IPsec по Сбоям TCP, когда Трафики через ASA

Содержание

Введение

Клиенты Cisco VPN, которые соединяются с головной станцией VPN с помощью IPsec по TCP, могли бы соединиться с прекрасным головным узлом, но тогда сбои соединения через какое-то время. Этот документ описывает, как коммутировать к IPsec по UDP или собственному компоненту ESP Инкапсуляцию IPSec для решения вопроса.

Перед началом работы

Требования

Для обнаружения с этой определенной проблемой клиенты Cisco VPN должны быть настроены для соединения с устройством головной станции VPN с помощью IPsec по TCP. В большинстве экземпляров администраторы сети настраивают ASA для принятия соединений Cisco VPN Client по Порту TCP 10000.

Используемые компоненты

Сведения в этом документе основываются на Cisco VPN Client.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Проблема

Когда клиент VPN будет настроен для IPsec по TCP (cTCP), ПО Cisco VPN Client не ответит, если двойной ACK TCP будет получен, прося клиент VPN повторно передавать данные. Если существует потеря пакета где-нибудь между клиентом VPN и головным узлом ASA, мог бы генерироваться двойной ACK. Неустойчивая потеря пакета является довольно общей действительностью в Интернете. Однако, так как оконечные точки VPN не используют протокол TCP (вспомните, что они используют cTCP), оконечные точки продолжат передавать, и соединение продолжится.

Если существует другое устройство, такое как межсетевой экран, отслеживающий TCP - подключение с отслеживанием состояния, в этом сценарии происходит проблема. Так как cTCP протокол не полностью внедряет клиента TCP, и ACK копии сервера не получают ответ, это может заставить другие устройства, встроенные с этим сетевым потоком отбрасывать Трафик TCP. Потеря пакета должна произойти в сети, заставляющей сегменты TCP пропасть, который инициирует проблему.

Это не дефект, а побочный эффект и потери пакета в сети и факта, что cTCP не является реальным TCP. cTCP пытается эмулировать протокол TCP путем накрутки Пакетов ipsec в рамках заголовка TCP, но это - степень протокола.

Эта проблема, как правило, происходит, когда администраторы сети внедряют ASA с IPS или делают своего рода контроль приложения на ASA, который заставляет межсетевой экран действовать как полный прокси TCP соединения. Если будет потеря пакета, то ASA будет ACK для недостающих данных от имени cTCP сервера или клиента, но никогда не будет отвечать клиент VPN. Так как ASA никогда не получает данные, которые он ожидает, связь не может продолжиться. В результате сбои соединения.

Решение

Для решения этой проблемы выполните любое из этих действий:

- Коммутатор от IPsec по TCP к IPsec по UDP или собственная инкапсуляция с протоколом ESP.
- Коммутатор клиенту AnyConnect для завершения VPN, которое использует полностью внедренный стек протокола TCP.
- Настройте ASA для применения обхода состояния TCP для них определенный IPSEC/ПОТОКИ TCP. Это по существу отключает все проверки безопасности для соединений, которые совпадают с обходной состоянием TCP политикой, но позволят соединениям работать, пока не может быть внедрено другое разрешение из этого списка. Для получения дополнительной информации обратитесь к Обходу состояния TCP Рекомендации и Ограничения.
- Определите источник потери пакета и примите меры по ликвидации последствий, чтобы препятствовать тому, чтобы IPSEC/ПАКЕТЫ TCP понизился в сети. Это обычно невозможно или чрезвычайно трудно, так как триггер к проблеме обычно является потерей пакета в Интернете, и отбрасывания не могут быть предотвращены.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация