPolicy4
tunnel-group DynamicSite2Site1 ipsec-attributes
  IKEv2 remote-authentication pre-shared-key *****
  IKEv2 local-authentication pre-shared-key *****

```

На ASDM названием профиля подключения является IP-адрес по умолчанию. Таким образом, при создании его необходимо изменить его, чтобы дать ему название как показано в снимке экрана здесь:



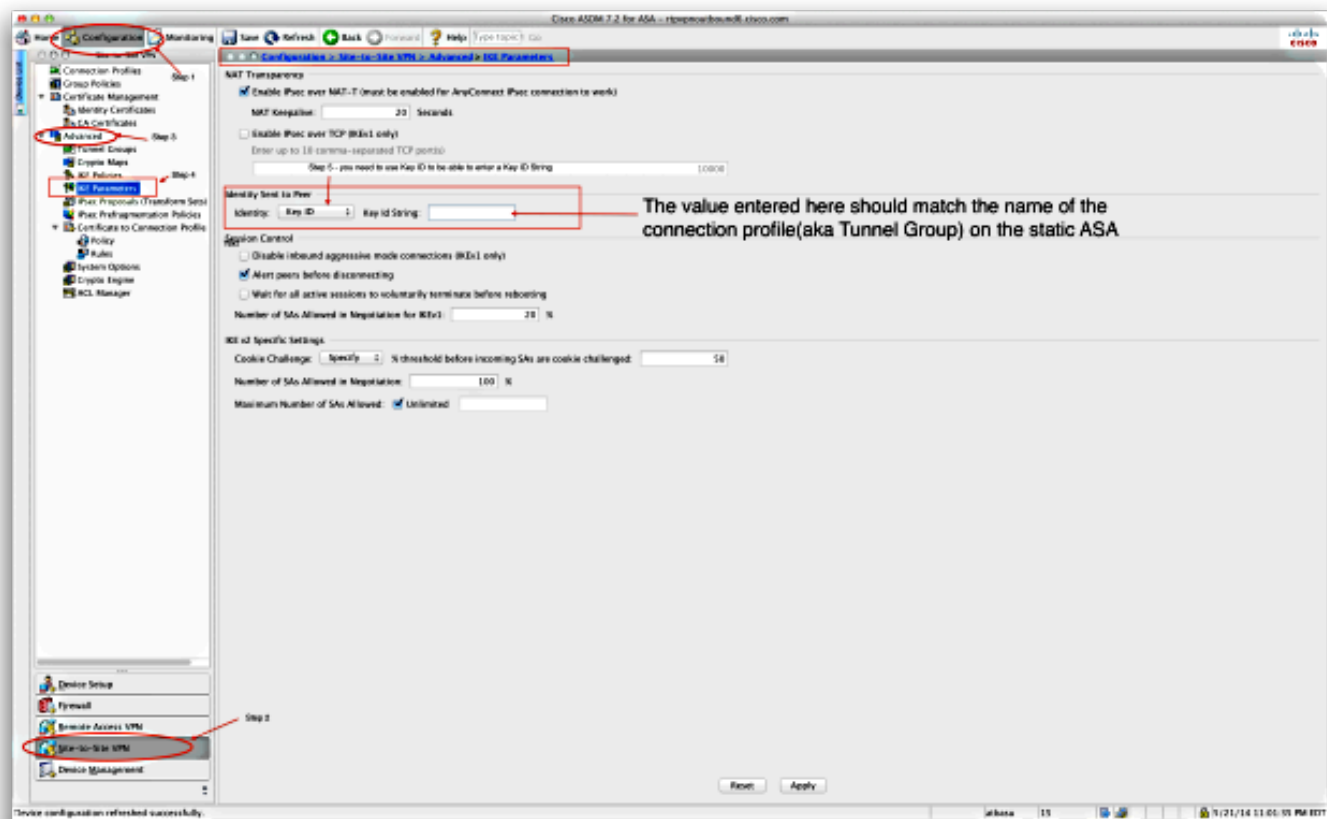
Динамическая конфигурация ASA

Динамический ASA настроен почти тот же путь в обоих решениях с добавлением одной команды как показано здесь:

```
crypto isakmp identity key-id DynamicSite2Site1
```

Как описано ранее, по умолчанию ASA использует IP-адрес интерфейса, что VPN-туннель сопоставлен с как ID ключа isakmp. Однако, в этом случае ключевой ID на динамическом ASA совпадает с названием туннельной группы на Статическом ASA. Таким образом на каждом динамическом узле, ключевой идентификатор будет другим, и соответствующая туннельная группа должна быть создана на Статическом ASA с правильным названием.

На ASDM это может быть настроено как показано в этом снимке экрана:



Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

На статическом ASA

Вот является результат покажите крипто-ikev2 sa det командой:

IKEv2 SAs:

```
Session-id:132, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id          Local              Remote            Status            Role
1574208993         198.51.100.1/4500 203.0.113.134/4500  READY            RESPONDER
    Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK,
Auth verify: PSK
    Life/Active Time: 86400/352 sec
    Session-id: 132
    Status Description: Negotiation done
    Local spi: 4FDF215BDEC73EC          Remote spi: 2414BEA1E10E3F70
    Local id: 198.51.100.1
    Remote id: DynamicSite2Site1
    Local req mess id: 13                Remote req mess id: 17
    Local next mess id: 13              Remote next mess id: 17
    Local req queued: 13                Remote req queued: 17
    Local window: 1                     Remote window: 1
    DPD configured for 10 seconds, retry 2
    NAT-T is detected outside
```

```
Child sa: local selector 172.0.0.0/0 - 172.255.255.255/65535
remote selector 172.16.1.0/0 - 172.16.1.255/65535
ESP spi in/out: 0x9fd5c736/0x6c5b3cc9
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Вот результат команды **show crypto ipsec sa:**

```
interface: Outside
Crypto map tag: DynamicSite2Site1, seq num: 4, local addr: 198.51.100.1

access-list Outside_cryptomap_1 extended permit IP 172.0.0.0 255.0.0.0
172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 203.0.113.134

#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 12, #pkts decrypt: 12, #pkts verify: 12
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 198.51.100.1/4500, remote crypto endpt.:
203.0.113.134/4500
path mtu 1500, ipsec overhead 82(52), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 6C5B3CC9
current inbound spi : 9FD5C736

inbound esp sas:
spi: 0x9FD5C736 (2681587510)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
sa timing: remaining key lifetime (kB/sec): (4193279/28441)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00001FFF

outbound esp sas:
spi: 0x6C5B3CC9 (1817918665)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
slot: 0, conn_id: 1081344, crypto-map: DynamicSite2Site1
sa timing: remaining key lifetime (kB/sec): (3962879/28441)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

На динамическом ASA

Вот результат **подробной** команды **покажите крипто-ikev2 sa:**

IKEv2 SAs:

Session-id:11, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id          Local              Remote            Status            Role
1132933595 192.168.50.155/4500 198.51.100.1/4500  READY           INITIATOR
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:24, Auth sign: PSK,
Auth verify: PSK
  Life/Active Time: 86400/267 sec
  Session-id: 11
  Status Description: Negotiation done
  Local spi: 2414BEA1E10E3F70      Remote spi: 4FDFF215BDEC73EC
  Local id: DynamicSite2Site1
  Remote id: 198.51.100.1
  Local req mess id: 13              Remote req mess id: 9
  Local next mess id: 13            Remote next mess id: 9
  Local req queued: 13              Remote req queued: 9
  Local window: 1                    Remote window: 1
  DPD configured for 10 seconds, retry 2
  NAT-T is detected inside
Child sa: local selector 172.16.1.0/0 - 172.16.1.255/65535
  remote selector 172.0.0.0/0 - 172.255.255.255/65535
  ESP spi in/out: 0x6c5b3cc9/0x9fd5c736
  AH spi in/out: 0x0/0x0
  CPI in/out: 0x0/0x0
  Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
  ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Вот результат команды show crypto ipsec sa:

```
interface: outside
  Crypto map tag: outside_map, seq num: 1, local addr: 192.168.50.155

  access-list outside_cryptomap extended permit IP 172.16.1.0 255.255.255.0
172.0.0.0 255.0.0.0
  local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (172.0.0.0/255.0.0.0/0/0)
  current_peer: 198.51.100.1

  #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
  #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 12, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.50.155/4500, remote crypto endpt.:
198.51.100.1/4500
  path mtu 1500, ipsec overhead 82(52), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: 9FD5C736
  current inbound spi : 6C5B3CC9

inbound esp sas:
  spi: 0x6C5B3CC9 (1817918665)
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 5, IKEv2, }
  slot: 0, conn_id: 77824, crypto-map: outside_map
  sa timing: remaining key lifetime (kB/sec): (4008959/28527)
  IV size: 16 bytes
  replay detection support: Y
```

```
Anti replay bitmap:
  0x00000000 0x00000003
outbound esp sas:
spi: 0x9FD5C736 (2681587510)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, PFS Group 5, IKEv2, }
slot: 0, conn_id: 77824, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4147199/28527)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
  0x00000000 0x00000001
```

[Средство интерпретации выходных данных \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды show . Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

[Средство интерпретации выходных данных \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды show . Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

Примечание: [Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки"](#).

- deb крипто-пакет IKEv2
- deb, крипто-IKEv2 внутренний