Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" Fehlermeldung mit Ping Loss Over IPsec Tunnel Troubleshooting

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Ping-Verluste über einen IPsec-Tunnel in Verbindung mit "%CRYPTO-4-RECVD_PKT_MAC_ERR"-Meldungen im Syslog wie im Feld gezeigt behoben werden:

```
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
```

Ein kleiner Prozentsatz dieser Tropfen gilt als normal. Eine hohe Fallrate kann sich jedoch auf den Service auswirken und die Aufmerksamkeit des Netzwerkbetreibers erfordern. Beachten Sie, dass diese Meldungen in den Syslogs in Intervallen von 30 Sekunden begrenzt sind, sodass eine einzige Protokollmeldung nicht immer darauf hinweist, dass nur ein Paket verworfen wurde. Um eine genaue Anzahl dieser Verwerfen zu erhalten, führen Sie den Befehl **show crypto ipsec as detail aus**, und sehen Sie sich die SA neben der in den Protokollen angezeigten Verbindungs-ID an. Unter den SA-Zählern **überprüfen** die **Pkte die** Konten **für fehlgeschlagene** Fehlerindikatoren für den Gesamtpaketverlust aufgrund des Verifizierungsfehlers für den Nachrichtenauthentifizierungscode (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
```

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Tests, die mit Cisco IOS® Version 15.1(4)M4 durchgeführt wurden. Die Skripts und die Konfiguration sind zwar noch nicht getestet, sollten aber auch mit früheren Cisco IOS-Softwareversionen funktionieren, da beide Applets EEM Version 3.0 verwenden (wird von IOS Version 12.4(22)T oder höher unterstützt).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Informationen zu Funktionen

"%CRYPTO-4-RECVD_PKT_MAC_ERR: entschlüsseln:" impliziert, dass ein verschlüsseltes Paket empfangen wurde, das die MAC-Verifizierung nicht bestanden hat. Diese Überprüfung ist das Ergebnis des konfigurierten Authentifizierungsturnus:

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

Im obigen Beispiel definiert *"esp-aes 256"* den Verschlüsselungsalgorithmus als 256-Bit-AES, und *"esp-md5"* definiert MD5 (HMAC-Variante) als den für die Authentifizierung verwendeten Hash-Algorithmus. Hash-Algorithmen wie MD5 werden in der Regel verwendet, um einen digitalen Fingerabdruck des Inhalts einer Datei bereitzustellen. Der digitale Fingerabdruck wird häufig verwendet, um sicherzustellen, dass die Datei nicht durch einen Eindringling oder Virus verändert wurde. Das Auftreten dieser Fehlermeldung impliziert in der Regel Folgendes:

- Der falsche Schlüssel wurde zur Verschlüsselung oder Entschlüsselung des Pakets verwendet. Dieser Fehler ist sehr selten und kann durch einen Softwarefehler verursacht werden.

ODER-

- Das Paket wurde während der Übertragung manipuliert. Dieser Fehler kann auf einen verschmutzten Stromkreis oder ein feindseliges Ereignis zurückzuführen sein.

Fehlerbehebungsmethode

Da diese Fehlermeldung in der Regel durch Paketfehler verursacht wird, besteht die einzige Möglichkeit, eine Ursachenanalyse durchzuführen, in der Verwendung von EPC, um vollständige Paketerfassungen von der WAN-Seite an beiden Tunnelendpunkten zu erhalten und diese zu vergleichen. Bevor Sie die Erfassungen abrufen, sollten Sie am besten ermitteln, welche Art von Datenverkehr diese Protokolle auslöst. In einigen Fällen kann es sich um eine bestimmte Art von Datenverkehr handeln. In anderen Fällen kann es zufällig sein, aber leicht reproduziert werden (z. B. 5-7 Tropfen alle 100 Pings). In solchen Situationen ist das Problem etwas leichter zu identifizieren. Der Trigger lässt sich am besten identifizieren, indem der Testdatenverkehr mit DSCP-Markierungen markiert und die Pakete erfasst werden. Der DSCP-Wert wird in den ESP-Header kopiert und kann dann mit Wireshark gefiltert werden. Diese Konfiguration, bei der ein Test mit 100 Pings vorausgesetzt wird, kann zum Markieren der ICMP-Pakete verwendet werden:

```
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
```

Diese Richtlinie muss nun auf die Eingangs-Schnittstelle angewendet werden, an der der ungehinderte Datenverkehr auf dem verschlüsselten Router eingeht:

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

Alternativ können Sie diesen Test auch mit Routerdatenverkehr ausführen. Dazu können Sie die Pakete nicht mit Quality of Service (QoS) kennzeichnen, sondern mit Policy-Based Routing (PBR).

> **Hinweis**: Um kritische (5) DSCP-Markierungen zu finden, verwenden Sie den Wireshark-Filter **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
```

Sobald die QoS-Markierung für Ihren ICMP-Datenverkehr konfiguriert ist, können Sie die integrierte Paketerfassung konfigurieren:

```
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"
```

Hinweis: Diese Funktion wurde in Cisco IOS Release 12.4(20)T eingeführt. Weitere Informationen zu EPCs finden Sie unter Embedded Packet Capture.

Die Verwendung einer Paketerfassung zur Behebung dieses Problems erfordert die Erfassung des gesamten Pakets, nicht nur eines Teils davon. Die EPC-Funktion in Cisco IOS-Versionen vor 15.0(1)M hat eine Puffergrenze von 512.000 und eine maximale Paketgrößenbeschränkung von 1024 Byte. Um diese Einschränkung zu vermeiden, aktualisieren Sie auf 15.0(1)M oder neueren Code, der jetzt eine Puffergröße von 100M bei einer maximalen Paketgröße von 9.500 Byte unterstützt.

Wenn das Problem mit jedem Ping mit 100 Zählern zuverlässig reproduziert werden kann, besteht das Worst-Case-Szenario darin, ein Wartungsfenster zu planen, um nur den Ping-Datenverkehr als kontrollierten Test zuzulassen und die Captures zu erfassen. Dieser Vorgang sollte nur wenige Minuten in Anspruch nehmen, aber er unterbricht den Produktionsdatenverkehr für diese Zeit. Wenn Sie QoS-Markierungen verwenden, können Sie die Anforderung, Pakete nur auf Pings zu beschränken, eliminieren. Um alle Ping-Pakete in einem Puffer zu erfassen, müssen Sie

sicherstellen, dass der Test nicht zu Spitzenzeiten durchgeführt wird.

Wenn das Problem nicht einfach reproduziert werden kann, können Sie ein EEM-Skript verwenden, um die Paketerfassung zu automatisieren. Die Theorie besagt, dass Sie die Aufnahmen auf beiden Seiten in einen Zirkelpuffer starten und EEM verwenden, um die Erfassung auf einer Seite zu stoppen. Gleichzeitig stoppt der EEM die Erfassung, lassen Sie ihn einen SNMP-Trap an den Peer senden, der seine Erfassung stoppt. Dieser Prozess könnte funktionieren. Bei starker Auslastung reagiert der zweite Router möglicherweise nicht schnell genug, um die Erfassung zu stoppen. Ein kontrollierter Test wird bevorzugt. Nachfolgend sind die EEM-Skripts aufgeführt, die den Prozess implementieren:

```
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!"
```

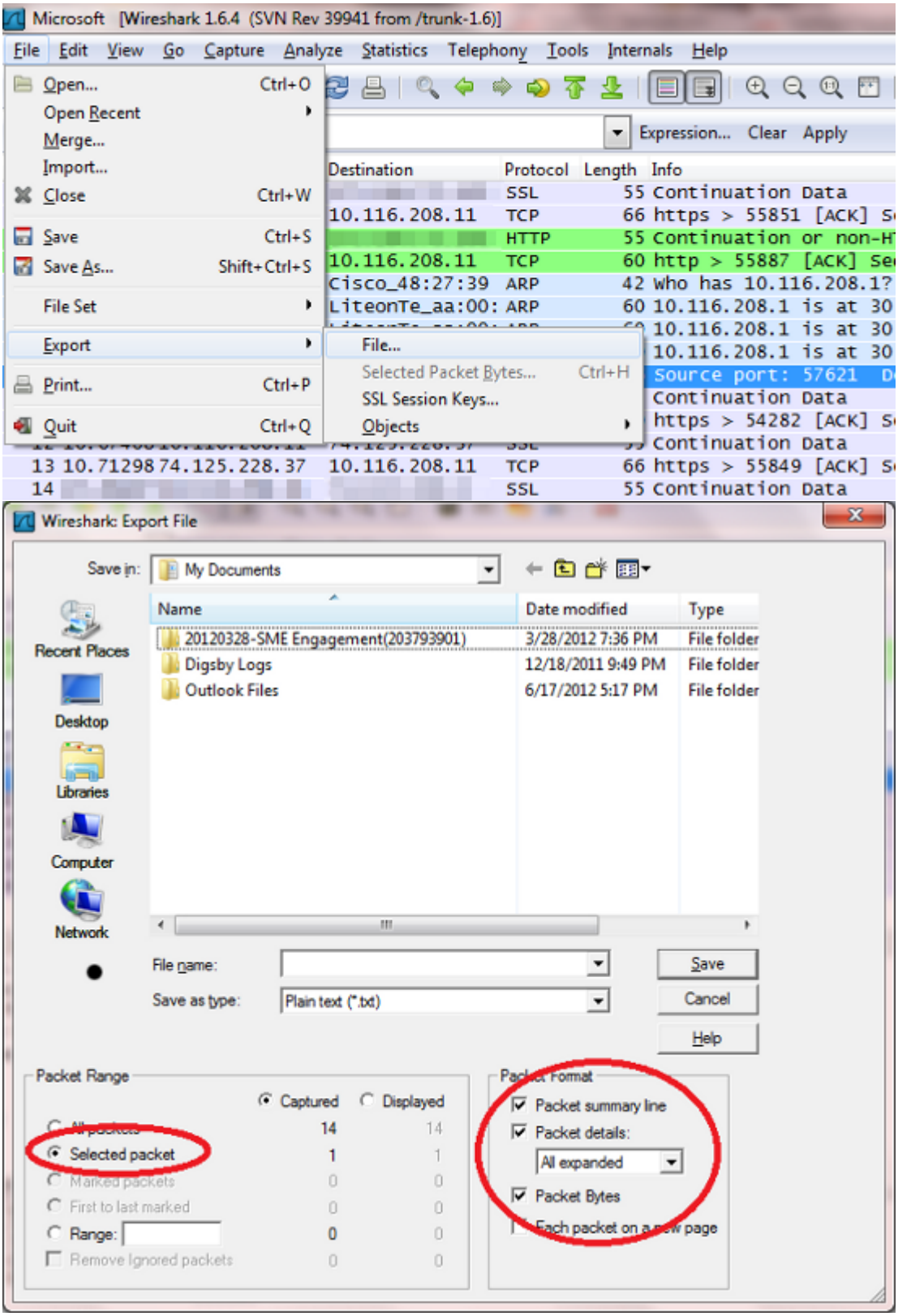
Beachten Sie, dass der Code im vorherigen Feld eine mit 15.0(1)M getestete Konfiguration ist. Möglicherweise möchten Sie diese mit der von Ihrem Kunden verwendeten Cisco IOS-Version testen, bevor Sie sie in der Kundenumgebung implementieren.

Datenanalyse

1. Nachdem die Erfassungen abgeschlossen sind, exportieren Sie sie mithilfe von TFTP auf einen PC.
2. Öffnen Sie die Erfassungen mit einem Netzwerkprotokoll-Analyzer (z. B. Wireshark).
3. Wenn die QoS-Markierung verwendet wurde, filtern Sie die entsprechenden Pakete heraus.

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

   "0x08" ist spezifisch für den DSCP-Wert AF21. Wenn ein anderer DSCP-Wert verwendet wird, kann der richtige Wert aus der Paketerfassung selbst oder aus der Liste der DSCP-Werte-Konvertierungsdiagramme abgeleitet werden. Weitere Informationen finden Sie unter DSCP und Precedence Values.
4. Identifizieren Sie den gefallenen Ping auf den Captures des Absenders, und suchen Sie das Paket auf den Captures sowohl auf der Empfänger- als auch auf der Absenderseite.
5. Exportieren Sie das Paket aus beiden Erfassungen, wie in diesem Bild gezeigt:



6. Führen Sie einen binären Vergleich der beiden durch. Wenn sie identisch sind, gab es keine Fehler bei der Übertragung, und das Cisco IOS wirft entweder ein falsches Negativ auf das empfangende Ende oder verwendet den falschen Schlüssel auf dem Absenderende. In beiden Fällen handelt es sich um einen Cisco IOS-Fehler. Wenn es sich um andere Pakete handelt, wurden die Pakete bei der Übertragung manipuliert.

   Das folgende Paket hat die Krypto-Engine im FC belassen:

```
*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.[!.
```

Hier ist das gleiche Paket, das auf dem Peer empfangen wurde:

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

An diesem Punkt handelt es sich höchstwahrscheinlich um ein ISP-Problem, und diese Gruppe sollte in die Fehlerbehebung einbezogen werden.

Häufige Probleme

- Die Cisco Bug-ID CSCed87408 beschreibt ein Hardwareproblem mit der Verschlüsselungs-Engine auf den 83xs, bei dem während der Verschlüsselung zufällige ausgehende Pakete beschädigt werden. Dies führt zu Authentifizierungsfehlern (in Fällen, in denen Authentifizierung verwendet wird) und Paketverlusten am empfangenden Ende. Es ist wichtig zu wissen, dass Sie diese Fehler nicht auf dem 83x selbst, sondern auf dem Empfangsgerät sehen.

- Manchmal wird dieser Fehler auf Routern angezeigt, die alten Code ausführen. Sie können ein Upgrade auf die aktuelleren Codeversionen wie 15.1(4) M4 durchführen, um das Problem zu beheben.

- Deaktivieren Sie die Hardwareverschlüsselung, um zu überprüfen, ob es sich um ein Hardware- oder Softwareproblem handelt. Wenn die Protokollmeldungen fortgesetzt werden, handelt es sich um ein Softwareproblem. Ist dies nicht der Fall, sollte eine RMA das Problem beheben.
  Denken Sie daran, dass bei Deaktivierung der Hardwareverschlüsselung die Netzwerkbelastung für stark ausgelastete VPN-Tunnel erheblich reduziert werden kann. Cisco empfiehlt daher, die in diesem Dokument beschriebenen Verfahren während eines Wartungsfensters zu testen.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems