Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" IPsec 터널을 통한 Ping 손실과 관련된 오류 메시지 문제 해결

목차

소개

이 문서에서는 다음 상자에 표시된 것처럼 syslog의 "%CRYPTO-4-RECVD_PKT_MAC_ERR" 메시지와 함께 IPsec 터널을 통한 ping 손실을 해결하는 방법에 대해 설명합니다.

```
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
```

그러한 하락의 적은 비율은 정상이라고 여겨진다.그러나 이 문제로 인해 높은 하락률이 서비스에 영향을 미칠 수 있으며 네트워크 운영자의 주의가 필요할 수 있습니다.syslog에 보고된 이러한 메시지는 30초 간격으로 제한되므로 단일 로그 메시지가 단일 패킷만 삭제되었음을 나타내는 것은 아닙니다.이러한 삭제의 정확한 수를 얻으려면 **show crypto ipsec sa detail** 명령을 실행하고 로그에 표시된 연결 ID 옆에 있는 SA를 확인합니다.SA 카운터 중에서 **pkts verify failed error counter accounts for the total packet drop** drop drop drop drop drop drop은 MAC(메시지 인증 코드) 확인 실패로 인해 발생합니다.

```
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
```

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® Release 15.1(4)M4에서 수행한 테스트를 기반으로 합니다. 아직 테스트되지 않았지만, 스크립트와 구성은 이전 Cisco IOS 소프트웨어 버전에서도 작동해야 합니다. 두 애플릿이 모두 EEM 버전 3.0(IOS 버전 12.4(22)T 이상에서 지원됨)을 사용하기 때문입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기능 정보

"%CRYPTO-4-RECVD_PKT_MAC_ERR:decrypt:"는 MAC 확인에 실패한 암호화된 패킷을 수신했음을 의미합니다.이 확인은 구성된 인증 변형 집합의 결과입니다.

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

위의 예에서 *"esp-aes 256"은* 암호화 알고리즘을 256비트 AES로 정의하고 *"esp-md5"*는 MD5(HMAC 변형)를 인증에 사용되는 해시 알고리즘으로 정의합니다.MD5와 같은 해시 알고리즘은 일반적으로 파일 내용의 디지털 핑거프린트를 제공하는 데 사용됩니다.디지털 핑거프린트는 침입자나 바이러스에 의해 파일이 변경되지 않도록 하는 데 자주 사용됩니다.따라서 이 오류 메시지가 나타나면 일반적으로 다음 중 하나를 의미합니다.

- 패킷을 암호화하거나 해독하는 데 잘못된 키를 사용했습니다.이 오류는 매우 드물며 소프트웨어 버그로 인해 발생할 수 있습니다.

-또는-

- 전송 중에 패킷이 변경되었습니다.이 오류는 더티 회선 또는 적대적인 이벤트 때문일 수 있습니다.

문제 해결 방법론

이 오류 메시지는 일반적으로 패킷 손상으로 인해 발생하므로 근본 원인 분석을 수행하는 유일한 방법은 EPC를 사용하여 양쪽 터널 엔드포인트의 WAN 측에서 완전한 패킷 캡처를 얻고 이를 비교하는 것입니다.캡처를 얻기 전에 이러한 로그를 트리거하는 트래픽 종류를 확인하는 것이 좋습니다.경우에 따라 특정 종류의 트래픽일 수 있습니다.다른 경우에는 무작위적이지만 쉽게 복제할 수 있습니다(예: 100ppings마다 5-7회 삭제). 이러한 상황에서 문제를 식별하기가 다소 쉬워집니다.트리거를 식별하는 가장 좋은 방법은 테스트 트래픽을 DSCP 표시로 표시하고 패킷을 캡처하는 것입니다.DSCP 값은 ESP 헤더에 복사되고 Wireshark를 사용하여 필터링할 수 있습니다.테스트를 100개의 ping으로 간주하는 이 컨피그레이션은 ICMP 패킷을 표시하는 데 사용할 수 있습니다.

```
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
```

이제 이 정책을 암호화 라우터에서 일반 트래픽을 수신하는 인그레스 인터페이스에 적용해야 합니다.

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

또는 라우터에서 생성된 트래픽으로 이 테스트를 실행할 수도 있습니다.이를 위해 QoS(Quality of Service)를 사용하여 패킷을 표시할 수는 없지만 PBR(Policy-Based Routing)을 사용할 수 있습니다.

> **참고:**Critical (5) DSCP 표시를 찾으려면 Wireshark 필터 **ip.dsfield.dscp == 0x28을** 사용합니다.

```
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
```

ICMP 트래픽에 대해 QoS 마킹이 구성되면 포함된 패킷 캡처를 구성할 수 있습니다.

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host
```

```
Router(config)# permit ip host
```

```
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"
```

참고:이 기능은 Cisco IOS Release 12.4(20)T에서 도입되었습니다.EPC에 대한 자세한 내용은 임베디드 패킷 캡처를 참조하십시오.

이 유형의 문제를 해결하기 위해 패킷 캡처를 사용하려면 전체 패킷을 캡처해야 하며 일부만 캡처해야 합니다.15.0(1)M 이전 Cisco IOS 릴리스의 EPC 기능은 버퍼 제한 512K와 최대 패킷 크기 제한 1024바이트를 가집니다.이러한 제한을 방지하려면 15.0(1)M 이상의 코드로 업그레이드하십시오. 이 코드는 최대 패킷 크기가 9500바이트인 100M인 캡처 버퍼 크기를 지원합니다.

100개의 카운트 ping을 실행할 때마다 이 문제를 안정적으로 재현할 수 있는 경우, 최악의 시나리오는 Ping 트래픽만 제어된 테스트로 허용하고 캡처를 수행하도록 유지 관리 기간을 예약하는 것입니다.이 프로세스는 단 몇 분 정도 걸릴 수 있지만 그 시간 동안 운영 트래픽이 중단됩니다.QoS 마킹을 사용하는 경우 패킷만 ping으로 제한하는 요건을 제거할 수 있습니다.하나의 버퍼에서 모든 ping 패킷을 캡처하려면 피크 시간 동안 테스트가 수행되지 않는지 확인해야 합니다.

문제가 쉽게 재현되지 않을 경우 EEM 스크립트를 사용하여 패킷 캡처를 자동화할 수 있습니다.따라서 양쪽의 캡처를 순환 버퍼로 시작하고 EEM을 사용하여 한 쪽의 캡처를 중지할 수 있습니다.동시에 EEM은 캡처를 중지하고 SNMP 트랩을 피어로 전송하도록 하여 캡처를 중지합니다.이 프로세스가 작동할 수 있습니다.그러나 로드가 많으면 두 번째 라우터가 캡처를 중지할 만큼 빠르게 반응하지 못할 수 있습니다.제어된 테스트가 선호됩니다.프로세스를 구현할 EEM 스크립트는 다음과 같습니다.

```
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!"
```

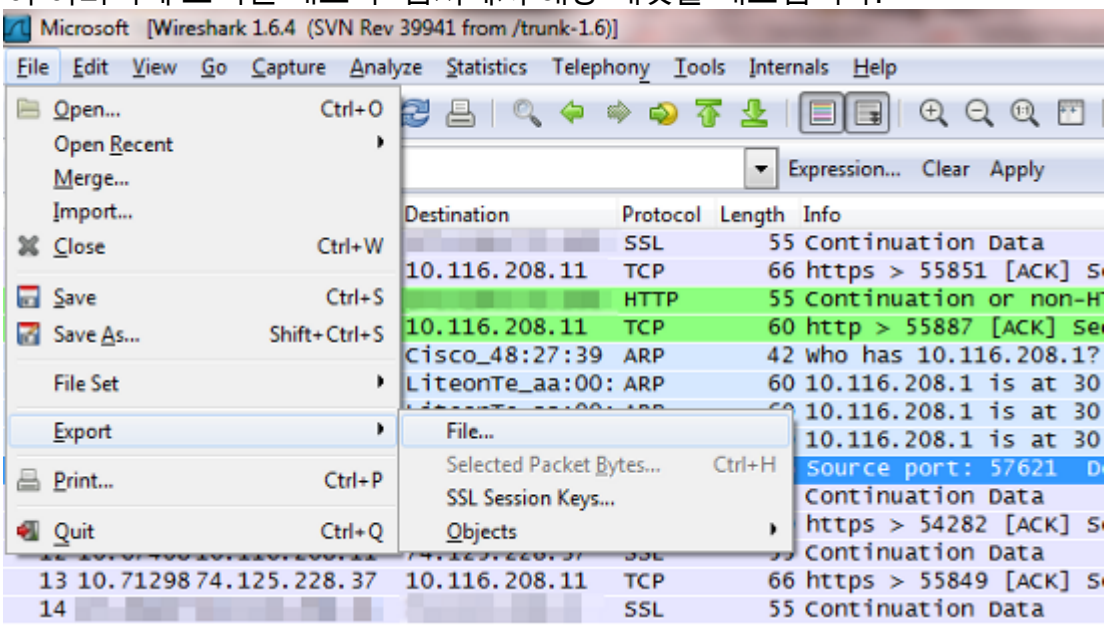
이전 상자의 코드는 15.0(1)M에서 테스트한 컨피그레이션입니다.고객 환경에서 구현하기 전에 고객이 사용하는 특정 Cisco IOS 버전으로 테스트할 수 있습니다.

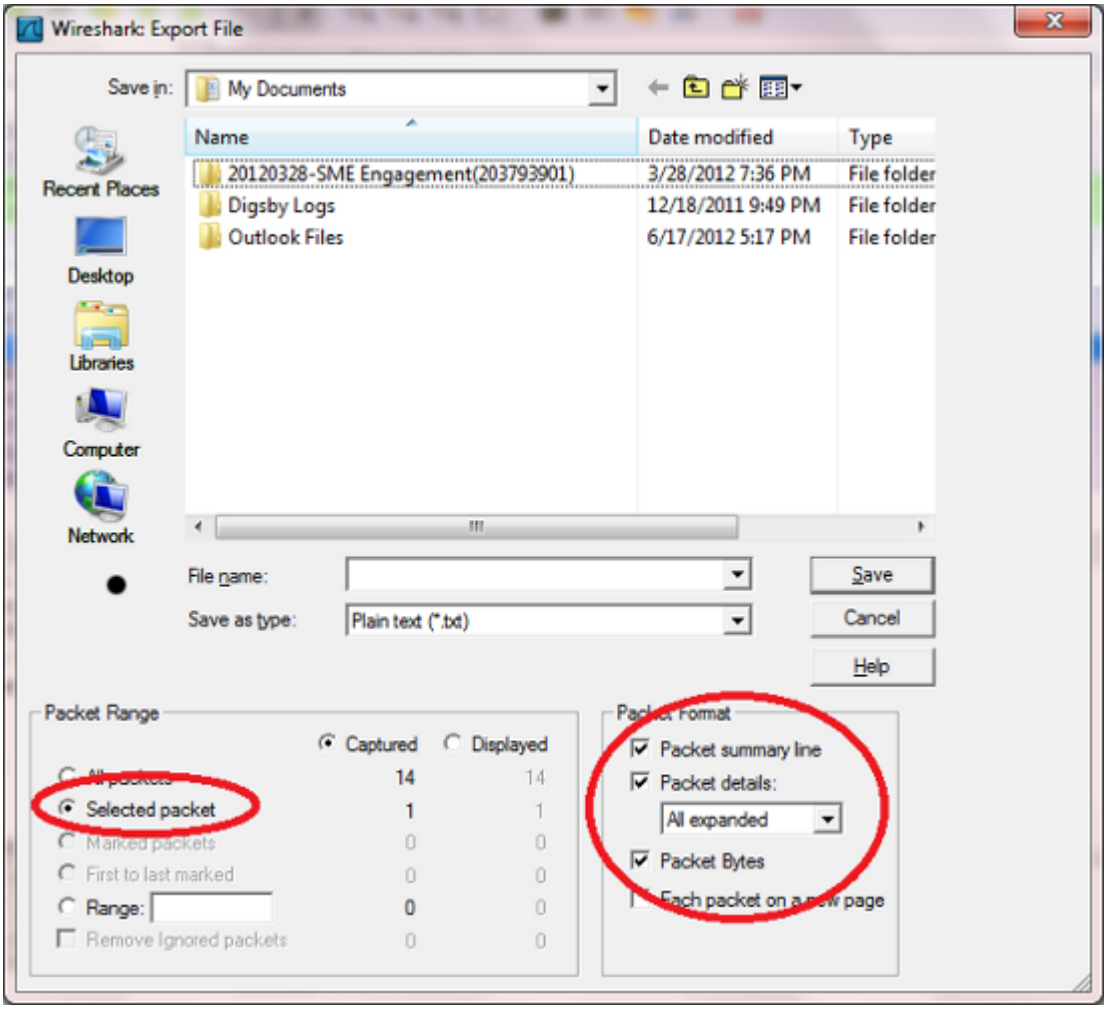
데이터 분석

1. 캡처가 완료되면 TFTP를 사용하여 PC로 내보냅니다.
2. 네트워크 프로토콜 분석기(예: Wireshark)를 사용하여 캡처를 엽니다.
3. QoS 마킹을 사용한 경우 해당 패킷을 필터링합니다.

   ```
   ip.dsfield.dscp==0x08
   ```

   "0x08"은 DSCP 값 AF21에 대해 고유합니다. 다른 DSCP 값을 사용하는 경우 패킷 캡처 자체 또는 DSCP 값 변환 차트 목록에서 올바른 값을 가져올 수 있습니다.자세한 내용은 DSCP 및 우선 순위 값을 참조하십시오.
4. 발신자로부터 캡처에 대해 삭제된 ping을 식별하고, 수신자측과 발신자측 모두에서 캡처에서 해당 패킷을 찾습니다.
5. 이 이미지에 표시된 대로 두 캡처에서 해당 패킷을 내보냅니다.





6. 두 가지를 이진 비교로 수행합니다. 동일한 경우 전송 중에 오류가 없고 Cisco IOS가 수신 끝에 오탐을 던지거나 발신자 끝에 잘못된 키를 사용했습니다.두 경우 모두 Cisco IOS 버그로 문제가 발생합니다. 패킷이 다른 경우 전송 시 패킷이 변조되었습니다.

   다음은 FC에서 암호화 엔진을 떠난 패킷입니다.

```
*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.[!.
```

   다음은 피어에서 수신한 패킷과 동일합니다.

```
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 ................
```

이 시점에서는 ISP 문제일 가능성이 높으며 해당 그룹이 문제 해결에 관여해야 합니다.

일반적인 문제

- Cisco 버그 ID CSCed87408은 암호화 중에 임의의 발신 패킷이 손상된 83xs의 암호화 엔진의 하드웨어 문제를 설명하며, 이로 인해 인증 오류(인증이 사용되는 경우) 및 수신 끝의 패킷이 삭제됩니다.이 오류는 83x 자체뿐 아니라 수신 장치에서도 볼 수 있다는 점을 인식하는 것이 중요합니다.

- 이전 코드를 실행하는 라우터에 이 오류가 표시되는 경우가 있습니다.15.1(4) M4와 같은 최신 코드 버전으로 업그레이드하여 문제를 해결할 수 있습니다.

- 문제가 하드웨어 또는 소프트웨어 문제인지 확인하려면 하드웨어 암호화를 비활성화합니다.로그 메시지가 계속 표시되면 소프트웨어 문제입니다.그렇지 않은 경우 RMA에서 문제를 해결해야 합니다.
  하드웨어 암호화를 비활성화하면 로드가 많은 VPN 터널에 심각한 네트워크 저하가 발생할 수 있습니다.따라서 유지 보수 기간 동안 이 문서에 설명된 절차를 시도할 것을 권장합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems