Message d'erreur du Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" avec la perte de ping au-dessus du dépannage de tunnel d'IPsec

Contenu

Introduction

Ce document décrit comment résoudre la perte de ping au-dessus d'un tunnel d'IPsec ajouté aux messages de "%CRYPTO-4-RECVD_PKT_MAC_ERR" dans le Syslog suivant les indications de la case :

```
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
```

Un petit pourcentage de telles baisses est considéré normal. Cependant, un débit élevé de baisse en raison de ce problème peut affecter le service et pourrait exiger l'attention de l'opérateur réseau. Notez que ces messages signalés dans les Syslog sont débit limité aux 30 seconde intervalles, ainsi un message de log simple n'indique pas toujours que seulement un paquet simple obtenu a relâché. Afin d'obtenir un compte précis de ces baisses, émettre le **détail de show crypto ipsec sa de** commande, et regarder SA à côté de l'ID de connexion vu dans les logs. Parmi les compteurs SA, les **paquets vérifient le** compteur d'erreurs **défectueux** explique toute la perte de paquets due à la panne de vérification de code d'authentification de message (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
```

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur des tests faits avec la release 15.1(4)M4 de Cisco IOS®. Bien que pas encore testés, les scripts et la configuration devraient fonctionner avec des versions de logiciel plus tôt de Cisco IOS aussi bien puisque les deux applet utilisent la version 3.0 (qui EEM est prise en charge dans la version IOS 12.4(22)T ou ci-dessus).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Les informations de caractéristique

Le « %CRYPTO-4-RECVD_PKT_MAC_ERR : déchiffrage : » implique qu'on a reçu un paquet chiffré qui a manqué la vérification de MAC. Cette vérification est un résultat du jeu de transformations d'authentification configuré :

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

Dans l'exemple ci-dessus, le *« ESP-aes 256"* définit l'algorithme de chiffrement comme 256-bit AES, et *"esp-md5"* définit le MD5 (variante HMAC) comme algorithme de hachage utilisé pour l'authentification. Des algorithmes de hachage comme le MD5 sont typiquement utilisés pour fournir une empreinte digital numérique du contenu d'un fichier. L'empreinte digital digitial est employée souvent pour s'assurer que le fichier n'a pas été modifié par un intrus ou un virus. Ainsi l'occurrence de ce message d'erreur implique habituellement l'un ou l'autre :

- La clé fausse a été utilisée pour chiffrer ou déchiffrer le paquet. Cette erreur est très rare et pourrait sont provoqué par par une erreur de programmation.

  - OU

- Le paquet a été trifouillé pendant le transit. Cette erreur a pu être due à un circuit modifié ou à un événement hostile.

Dépannage de la méthodologie

Puisque ce message d'erreur est typiquement provoqué par la corruption de paquet, la seule manière de faire une analyse de la cause d'origine est d'employer la CPE afin d'obtenir les captures complètes de paquet du côté WAN sur des points d'extrémité de tunnel et les comparer. Avant que vous obteniez les captures, il est le meilleur d'identifier ce qu'un peu le trafic déclenche ces logs. Dans certains cas, ce peut être un genre de particularité de trafic ; dans d'autres cas, il pourrait être aléatoire mais s'est facilement reproduit (comme 5-7 goutte chaque 100 pings). Dans de telles situations, il devient légèrement plus facile l'identifier la question. La meilleure manière d'identifier le déclencheur est de marquer le trafic de test avec des marquages de DSCP et de capturer les paquets. La valeur DSCP est copiée sur l'en-tête de l'ESP et peut alors être filtrée avec Wireshark. Cette configuration, qui assume un test avec 100 pings, peut être utilisée pour marquer les paquets d'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
```

Cette stratégie doit maintenant être appliquée à l'interface d'entrée où le trafic clair est reçu sur le routeur de cryptage :

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

Alternativement, vous pourriez vouloir exécuter ce test avec le trafic routeur-généré. Pour ceci, vous ne pouvez pas employer le Qualité de service (QoS) pour marquer les paquets, mais vous pouvez utiliser la Gestion de réseau à base de règles.

Remarque: Afin de localiser (5) les marquages essentiels de DSCP, utilisez le **== 0x28 du**

filtre **ip.dsfield.dscp de** Wireshark.

```
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
```

Une fois que le marquage de QoS est configuré pour votre trafic d'ICMP, vous pouvez configurer la capture incluse de paquet :

```
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"
```

Remarque: cette caractéristique a été introduite dans la Cisco IOS version 12.4(20)T. Référez-vous à la capture incluse de paquet pour plus d'informations sur EPCs.

L'utilisation d'une capture de paquet de dépanner ce type de problème exige que le paquet entier soit capturé, pas simplement une partie de elle. La caractéristique CPE dans des releases de Cisco IOS avant 15.0(1)M a une limite de mémoire tampon de 512K et une limite de taille maximum de paquet de 1024 octets. Afin d'éviter cette limite, mise à jour à 15.0(1)M ou plus nouveau code, qui prend en charge maintenant une taille de mémoire tampon de capture de 100M avec une longueur de paquet maximum de 9500 octets.

Si la question peut être sûrement reproduite avec chaque ping de 100 comptes, le pire scénario est de programmer une fenêtre de maintenance afin de permettre seulement le trafic ping comme test commandé et prendre les captures. Ce processus devrait prendre seulement quelques minutes, mais il perturbe le trafic de production pendant ce temps. Si vous utilisez le marquage de QoS, vous pouvez éliminer la condition requise de limiter des paquets seulement aux pings. Afin de capturer tous les paquets de ping dans une mémoire tampon, vous devez s'assurer que le test n'est pas effectué pendant des heures de pointe.

Si la question n'est pas facilement reproduite, vous pouvez employer un script EEM pour automatiser la capture de paquet. La théorie est que vous engagez les captures des deux côtés dans une mémoire tampon circulaire et employez EEM pour arrêter la capture d'un côté. En même temps l'EEM arrête la capture, le fait envoyer un déroutement SNMP au pair, qui arrête sa capture. Ce processus pourrait fonctionner. Mais si le chargement est lourd, le deuxième routeur ne pourrait pas réagir assez rapidement pour arrêter sa capture. Un test commandé est préféré. Voici les scripts EEM qui implémenteront le processus :

```
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!"
```

Notez que le code dans la case précédente est une configuration testée avec 15.0(1)M. Vous pourriez vouloir le tester avec la version spécifique de Cisco IOS vos utilisations de client avant que vous l'implémentiez dans l'environnement de client.

Analyse de données

1. Une fois les captures ont été terminées, l'utilisation TFTP de les exporter à un PC.
2. Ouvrez les captures avec un analyseur de protocole réseau (tel que Wireshark).
3. Si le marquage de QoS était utilisé, filtrez les paquets respectifs.
   `ip.dsfield.dscp==0x08`
   "0x08" est spécifique pour la valeur DSCP AF21. Si une valeur DSCP différente est utilisée, la valeur correcte peut être obtenue de la capture de paquet elle-même ou de la liste de table de conversion de valeurs DSCP. Référez-vous au DSCP et au pour en savoir plus de valeurs de priorité.
4. Identifiez le ping relâché sur les captures de l'expéditeur, et localisez ce paquet sur des captures du côté de récepteur et du côté d'expéditeur.
5. Exportez ce paquet des deux captures suivant les indications de cette image :
6. Conduisez une comparaison binaire des deux. S'ils sont identiques, alors il n'y avait aucune erreur en transit et le Cisco IOS a jeté un faux négatif sur l'extrémité réceptrice ou a utilisé la clé fausse sur l'extrémité d'expéditeur. Dans l'un ou l'autre de cas, la question est une bogue de Cisco IOS. Si les paquets sont différents, alors les paquets ont été trifouillés dedans transmettent.

   Voici le paquet en tant que lui a laissé le moteur de chiffrement sur le 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.[!.
   ```

   Voici le même paquet qu'il a été reçu sur le pair :
   ```
   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 ................
   ```

En ce moment, il est le plus susceptible un problème ISP, et ce groupe devrait être impliqué dans le dépannage.

Problèmes courants

- L'ID de bogue Cisco CSCed87408 décrit un problème de matériel avec le moteur de chiffrement sur le 83xs où des paquets sortants aléatoires sont corrompus pendant le cryptage, qui mène aux erreurs d'authentification (dans les cas où l'authentification est utilisée) et des pertes de paquets sur l'extrémité réceptrice. Il est important de se rendre compte que vous ne verrez pas ces erreurs sur le 83x elle-même, mais sur le périphérique récepteur.

- Parfois Routeurs qui exécutent la vieille exposition de code cette erreur. Vous pouvez améliorer aux versions plus récentes de code telles que 15.1(4) M4 pour résoudre le problème.

- Afin de vérifier si le problème est un problème matériel ou logiciel, désactivez le chiffrement matériel. Si les messages de log continuent, c'est un problème logiciel. Sinon, alors un RMA devrait résoudre le problème.
  Souvenez-vous que si vous désactivez le chiffrement matériel, il peut entraîner la dégradation grave de réseau pour les tunnels VPN fortement chargés. Par conséquent, Cisco vous recommande tentent les procédures décrites dans ce document pendant une fenêtre de maintenance.

Informations connexes

- Support et documentation techniques - Cisco Systems