与Ping损耗的Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:"错误消息在IPSec隧道故障排除

目录

简介

本文描述如何解决在IPSec隧道的ping损耗加上在Syslog的"%CRYPTO-4-RECVD_PKT_MAC_ERR"消息如方框所显示：

```
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
```

小百分比的这样丢包被认为正常。因此然而，一高丢弃速率问题影响服务，并且也许要求网络操作员的注意。注意在Syslog报告的这些消息是速率被限制在30个秒间隔，因此单个日志消息总是不表明仅单个数据包被撤销了。为了获取准确计数这些丢包，请发出show crypto ipsec sa detail命令，并且查看SA在日志看到的连接ID旁边。在SA计数器中， **pkts验证**信息包总数丢弃的**失败的**错误计数器帐户由于消息认证编码(MAC)验证失败。

```
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
```

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据用Cisco IOS版本15.1(4)M4进行的测验。虽然不测试，脚本和配置应该与初期的Cisco IOS软件版本一起使用，因为两applet使用EEM版本(IOS版本12.4(22)T支持以上)的3.0。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

以信息为特色

“%CRYPTO-4-RECVD_PKT_MAC_ERR ：解密：”暗示失败MAC验证的加密的信息包接收。此验证是设置配置的验证转换的结果：

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

在上述示例中， *“ESP aes 256”*定义了加密算法作为256-bit AES，并且*"esp-md5"*定义了MD5

(HMAC变量)作为用于验证的散列算法。散列算法类似MD5典型地用于提供文件目录的一数字指纹。digitial指纹是常用的保证文件未由入侵者或病毒修改。因而此错误消息出现通常暗示：

- 错误的密钥用于加密或解码数据包。此错误是非常少见的，并且可能由软件Bug造成。

-或

- 在传输期间，数据包被窜改。此错误能归结于一个坏的电路或一个敌对事件。

故障排除方法

因为此错误消息是典型地由信息包损坏造成的，要执行问题根源分析的唯一方法是使用EPC为了从在两个通道端点的广域网端得到完整数据包捕获和比较他们。在您获取捕获前，识别是最佳的什么样的流量触发这些日志。有时，它可以是一特定流量;在某些情况下，它也许随机，但是容易地再生产了(例如5-7下降每100 ping)。在这些情况下，问题变得轻微更加容易识别。识别触发的最佳方法是用DSCP标记标记测试流量和获取数据包。DSCP值复制对ESP报头，并且可能然后过滤与Wireshark。此配置，假设与100 ping的一测验，可以用于标记ICMP数据包：

```
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
```

必须当前应用此策略到清楚流量在加密路由器接收的入口接口：

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

或者，您也许要运行此测验以路由器生成的流量。对于此，您不能使用服务质量(QoS)标记数据包，但是您能使用基于策略的路由(PBR)。

注意：为了找出关键(5) DSCP标记，请使用Wireshark过滤器**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
```

一旦QoS标记为您的ICMP流量配置，您能配置嵌入式数据包捕获：

```
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"
```

注意：此功能在Cisco IOS版本12.4(20)T介绍。参考嵌入式数据包捕获关于EPCs的更多信息。

使用数据包捕获排除故障此种问题要求整个数据包捕获，不仅部分的它。在Cisco IOS版本的EPC功能在15.0(1)M之前有512K缓冲限额和1024个字节一最大数据包大小限制。为了避免此限制、升级到

15.0(1)M或更新的代码，现在支持捕获缓冲区大小100M与一最大数据包大小9500个字节。

如果问题可以可靠再生产与每100计数ping，最坏局面是安排维护窗口为了允许仅ping数据流，因为一受控的测验并且采取捕获。此进程应该花费仅几分钟，但是阻碍该时间的生产数据流。如果使用QoS标记，您能排除需求仅限制数据包到ping。为了获取在一缓冲区的所有ping信息包，您必须保证在峰值时间，测验没有进行。

如果问题没有容易地被再生产，您能使用EEM脚本自动化数据包捕获。理论是您开始在两边的捕获一圆的缓冲区并且使用EEM终止在一端的捕获。同时EEM终止捕获，安排它发送SNMP陷阱对对等体，终止其捕获。此进程也许工作。但是，如果负载是大量的，第二个路由器也许不起反应足够迅速终止其捕获。一受控的测验更喜欢。这是将实现进程的EEM脚本：

```
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!"
```

注意在上一个方框的代码是用15.0(1)M测试的配置。在您在用户环境前，实现它您也许要测试它与特定Cisco IOS版本您的客户用途。

数据分析

1. 一旦捕获完成，请使用TFTP导出他们到PC。
2. 打开捕获用网络协议分析器(例如Wireshark)。
3. 如果使用了QoS标记，请过滤各自数据包。
   `ip.dsfield.dscp==0x08`
   "0x08"为DSCP值AF21是特定。如果使用一个不同的DSCP值，正确值可以获取从数据包捕获或从DSCP值换算表列表。参考的DSCP和优先值欲知更多信息。
4. 识别在捕获的已丢失ping从发送方，并且查找在捕获的数据包在接收方和发送方支持。
5. 如此镜像所显示，导出从两个捕获的该数据包：
6. 执行一个二进制比较两个。 如果他们是相同的，则没有在运送中错误，并且Cisco IOS投掷了在接收端的假攻击或使用了在发送方末端的错误的密钥。无论如何，问题是Cisco IOS bug。 如果数据包不同的，则数据包在传输被窜改。

   这是数据包作为它留下在FC的加密引擎：

   ```
   *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.[!.
```

这是和一样它在对等体接收的数据包：

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

这时，是很可能ISP问题，并且该组在故障排除应该涉及。

常见问题

- Cisco Bug ID CSCed87408描述硬件问题用在随机的输出数据包在加密时是损坏的，导致验证错误的83xs的加密引擎(在使用验证)处和在接收端的丢包。意识到您将看不到在83x的这些错误是重要的，但是在接收设备。

- 有时运行旧有代码的路由器显示此错误。您能升级到更多最近代码版本例如15.1(4) M4解决问题。

- 为了验证，如果问题是硬件或软件问题，请禁用硬件加密。如果日志消息继续，它是软件问题。否则， RMA应该然后解决问题。
  切记，如果禁用硬件加密，能导致大量地装载的VPN通道的严重网络下降。所以，思科推荐您在维护窗口期间，步骤在本文描述的尝试。

相关信息

- 技术支持和文档 - Cisco Systems