Подключение VPN Client ASA через пример конфигурации туннеля L2L

Содержание

Введение

Этот документ описывает, как настроить устройство адаптивной защиты Cisco (ASA) для разрешения соединения удаленного клиента VPN от От lan к lan (L2L) адрес партнера (peer).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco ASA
- VPN для удаленного доступа
- VPN LAN-LAN

Используемые компоненты

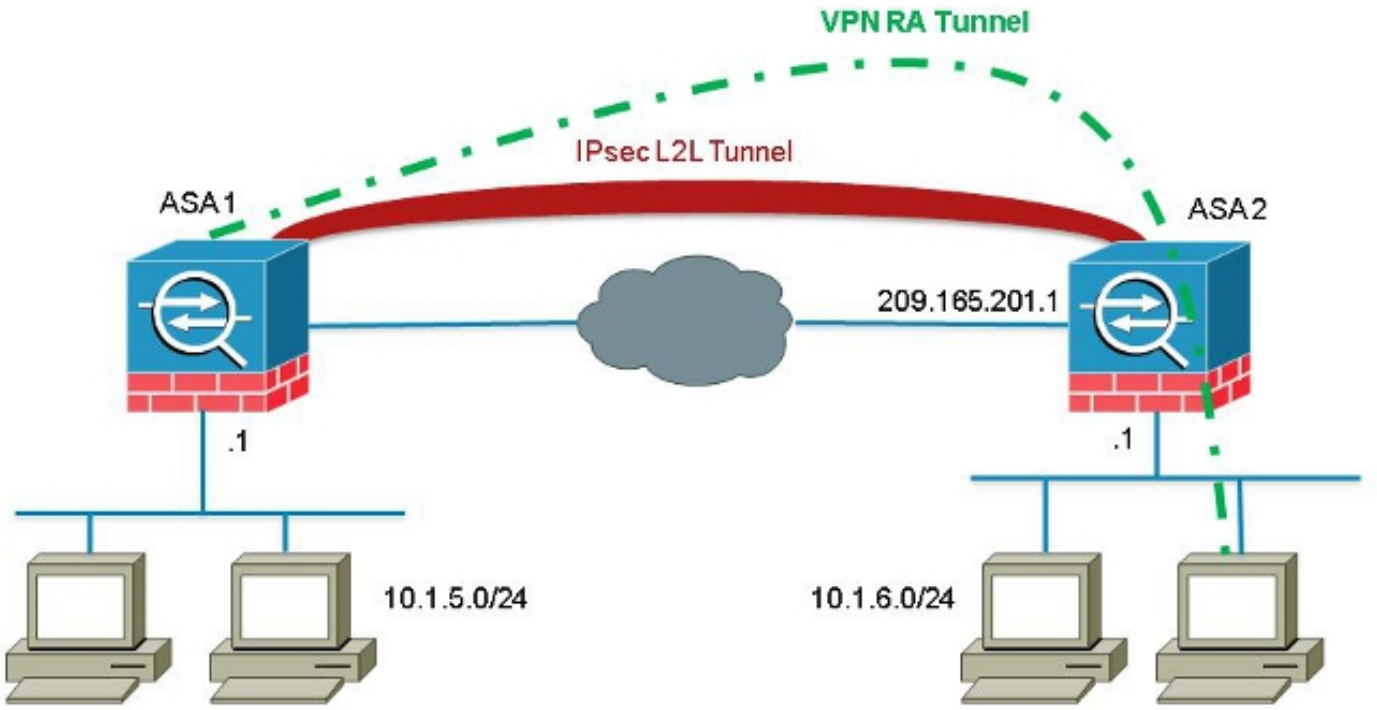
Сведения в этом документе основываются на Cisco ASA серии 5520, который работает под управлением ПО версии 8.4 (7).

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

Несмотря на то, что не распространено встретиться со сценарием, где клиент VPN пытается установить соединение через туннель L2L, администраторы могли бы хотеть назначить определенные привилегии или ограничения доступа определенным удаленным пользователям и дать им команду использовать клиентское программное обеспечение, когда требуется доступ к этим ресурсам.

> **Примечание:** Этот сценарий работал в прошлом, но после обновления ASA головного узла к Версии 8.4 (6) или позже, клиент VPN больше не не быть в состоянии установить соединение.



Идентификатор ошибки Cisco CSCuc75090 представил изменение поведения. Ранее, с Обменом через закрытый Интернет (PIX), когда протокол IPSEC (Internet Protocol Security) (IPSec) прокси не совпадал со Списком контроля доступа (ACL) криптокарты, это продолжило проверять записи далее вниз список. Это включало соответствия с динамической криптокартой без заданного узла.

Это считали уязвимостью, поскольку удаленные администраторы могли получить доступ к ресурсам, которые не предназначал администратор головного узла, когда был настроен статический L2L.

Исправление было создано, который добавил проверку для предотвращения соответствий с элементом криптокарты без узла, когда оно уже проверило элемент схемы, который совпал с узлом. Однако это влияло на сценарий, который обсужден в этом документе. В частности удаленный клиент VPN, который пытается соединиться от адреса партнера (peer) L2L, не в состоянии соединиться с головным узлом.

Настройка

Используйте этот раздел для настройки ASA для разрешения соединения удаленного клиента VPN от адреса партнера (peer) L2L.

Добавьте новую динамическую запись

Для разрешения удаленных VPN-подключений от адресов партнера (peer) L2L необходимо добавить новую динамическую запись, которая содержит тот же IP - адрес адресуемой точки.

> **Примечание:** Необходимо также оставить другую динамическую запись без узла так, чтобы любой клиент из Интернета мог соединиться также.

Вот пример предыдущей действующей конфигурации динамической криптокарты:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Вот конфигурация динамической криптокарты с новой настроенной динамической записью:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.