Системный журнал "%CRYPTO-4-RECVD_PKT_MAC_ERR": сообщение об ошибках с потерей эхо-запроса по устранению проблем туннеля IPSec

Содержание

Введение

Этот документ описывает, как решить потерю эхо-запроса по Туннелю IPSec вместе с сообщениями "%CRYPTO-4-RECVD_PKT_MAC_ERR" в системном журнале как показано в коробке:

```
May 23 11:41:38.139 GMT: %CRYPTO-4-RECVD_PKT_MAC_ERR:
decrypt: mac verify failed for connection
id=2989 local=172.16.200.18 remote=172.16.204.18 spi=999CD43B
seqno=00071328
```

Небольшой процент таких отбрасываний считают обычным. Однако высокий уровень сброса из-за этой проблемы может повлиять на сервис и мог бы потребовать внимания оператора сети. Обратите внимание на то, что эти сообщения, о которых сообщают в системных журналах, являются скоростью, ограниченной в 30-секундных интервалах, таким образом, одиночное сообщение журнала не всегда указывает, что был отброшен только один пакет. Для получения точного количества этих отбрасываний выполните **подробность команды show crypto ipsec sa** и посмотрите на SA рядом с идентификатором соединения, замеченным в журналах. Среди счетчиков SA **pkts проверяет, что подведенный** счетчик ошибок составляет отбрасывание общего пакета из-за сбоя проверки кода аутентификации сообщения (MAC).

```
interface: GigabitEthernet0/1
Crypto map tag: MPLSWanGREVPN, local addr 172.16.204.18

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.204.18/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (172.16.205.18/255.255.255.255/47/0)
current_peer 172.16.205.18 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 51810, #pkts encrypt: 51810, #pkts digest: 51810
#pkts decaps: 44468, #pkts decrypt: 44468, #pkts verify: 44468
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 8
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.204.18, remote crypto endpt.: 172.16.205.18
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0xD660992C(3596654892)

inbound esp sas:
spi: 0x999CD43B(2577191995)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2989, flow_id: AIM-VPN/SSL-3:2989, sibling_flags 80000006,
crypto map: MPLSWanGREVPN
sa timing: remaining key lifetime (k/sec): (4257518/24564)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound esp sas:
spi: 0xD660992C(3596654892)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2990, flow_id: AIM-VPN/SSL-3:2990, sibling_flags 80000006,
crypto map: MPLSWanGREVPN
sa timing: remaining key lifetime (k/sec): (4199729/24564)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE
```

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на тестах, сделанных с Cisco IOS® Release 15.1 (4) M4. Несмотря на то, что еще не протестированный, сценарии и конфигурация должны работать с более ранними версиями программного обеспечения Cisco IOS также, так как оба апплета используют версию 3.0 EEM (который поддерживается в версии IOS 12.4 (22) T или выше).

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.

Информация о функциональной возможности

"%CRYPTO-4-RECVD_PKT_MAC_ERR: дешифруйте": подразумевает, что зашифрованный пакет был получен, который отказал проверку MAC. Эта проверка является результатом опознавательного настроенного набора преобразований:

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

В вышеупомянутом примере, *"aes ESP 256"* определяет алгоритм шифрования как 256-разрядный AES, и *"md5 ESP"* определяет MD5 (вариант HMAC) как алгоритм хэширования, используемый для аутентификации. Алгоритмы хэширования как MD5, как правило, используются для обеспечения цифрового отпечатка содержания файла. digitial отпечаток пальца часто используется, чтобы гарантировать, что файл не был изменен злоумышленником или вирусом. Таким образом возникновение этого сообщения об ошибках обычно подразумевает также:

- Неправильный ключ использовался, чтобы зашифровать или дешифровать пакет. Эта ошибка очень редка и могла быть вызвана ошибкой в программном обеспечении.

  или-
- В пакет вмешались во время транзита. Эта ошибка могла произойти из-за грязного канала или враждебного события.

Методика устранения проблем

Так как это сообщение об ошибках, как правило, вызывается порчей пакетов, единственный способ сделать, анализ корневых причин должен использовать EPC для получения перехватов полного пакета из Стороны WAN на обеих оконечных точках туннеля и сравнить их. Перед получением перехватов лучше определять, какой трафик инициирует эти журналы. В некоторых случаях это может быть определенный вид трафика; в других случаях это могло бы быть случайно, но легко воспроизведенное (такие как 5-7 отбрасываний каждые 100 эхо-запросов). В таких ситуациях проблема становится немного легче определить. Лучший способ определить триггер состоит в том, чтобы отметить тестовый поток данных маркировками DSCP и перехватывать пакеты. DSCP-значение скопировано к заголовку ESP и может тогда фильтроваться с Wireshark. Эта конфигурация, которая принимает тест с 100 эхо-запросами, может использоваться для маркировки пакетов ICMP:

```
ip access-list extended VPN_TRAFFIC
 permit icmp <source> <destination>
class-map match-all MARK
 match access-group name VPN_TRAFFIC
policy-map MARKING
 class MARK
  set dscp af21
```

Эта политика должна теперь быть применена к входному интерфейсу, где ясный трафик получен на маршрутизаторе шифрования:

```
interface GigabitEthernet0/0
service-policy MARKING in
```

Также вы могли бы хотеть запустить этот тест с генерируемым маршрутизатором трафиком. Для этого вы не в состоянии использовать Качество обслуживания (QoS) для маркировки пакетов, но вы можете Use Policy-Based Routing (PBR).

> **Примечание:** Для определения местоположения важный (5) маркировки DSCP, используйте фильтр Wireshark **ip.dsfield.dscp == 0x28**.

```
ip access-list extended VPN_TRAFFIC
 permit icmp <source> <destination>
route-map markicmp permit 10
match ip address vpn
set ip precedence critical
ip local policy route-map markicmp
```

Как только маркировка QoS настроена для вашего трафика ICMP, можно настроить встроенный захват пакета:

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host <local> <peer>
Router(config)# permit ip host <peer> <local>
Router(config)# exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

Примечание: эта функция была представлена в Cisco IOS Release 12.4 (20) T. См. Встроенный Захват пакета для получения дополнительной информации относительно EPC.

Использование захвата пакета для устранения проблем этого типа ошибки требует, чтобы целый пакет был перехвачен, не только часть его. Функция EPC в Cisco IOS Release до 15.0 (1) M имеет предельную емкость буфера 512K и предел максимального размера пакета 1024 байтов. Во избежание этого ограничения обновите к 15.0 (1) M или более новый код, который теперь поддерживает размер накопительного буфера 100M с максимальным размером пакета 9500 байтов.

Если проблема может быть надежно воспроизведена с каждыми 100 эхо-запросами количества, самый неблагоприятный сценарий должен планировать период технического обслуживания, чтобы позволить только трафик эхо-тестирования как управляемый тест и взять перехваты. Этот процесс должен занять только несколько минут, но он действительно разрушает рабочий трафик в течение того времени. При использовании маркировки QoS можно устранить требование для ограничения пакетов только эхо-запросами. Для получения всех ping - пакетов в одном буфере необходимо гарантировать, что тест не проводится в течение часов пик.

Если проблема легко не воспроизведена, можно использовать сценарий EEM для автоматизации захвата пакета. Теория состоит в том, что вы запускаете перехваты с обеих сторон в кольцевой буфер и используете EEM для остановки перехвата на одной стороне. В то же время EEM останавливает перехват, имейте его, передают trap-сообщение snmp к узлу, который останавливает его перехват. Этот процесс мог бы работать. Но если загрузка тяжела, второй маршрутизатор не мог бы реагировать достаточно быстро для остановки его перехвата. Предпочтен управляемый тест. Вот сценарии EEM, которые внедрят процесс:

```
Receiver
========
event manager applet detect_bad_packet
event syslog pattern "RECVD_PKT_MAC_ERR"
action 1.0 cli command "enable"
action 2.0 cli command "monitor capture point stop test"
action 3.0 syslog msg "Packet corruption detected and capture stopped!"
action 4.0 snmp-trap intdata1 123456 strdata ""

 Sender
======
event manager applet detect_bad_packet
event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.2.3.1.9.
oid-val "123456" op eq src-ip-address 20.1.1.1
action 1.0 cli command "enable"
action 2.0 cli command "monitor capture point stop test"
action 3.0 syslog msg "Packet corruption detected and capture stopped!"
```

Обратите внимание на то, что код в предыдущей коробке является конфигурацией, протестированной с 15.0 (1) M. Вы могли бы хотеть протестировать его с определенной версией Cisco IOS ваше использование клиента перед реализацией его в пользовательском окружении.

Анализ данных

1. Как только перехваты были завершены, используйте TFTP для экспортирования их в ПК.
2. Откройте перехваты с сетевым протоколом анализатор (такие как Wireshark).
3. Если маркировка QoS использовалась, отфильтруйте соответствующие пакеты.
   `ip.dsfield.dscp==0x08`
   "0x08" является определенным для AF21 DSCP-значения. Если другое DSCP-значение используется, правильное значение может быть получено из самого захвата пакета или из списка схемы преобразования DSCP-значений. См. DSCP и Значения приоритета для получения дополнительной информации.
4. Определите отброшенный эхо-запрос на перехватах от отправителя и найдите тот пакет на перехватах и на стороне получателя и на стороне отправителя.
5. Экспортируйте тот пакет от обоих перехватов как показано в этом образе:
6. Проведите двоичное сравнение двух. Если они идентичны, то не было никаких ошибок в пути и Cisco IOS или не бросили ложного отрицательного на принимающую сторону или использовали несправедливость, включают конец отправителя. В любом случае проблема является дефектом Cisco IOS. Если пакеты являются другими, то в пакеты вмешались в передаче.

   Вот пакет, поскольку он оставил ядро шифрования на FC:

```
*Mar  1 00:01:38.923: After encryption:
05F032D0: 45000088 00000000 E.......
05F032E0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a.
05F032F0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z.$
05F03300: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
05F03310: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
05F03320: 09CE001B 70CC56AB 746D6A3A 63C2652B .N..pLV+tmj:cBe+
05F03330: 1992E8AF 2CE2A279 46367BDB 660854ED ..h/,b"yF6{[f.Tm
05F03340: 77B69453 83E47778 1470021F 09436285 w6.S.dwx.p...Cb.
05F03350: CB94AEF5 20A65B1F 480D86F6 125BA12E K..u &[.H..v.[!.
```

Вот тот же пакет, как он был получен на узле:

```
4F402C90:                   45000088 00000000          E.......
4F402CA0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a.
4F402CB0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z.$
4F402CC0: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
4F402CD0: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
4F402CE0: 09CE001B 70CC56AB 00000000 00000000 .N..pLV+........
4F402CF0: 00000000 00000000 00000000 00000000 ................
4F402D00: 00000000 00000000 00000000 00000000 ................
4F402D10: 00000000 00000000 00000000 00000000 ................
```

На этом этапе это наиболее вероятно проблема интернет-провайдера, и та группа должна быть вовлечена в устранение проблем.

Типичные неполадки

- CSCed87408 идентификатора ошибки Cisco описывает проблему аппаратных средств с ядром шифрования на 83xs, где случайные исходящие пакеты повреждены во время шифрования, которое приводит к ошибкам аутентификации (в случаях, где аутентификация используется), и отбрасывание пакета на принимающей стороне. Важно понять, что вы не будете видеть эти ошибки на 83x само, но на принимающем устройстве.

- Иногда маршрутизаторы, которые выполняют старый код, показывают эту ошибку. Можно обновить к более свежим версиям кода такой как 15.1 (4) M4 для решения вопроса.

- Чтобы проверить, является ли проблемой проблема программного или аппаратного обеспечения, отключите аппаратное шифрование. Если сообщения журнала продолжаются, это - проблема программного обеспечения. В противном случае тогда RMA должен решить проблему.
  Помните, что при отключении аппаратного шифрования оно может вызвать серьезное снижение производительности сети для в большой степени загруженных VPN-туннелей. Поэтому Cisco рекомендует делать попытку процедур, описанных в этом документе во время периода технического обслуживания.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация