Standaard "%CRYPTO-4-RECVD_PKT_MAC_ERR:" foutmelding met Ping Loss over IPsec tunnelprobleemoplossing

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Functieinformatie
Methode voor probleemoplossing
Gegevensanalyse
Vaak voorkomende problemen
Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u ping-verlies via een IPsec-tunnel kunt oplossen in combinatie met "%CRYPTO-4-RECVD_PKT_MAC_ERR"-berichten in het systeem zoals in het vakje weergegeven:

```
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
```

Een klein percentage van deze druppels wordt als normaal beschouwd. Een hoge daling vanwege dit probleem kan echter gevolgen hebben voor de dienstverlening en kan de aandacht van de netwerkexploitant vereisen. Merk op dat deze berichten die in de syslogs worden gemeld, met tussenpozen van 30 seconden relatief beperkt zijn, dus één logbericht geeft niet altijd aan dat er slechts één pakje is gevallen. Om een nauwkeurige telling van deze druppels te verkrijgen, geef de opdracht de **crypto ipsec als detail** uit, en kijk naar de SA naast de verbinding-ID in de logs. Onder de SA tellers, **verifiëren pkts mislukte** fout teller rekeningen voor de totale pakketdaling wegens de van de berichtauthenticatie code (MAC) controle mislukte.

```
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
```

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op testen die uitgevoerd zijn met Cisco IOS® release 15.1(4)M4. Hoewel nog niet getest, moeten de scripts en configuratie ook werken met eerdere Cisco IOS-softwareversies, omdat beide applets EEM versie 3.0 gebruiken (die ondersteund wordt in IOS versie 12.4(22)T of hoger).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Functieinformatie

De "%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt:" impliceert dat een versleuteld pakket werd ontvangen dat de MAC-verificatie niet had uitgevoerd. Deze verificatie is een resultaat van de reeks van de authenticatie die is ingesteld:

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

In het bovenstaande voorbeeld definieert *"esp-aes 256"* het encryptiealgoritme als 256-bits AES, en *"esp-md5"* definieert de MD5 (HMAC-variant) als het hashalgoritme dat gebruikt wordt voor verificatie. Hash-algoritmen zoals MD5 worden normaal gebruikt om een digitale vingerafdruk van de inhoud van een bestand te geven. De digitale vingerafdruk wordt vaak gebruikt om er zeker van te zijn dat het bestand niet door een indringer of virus is gewijzigd. Het optreden van deze foutmelding impliceert dus gewoonlijk:

- De verkeerde toets werd gebruikt om het pakket te versleutelen of decrypteren. Deze fout is zeer zeldzaam en kan worden veroorzaakt door een softwarebug.

-OF-

- Tijdens het vervoer is met de pakje geknoeid. Deze fout kan het gevolg zijn van een vuil circuit of een vijandig voorval.

Methode voor probleemoplossing

Aangezien deze foutmelding doorgaans wordt veroorzaakt door pakketcorruptie, is de enige manier om een basisanalyse te doen EPC te gebruiken om volledige pakketvastlegging van de kant van WAN op beide tunneleindpunten te verkrijgen en deze te vergelijken. Voordat u de Captures verkrijgt, is het het best om te identificeren wat voor soort verkeer deze logs in gang zet. In sommige gevallen kan het om een specifiek soort verkeer gaan; In andere gevallen kan het willekeurig zijn, maar gemakkelijk reproduceren (zoals 5-7 druppels elke 100 pings). In zulke situaties wordt het probleem iets makkelijker te identificeren. De beste manier om de trigger te identificeren is het testverkeer te markeren met DSCP-markeringen en de pakketten op te nemen. De DSCP-waarde wordt naar de ESP-header gekopieerd en kan vervolgens worden gefilterd met Wireshark. Deze configuratie, waarbij wordt uitgegaan van een test met 100 pings, kan worden gebruikt om de ICMP-pakketten te markeren:

```
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
```

Dit beleid moet nu worden toegepast op de ingangsinterface waar het duidelijke verkeer op de versleutelde router wordt ontvangen:

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

In plaats hiervan kunt u deze test ook uitvoeren met door de router gegenereerd verkeer. Hiervoor kunt u Quality of Service (QoS) niet gebruiken om de pakketten te markeren, maar u kunt op

beleid gebaseerde routing (PBR) gebruiken.

> Opmerking: Om kritieke (5) DSCP-markeringen te vinden, gebruikt u het filter 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
```

Nadat QoS-markering is ingesteld voor uw ICMP-verkeer, kunt u de ingesloten pakketvastlegging configureren:

```
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"
```

Opmerking: deze optie is geïntroduceerd in Cisco IOS release 12.4(20)T. Raadpleeg Ingesloten pakketvastlegging voor meer informatie over EPC's.

Het gebruik van een pakketvastlegging om problemen op te lossen van dit type probleem vereist dat het gehele pakket wordt opgenomen, en niet slechts een deel ervan. De EPC optie in Cisco IOS-releases vóór 15.0(1)M heeft een bufferlimiet van 512K en een max. pakketgrootte van 1024 bytes. Om deze beperking te voorkomen, moet u een upgrade uitvoeren naar 15.0(1)M of een nieuwere code, die nu een opnamefaberusgrootte van 100M ondersteunt met een maximale pakketgrootte van 9500 bytes.

Als de kwestie op betrouwbare wijze kan worden gereproduceerd met elke 100 teller ping, is het slechtst denkbare scenario om een onderhoudsvenster te plannen zodat alleen het pingverkeer als gecontroleerde test kan worden uitgevoerd en de opnamen kunnen nemen. Dit proces zou slechts een paar minuten in beslag moeten nemen, maar het verstoort het productieverkeer destijds. Als u QoS-markering gebruikt, kunt u de eis elimineren om pakketten alleen tot pings te beperken. Om alle ping-pakketten in één buffer op te nemen moet u ervoor zorgen dat de test niet tijdens piekuren wordt uitgevoerd.

Als de kwestie niet gemakkelijk reproduceerd is, kunt u een EEM script gebruiken om de pakketvastlegging te automatiseren. De theorie is dat je aan beide kanten de opname in een circulaire buffer start en EEM gebruikt om de opname aan één kant tegen te gaan. Tegelijkertijd stopt het EEM de opname, laat het een snmp-val naar de peer sturen, die de opname ervan stopt. Dit proces zou kunnen werken. Maar als de lading zwaar is, zou de tweede router niet snel genoeg kunnen reageren om de opname te stoppen. Een gecontroleerde test verdient de voorkeur. Dit zijn de EEM scripts die het proces zullen uitvoeren:

```
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!"
```

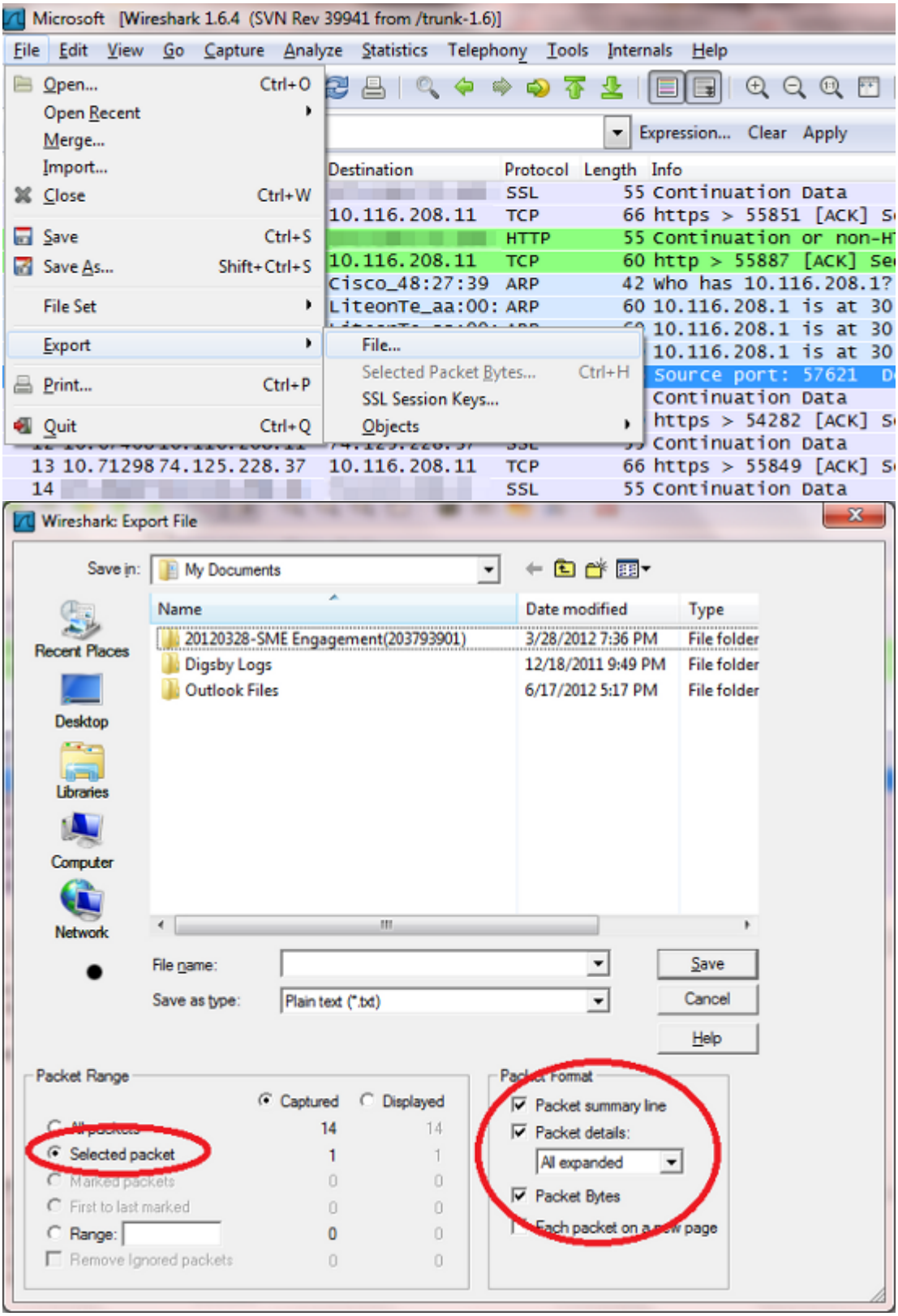
Merk op dat de code in het vorige vak een configuratie is die is getest met 15.0(1)M. U kunt het met de specifieke Cisco IOS versie willen testen uw klant gebruikt voordat u het in de klantomgeving implementeert.

Gegevensanalyse

1. Nadat de opnamen zijn voltooid, gebruikt u TFTP om ze naar een pc te exporteren.
2. Open de Captures met een netwerkprotocolanalyzer (zoals Wireshark).
3. Als u een QoS-markering hebt gebruikt, verwijdert u de betreffende pakketten.

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

   "0x08" is specifiek voor de DSCP-waarde AF21. Als een andere DSCP-waarde wordt gebruikt, kan de juiste waarde worden verkregen uit de pakketvastlegging zelf of uit de lijst met DSCP-waarden conversievenster. Raadpleeg DSCP- en prioriteitswaarden voor meer informatie.
4. Identificeer het laten vallen op de opnamen van de afzender, en plaats dat pakket op opnamen op zowel de ontvangstkant als de afzender.
5. Exporteren dat pakket van beide opnamen is zoals in deze afbeelding:



6. Gedraag een binaire vergelijking van de twee. Als ze identiek zijn, dan waren er geen fouten in doorvoer en Cisco IOS gooide een valse negatief op het ontvangende eind of gebruikte de verkeerde sleutel op het afzender eind. In beide gevallen is het probleem een Cisco IOS bug. Als de pakketten verschillend zijn, werden de pakketten geknoeid met in transport.

   Hier is het pakje toen de crypto-motor op de FC werd achtergelaten:

```
*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.[!.
```

Dit is hetzelfde pakket als het op de peer werd ontvangen:

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

Op dit punt is het zeer waarschijnlijk een ISP-probleem en moet die groep bij de probleemoplossing betrokken zijn.

Vaak voorkomende problemen

- Cisco bug-ID CSCed87408 beschrijft een hardwareprobleem met de encryptiemachine op de 83xs waar willekeurige uitgaande pakketten tijdens de encryptie beschadigd worden, wat leidt tot verificatiefouten (in gevallen waarin verificatie wordt gebruikt) en pakketdalingen aan het ontvangende einde. Het is belangrijk om te realiseren dat u deze fouten niet op de 83x zelf ziet, maar op het ontvangende apparaat.

- Soms tonen routers die oude code uitvoeren deze fout. U kunt upgraden naar de recentere codeversies zoals 15.1(4) M4 om het probleem op te lossen.

- Om te verifiëren of het probleem een hardware- of softwareprobleem is, schakelt u hardwareencryptie uit. Als de logberichten doorgaan, is dit een softwareprobleem. Als dat niet het geval is, moet een RMA het probleem oplossen.
  Onthoud dat als u hardwareencryptie uitschakelt, dit ernstige netwerkdegradatie kan veroorzaken voor zwaar geladen VPN-tunnels. Daarom raadt Cisco u aan de procedures te proberen die in dit document worden beschreven tijdens een onderhoudsvenster.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems