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

Содержание

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 оборотная 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

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

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

Динамический ASA

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

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

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

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:

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

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

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

На динамическом ASA

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

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

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

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

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**