Динамический узел к узлу VPN-туннель IKEv2 между ASA и примером конфигурации маршрутизатора IOS

Содержание

Введение

Этот документ описывает, как настроить VPN-туннель второй версии протокола Internet Key Exchange (IKEv2) от узла к узлу между Устройством адаптивной защиты (ASA) и маршрутизатором Cisco, где маршрутизатор имеет динамический IP - адрес, и ASA имеет статический IP - адрес на стоящих с общественностью интерфейсах.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco IOS® Version 15.1 (1) T или позже
- Версия 8.4 (1) Cisco ASA или позже

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

Этот документ обсуждает эти сценарии:

- Сценарий 1: ASA настроен со статическим IP - адресом, который использует именованную туннельную группу, и маршрутизатор настроен с динамическим IP - адресом.

- Сценарий 2: ASA настроен с динамическим IP - адресом, и маршрутизатор настроен с динамическим IP - адресом.

- Ситуация 3: Этот сценарий не обсужден здесь. В этом сценарии ASA настроен со статическим IP - адресом, но использует туннельную группу DefaultL2LGroup. Конфигурация для этого подобна тому, что описано в статье Dynamic Site to Site IKEv2 VPN Tunnel Between Two ASAs Configuration Example.

Самое большое различие в настройке между Сценариями 1 и 3 является ID Протокола ISAKMP, используемым удаленным маршрутизатором. Когда DefaultL2LGroup используется на статическом ASA, ID ISAKMP узла на маршрутизаторе должен быть адресом ASA. Однако, если именованная туннельная группа используется, ID ISAKMP узла на маршрутизаторе должен совпасть с именем группы туннелей, настроенным на ASA. Это выполнено с этой командой на маршрутизаторе:

```
identity local key-id <name of the tunnel-group on the static ASA>
```

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

Настройка

Сценарий 1

Схема сети

!--- конфигурацию

В этом разделе описываются конфигурацию на ASA и маршрутизаторе на основе Именованной конфигурации туннельной группы.

Статическая конфигурация ASA

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

Динамическая конфигурация маршрутизатора

Динамический маршрутизатор настроен почти тот же путь, как вы обычно настраиваете в случаях, где маршрутизатор является динамическим узлом для туннеля IKEv2 L2L с добавлением одной команды как показано здесь:

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
```

```
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

Таким образом на каждом динамическом узле, ключевой идентификатор является другим, и соответствующая туннельная группа должна быть создана на Статическом ASA с правильным названием, которое также увеличивает глубину детализации polocies, которые внедрены на ASA.

Сценарий 2

> **Примечание:** Когда по крайней мере одна сторона является маршрутизатором, эта конфигурация только возможна. Если обе стороны являются ASA, эта настройка не работает в это время. В Версии 8.4 ASA не в состоянии использовать Полное доменное имя (FQDN) с **командой set peer**, но усовершенствование CSCus37350 запросили на будущие версии.

Если IP-адрес удаленного ASA является динамичным, также, однако, назначили Полное доменное имя для его интерфейса VPN, то вместо того, чтобы определять IP-адрес удаленного ASA, вы теперь определяете FQDN удаленного ASA с этой командой на маршрутизаторе:

```
C1941(config)#do show run | sec crypto map

crypto map vpn 10 ipsec-isakmp
 set peer <FQDN> dynamic
```

> **Совет: Динамическое ключевое слово** является дополнительным. При определении имени хоста удаленного узла IPsec через **команду set peer** можно также выполнить динамическое ключевое слово, которое отсрочивает разрешение Сервера доменных имен (DNS) имени хоста до прямо, прежде чем был установлен Туннель IPSec.
>
> Задержка разрешения позволяет программному обеспечению Cisco IOS обнаружить, изменился ли IP-адрес удаленного узла IPsec. Таким образом программное обеспечение может связаться с узлом в новом IP-адресе. Если динамическое ключевое слово не выполнено, имя хоста сразу решено после того, как это задано.

Так, программное обеспечение Cisco IOS не может обнаружить изменение IP-адреса и, поэтому, попытки соединиться с IP-адресом, который оно ранее решило.

Схема сети

!--- конфигурацию

Динамическая конфигурация ASA

Конфигурация на ASA совпадает со Статической Конфигурацией ASA только за одним исключением, которое является, что статически не определен IP-адрес на физическом интерфейсе.

Настройка маршрутизатора

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
 hostname asa5510.test.com
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
 !
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel

crypto map vpn 10 ipsec-isakmp
 set peer asa5510.test.com dynamic
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Статический ASA

- Вот является результат **покажите крипто-ikev2 sa det** командой:

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id                Local                Remote    Status        Role
120434199       201.1.1.2/4500       201.1.1.1/4500     READY   RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C      Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
     Remote id: S2S-IKEv2
     Local req mess id: 43            Remote req mess id: 2
     Local next mess id: 43           Remote next mess id: 2
     Local req queued: 43             Remote req queued: 2
     Local window: 1                  Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected outside
Child sa: local selector 201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

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

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote    Status        Role
120434199       201.1.1.2/4500       201.1.1.1/4500     READY   RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C      Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
     Remote id: S2S-IKEv2
     Local req mess id: 43            Remote req mess id: 2
     Local next mess id: 43           Remote next mess id: 2
     Local req queued: 43             Remote req queued: 2
     Local window: 1                  Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected outside
Child sa: local selector 201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Динамический маршрутизатор

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

```
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                Remote               fvrf/ivrf            Status
1         192.168.1.2/4500     201.1.1.2/4500       none/none            READY
```

```
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
     Local spi: 67E01CB8E8619AF1      Remote spi: 97272A4B4DED4A5C
     Local id: S2S-IKEv2
     Remote id: 201.1.1.2
     Local req msg id: 2             Remote req msg id: 48
     Local next msg id: 2             Remote next msg id: 48
     Local req queued: 2             Remote req queued: 48
     Local window:     5             Remote window:     1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2 SA
```

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

```
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
     Local spi: 67E01CB8E8619AF1      Remote spi: 97272A4B4DED4A5C
     Local id: S2S-IKEv2
     Remote id: 201.1.1.2
     Local req msg id: 2             Remote req msg id: 48
     Local next msg id: 2             Remote next msg id: 48
     Local req queued: 2             Remote req queued: 48
     Local window:     5             Remote window:     1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2 SA
```

Динамический маршрутизатор (с удаленным динамическим ASA)

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

```
C1941#show cry ikev2 sa detailed
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1516 sec
     CE id: 1034, Session-id: 24
     Status Description: Negotiation done
     Local spi: 98322AED6163EE83      Remote spi: 092A1E5620F6AA9C
     Local id: S2S-IKEv2
```

```
      Remote id: asa5510.test.com
      Local req msg id: 2             Remote req msg id: 73
      Local next msg id: 2             Remote next msg id: 73
      Local req queued: 2             Remote req queued: 73
      Local window:     5             Remote window:     1
      DPD configured for 0 seconds, retry 0
      Fragmentation not configured.
      Extended Authentication not configured.
      NAT-T is detected inside
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes

 IPv6 Crypto IKEv2 SA
```

Примечание: Удаленный и локальный ID в этих выходных данных является **именованной туннельной группой**, которую вы определили на ASA, чтобы проверить, падаете ли вы на правильную туннельную группу. Это может также быть проверено при отладке IKEv2 на любом конце.

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".

На маршрутизаторе Cisco IOS используйте:

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

На ASA используйте:

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```