IPsec %RECVD_PKT_INV_SPI ошибки и информация о функции восстановления недопустимого SPI

Содержание

Введение

Когда Сопоставления безопасности (SA) становятся из синхронизования между одноранговыми устройствами, этот документ описывает проблему IPsec.

Проблема

Одна из наиболее распространенных проблем IPsec - то, что SA могут стать из синхронизования между одноранговыми устройствами. В результате устройство шифрования шифрует трафик с SA, о которых не знает его узел. Эти пакеты отброшены узлом, и это сообщение появляется в системном журнале:

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet



has invalid spi for destaddr=20.1.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> **Примечание:** С NAT-T правильно не сообщили о сообщениях **RECVD_PKT_INV_SPI** до идентификатора ошибки Cisco был исправлен CSCsq59183. (IPsec не сообщает о сообщениях **RECVD_PKT_INV_SPI** с NAT-T.)

> **Примечание:** На платформе Маршрутизаторов агрегации (ASR) Cisco сообщения **%CRYPTO-4-RECVD_PKT_INV_SPI** не были внедрены до Cisco IOS® XE Release 2.3.2 (12.2 (33) XNC2). Также обратите внимание с платформой ASR, что это определенное отбрасывание зарегистрировано под обоими глобальный счетчик сбросов процессора Quantum Flow (QFP), а также в счетчике сбросов функции IPsec, как показано в следующих примерах.

```
Router# show platform hardware qfp active statistics drop | inc Ipsec
IpsecDenyDrop 0 0
IpsecIkeIndicate 0 0
IpsecInput 0 0 <======
IpsecInvalidSa 0 0
```

```
IpsecOutput 0 0
IpsecTailDrop 0 0
IpsecTedIndicate 0 0Router# show platform hardware qfp active feature ipsec datapath drops all |
in SPI
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Следует отметить, что это конкретное сообщение находится с ограниченной скоростью в Cisco IOS на скорости одной в минуту из очевидных соображений безопасности. Если это сообщение для отдельного потока (SRC, DST или SPI) только появляется однажды в журнале, то это могло бы только быть переменное состояние, которое присутствует в то же время, что и IPsec повторно вводит, где один узел мог бы начать использовать новый SA, в то время как одноранговое устройство не совсем готово использовать тот же SA. Это обычно - не проблема, поскольку это является только временным и только влияло бы на несколько пакетов. Однако были дефекты, где это может быть проблемой.

> **Совет:** Для примеров посмотрите идентификатор ошибки Cisco CSCsl68327 (Потеря пакета во время повторно вводят), идентификатор ошибки Cisco CSCtr14840 (ASR: отбрасывание пакета во время фазы 2 повторно вводит при определенных условиях), или идентификатор ошибки Cisco CSCty30063 (ASR использует новый SPI перед концами QM).

Если несколько экземпляров того же сообщения, как наблюдают, сообщают о том же SPI для того же потока, такого как эти сообщения, Также существует проблема:

```
Router# show platform hardware qfp active feature ipsec datapath drops all | in SPI
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Это - индикация, что трафик помещен в черный список и не мог бы восстановиться, пока SA не истекают на передающем устройстве или пока не активирован Dead Peer Detection (DPD).

Решение

Этот раздел предоставляет сведения, который можно использовать для решения вопроса, который описан в предыдущем разделе.

Восстановление недопустимого SPI

Для решения этого вопроса Cisco рекомендует включить функцию восстановления недопустимого SPI. Например, введите **команду crypto isakmp invalid-spi-recovery**. Вот некоторые важные замечания, которые описывают использование этой команды:

- Во-первых, когда SA вне синхронизования, восстановление недопустимого SPI только служит механизмом восстановления. Это помогает восстанавливаться с этого условия, но это не решает основную проблему, которая заставила SA становиться из синхронизования во-первых. Чтобы лучше понять основную причину, необходимо включить ISAKMP и отладки IPSec на обеих из оконечных точек туннеля. Если проблема часто происходит, то получите отладки и попытку обратиться к основной причине (и не только замаскировать проблему).

- Существует общее несовпадение о цели и функциональности **команды crypto isakmp invalid-spi-recovery**. Даже без этой команды, Cisco IOS уже выполняет тип функциональности восстановления недопустимого SPI, когда это передает УДАЛИТЬ уведомление узлу передачи для SA, который получен, если это уже имеет IKE SA с тем узлом. Снова, это происходит независимо от того, активирована ли **команда crypto isakmp invalid-spi-recovery**.

- **Команда crypto isakmp invalid-spi-recovery** пытается обратиться к условию, где маршрутизатор получает Трафик IPSec с недопустимым SPI, и это не имеет IKE SA с тем узлом. В этом случае это пытается установить новый сеанс IKE с узлом и передает УДАЛИТЬ уведомление по недавно созданной IKE SA. Однако эта команда не функционирует для всех крипт - настроек. Единственные конфигурации, для которых работает эта команда, являются статическими криптокартами, где узел явно определен и статические одноранговые узлы, которые получены из инстанцированных криптокарт, таких как VTI. Вот сводка обычно используемых крипт - настроек и работает ли восстановление недопустимого SPI с той конфигурацией:

Крипто - настройка	Восстановление Недопустимо SPI?
Статическая криптокарта	Да
!--- динамическую карту шифрования	Нет
GRE P2P с TP	Да
TP mGRE, который использует w/статический NHRP - маршрутизацию	Да
TP mGRE, который использует w/динамический NHRP - маршрутизацию	Нет
sVTI	Да
Клиент EzVPN	Н/Д

Устраните неполадки неустойчивых сообщений об ошибках недопустимого SPI

Много раз сообщение об ошибках недопустимого SPI происходит периодически. Это мешает устранять неполадки, поскольку становится очень трудно собрать соответствующие отладки. Сценарии встроенного диспетчера событий (EEM) могут быть очень полезными в этом случае.

> **Примечание:** Для получения дополнительной информации обратитесь к Сценариям EEM, используемым для Устранения проблем Туннельных Откидных створок, Вызванных Недопустимым Документом Cisco Индексов параметра безопасности.