Содержание

Введение

Этот документ описывает одну из наиболее распространенных проблем IPsec, которая является, что Сопоставления безопасности (SA) могут стать из синхронизования между одноранговыми устройствами. В результате устройство шифрования зашифрует трафик с SA, о которых не знает одноранговое утройство шифрования.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Эти сведения в этом документе основываются на тестах, завершенных с Cisco IOS® Release 15.1 (4) M4. Сценарии и конфигурация должны работать с более ранними версиями программного обеспечения Cisco IOS также, так как оба апплета используют версию 3.0 встроенного диспетчера событий (EEM), которая поддерживается в Cisco IOS Release 12.4 (22) T или позже. Однако это не было протестировано.

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.

Условные обозначения

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

Проблема

Пакеты отброшены на узле с этим сообщением, зарегистрированным к системному журналу:

Для получения дальнейшей информации на недопустимых Индексах параметра безопасности (SPI), обратитесь к IPSec %RECVD_PKT_INV_SPI Восстановление Недопустимого SPI и Ошибки. Этот документ описывает, как устранить неполадки сценариев, в которых ошибка происходит периодически, который делает его трудно для сбора необходимых данных для устранения проблем.

Этот тип ошибки не походит на обычное устранение проблем VPN, где можно получить отладки, когда происходит проблема. Для устранения проблем неустойчивых туннельных откидных створок, вызванных недопустимыми SPI, необходимо сначала определить, как эти два головных узла вышли из синхронизования. Так как невозможно предсказать, когда следующий простой произойдет, сценарии EEM являются решением.

Решение

Так как важно знать то, что происходит, прежде чем это сообщение системного журнала инициировано, продолжите выполнять условные отладки на маршрутизаторе (маршрутизаторах) и передавать им к серверу системного журнала так, чтобы это не влияло на рабочий трафик. Если отладки включены в сценарии вместо этого, они генерируются после того, как сообщение системного журнала инициировано, который может не быть полезным. Вот список отладок, что вы могли бы хотеть работать на отправителе этого журнала и получателя:

Сценарий EEM разработан, чтобы сделать две вещи:

1. Выключите отладки на получателе, когда они собраны в течение 18 секунд после того, как генерируется первое сообщение системного журнала. Таймер задержки, возможно, должен был бы модифицироваться, который зависит от суммы генерируемых отладок/журналов.
2. В то же время это отключает отладки, имейте его, передают trap-сообщение SNMP к узлу, который тогда отключает отладки на одноранговом устройстве.

Конфигурация SNMP

Конфигурации Протокола SNMP показывают здесь:

Заключительный сценарий

Сценарии для получателя и отправителя показывают здесь:

Журналы сценариев EEM

Список сообщений журнала сценариев EEM показывают здесь:

Проверка

Чтобы проверить, что проблема была решена, введите **команду show debug**.

```
Receiver:=========hub# show debugSender:=======spoke# show debug
```

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация