Устройство шлюза VPN, настроенное как респондент на крипто-согласовании

Содержание

Введение

Этот документ предоставляет сведения о том, как настроить устройство Шлюза VPN, чтобы всегда действовать как респондент на Ike согласование. Устройство ответит на любые крипто-согласования, инициируемые его узлами.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Маршрутизатор Cisco с Выпуском 12.4 (24) T программного обеспечения Cisco IOS и позже
- Устройство адаптивной защиты Cisco (ASA) с версией 7.0 и позже

Родственные продукты

Этот документ может также использоваться с этими версиями программного и аппаратного обеспечения:

- Межсетевой экран Cisco PIX с Версией программного обеспечения 7.0 и позже

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Любое крипто-согласование устраивает две вечеринки для игры ролей Инициатора и Респондента. Инициатор передает крипто-предложения респонденту, который содержит другие параметры о шифровании, алгоритмах аутентификации, повторно вводя опции и пожизненные значения и т.д. Респондент выбирает правильное предложение, и сеанс шифрования устанавливает. Роль, которую играет конечное устройство, может быть просмотрена этими выходными данными команды:

```
Router#show crypto isakmp sa1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no State : MM_ACTIVE ASA(config)#show crypto isakmp sa detailIKE Peer Type Dir Rky State Encrypt Hash Auth Lifetime1 209.165.200.225 User Resp No AM_Active 3des SHA preshrd 86400
```

Преимущества IKE функция режима только для респондента

Так как появление функций виртуальной частной сети (VPN), которые позволяют одновременные двунаправленные Ike согласование (с или без представляющего интерес трафика), проблемы с обработкой и восстановлением данных от двойных SA IKE, произошло. IKE как протокол не имеет никакой способности сравнить Ike согласование, чтобы определить, существует ли уже существующее или незавершенное согласование между двумя узлами, имеющими место. Эти двойные согласования могут быть дорогостоящими с точки зрения ресурсов и путающий администраторам маршрутизатора. Когда устройство будет настроено как устройство только для респондента, оно не будет инициировать IKE, основной, агрессивный, или быстрые режимы (для IKE и установления КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC), и при этом оно не повторно введет IKE и КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC. Поэтому вероятность двойных SA уменьшена.

Другое преимущество этой функции должно позволить управляемую поддержку согласования о соединениях в одном направлении только в распределяющем нагрузку сценарии. Не рекомендуется, чтобы серверы или концентраторы инициировали VPN-подключения к клиентам или лучам, потому что к этим устройствам все обращается одиночно стоящий IP-адрес, как объявлено через балансировщик загрузки. Если бы концентраторы должны были инициировать соединение, они сделали бы настолько использующий адрес отдельного IP, таким образом обойдя преимущества балансировщика загрузки. То же верно для запросов смены ключа, которые получены от концентраторов или серверов позади балансировщика загрузки.

Маршрутизатор, который будет настроен как устройство Только для респондента на крипто-согласовании

Программное обеспечение Cisco IOS версии 12.4(24)T представляет функциональность

маршрутизатора, чтобы всегда ответить на Ike согласование, инициируемые его узлами. Основное ограничение - то, что эта функция конфигурируема только под Профилем IPSEC и относится только к сценарию виртуального интерфейса. Никакая поддержка статического или сценариев динамической криптокарты.

Для настройки маршрутизатора как только для респондента, выполните эти шаги:

```
enable configure terminal crypto ipsec profile <name>   responder-only
```

ASA, который будет настроен как устройство Только для респондента на крипто-согласовании

В общих соединениях IPSec LAN-to-LAN ASA может функционировать как инициатор или респондент. В КЛИЕНТЕ IPSEC К ПОДКЛЮЧЕНИЯМ LAN ASA функционирует только как респондент. ASA может быть настроен как устройство только отвечания в VPN-подключениях LAN-LAN. Однако ограничение - то, что устройство в другом конце VPN-туннеля должно быть одним из них:

- Устройство серии 5500 Cisco ASA
- Концентратор серии Cisco VPN 3000
- Межсетевой экран серии Cisco PIX 500, который выполняет 7.0 программных обеспечений и позже

Для настройки ASA как устройства только для респондента выполните эту команду:

имя хоста (config) # криптокарта mymap 10 установило тип только ответ типа соединения

Примечание: Предложено настроить устройство Шлюза VPN как только для респондента, где множественная VPN взаимодействует оконечный.

Дополнительные сведения

- Конфигурация Router-to-Router LAN-to-LAN туннеля с маршрутизатором, инициирующим агрессивный режим IKE
- Примеры конфигурации Cisco ASA и технические примечания
- Cisco Systems – техническая поддержка и документация