Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR : » Message d'erreur avec perte de Ping sur le tunnel IPsec Dépannage

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations sur les fonctionnalités
Méthodologie de dépannage
Analyse des données
Problèmes courants
Informations connexes

Introduction

Ce document décrit comment résoudre la perte de requêtes ping sur un tunnel IPsec couplé aux messages "%CRYPTO-4-RECVD_PKT_MAC_ERR » dans le syslog comme indiqué dans la zone :

```
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 faible pourcentage de ces chutes est considéré comme normal. Cependant, un taux de chute élevé en raison de ce problème peut avoir un impact sur le service et peut nécessiter l'attention de l'opérateur réseau. Notez que ces messages signalés dans les syslogs sont limités à un débit de 30 secondes, de sorte qu'un seul message de journal n'indique pas toujours qu'un seul paquet a été abandonné. Afin d'obtenir un nombre exact de ces pertes, émettez la commande **show crypto ipsec sa detail**, et regardez la SA en regard de l'ID de connexion affiché dans les journaux. Parmi les compteurs SA, les **pkts vérifient les** comptes de compteur d'erreurs **ayant échoué** pour la perte totale de paquet due à l'échec de vérification du 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.

Components Used

Les informations de ce document sont basées sur des tests effectués avec Cisco IOS® Version 15.1(4)M4. Bien qu'ils ne soient pas encore testés, les scripts et la configuration doivent également fonctionner avec les versions antérieures du logiciel Cisco IOS, puisque les deux applets utilisent la version 3.0 du module EEM (qui est prise en charge dans la version 12.4(22)T ou ultérieure du logiciel IOS).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations sur les fonctionnalités

Le message "%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: » signifie qu'un paquet chiffré a été reçu et qu'il a échoué à la vérification MAC. Cette vérification est le résultat du jeu de transformation d'authentification configuré :

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

Dans l'exemple ci-dessus, *« esp-aes 256 »* définit l'algorithme de chiffrement comme AES 256 bits, et *« esp-md5 »* définit le MD5 (variante HMAC) comme l'algorithme de hachage utilisé pour l'authentification. Les algorithmes de hachage tels que MD5 sont généralement utilisés pour fournir une empreinte numérique du contenu d'un fichier. L'empreinte digitale est souvent utilisée 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 généralement :

- La mauvaise clé a été utilisée pour chiffrer ou déchiffrer le paquet. Cette erreur est très rare et pourrait être causée par un bogue logiciel.

-OU-

- Le paquet a été altéré pendant le transit. Cette erreur peut être due à un circuit sale ou à un événement hostile.

Méthodologie de dépannage

Puisque ce message d'erreur est généralement causé par la corruption de paquets, la seule façon d'effectuer une analyse de cause à racine est d'utiliser EPC afin d'obtenir des captures de paquets complètes du côté WAN sur les deux points d'extrémité du tunnel et de les comparer. Avant d'obtenir les captures, il est préférable d'identifier quel type de trafic déclenche ces journaux. Dans certains cas, il peut s'agir d'un type spécifique de trafic ; dans d'autres cas, il peut être aléatoire mais facilement reproduit (par exemple 5 à 7 abandons toutes les 100 requêtes ping). Dans de telles situations, la question devient un peu plus facile à cerner. La meilleure façon d'identifier le déclencheur est de marquer le trafic de test avec des marquages DSCP et de capturer les paquets. La valeur DSCP est copiée dans l'en-tête ESP et peut ensuite être filtrée avec Wireshark. Cette configuration, qui suppose un test avec 100 requêtes ping, peut être utilisée pour marquer les paquets 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 chiffrement :

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

Vous pouvez également exécuter ce test avec le trafic généré par le routeur. Pour cela, vous ne pouvez pas utiliser la qualité de service (QoS) pour marquer les paquets, mais vous pouvez

utiliser le routage basé sur des stratégies (PBR).

> **Note**: Afin de localiser les marquages DSCP critiques (5), utilisez le filtre 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
```

Une fois le marquage QoS configuré pour votre trafic ICMP, vous pouvez configurer la capture de paquets intégrée :

```
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"
```

Note: cette fonctionnalité a été introduite dans Cisco IOS version 12.4(20)T. Référez-vous à Embedded Packet Capture pour plus d'informations sur les EPC.

L'utilisation d'une capture de paquets pour résoudre ce type de problème nécessite que le paquet entier soit capturé, et pas seulement une partie. La fonctionnalité EPC des versions de Cisco IOS antérieures à 15.0(1)M a une limite de tampon de 512 K et une limite de taille de paquet maximale de 1024 octets. Afin d'éviter cette limitation, mettez à niveau vers 15.0(1)M ou un code plus récent, qui prend désormais en charge une taille de tampon de capture de 100M avec une taille de paquet maximale de 9500 octets.

Si le problème peut être reproduit de manière fiable avec une requête ping de 100 nombres, le pire scénario est de planifier une fenêtre de maintenance afin de ne permettre que le trafic ping comme test contrôlé et de prendre les captures. Ce processus ne devrait prendre que quelques minutes, mais il perturbe le trafic de production pendant ce temps. Si vous utilisez le marquage QoS, vous pouvez éliminer l'obligation de limiter les paquets uniquement aux requêtes ping. Afin de capturer tous les paquets ping dans une mémoire tampon, vous devez vous assurer que le test n'est pas effectué pendant les heures de pointe.

Si le problème n'est pas facilement reproduit, vous pouvez utiliser un script EEM pour automatiser la capture de paquets. La théorie est que vous démarrez les captures des deux côtés dans une mémoire tampon circulaire et utilisez EEM pour arrêter la capture d'un côté. En même temps, l'EEM arrête la capture, lui demande d'envoyer un piège snmp à l'homologue, qui arrête sa capture. Ce processus pourrait fonctionner. Mais si la charge est lourde, le second routeur risque de ne pas réagir assez rapidement pour arrêter sa capture. Un test contrôlé est préférable. 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!"
```

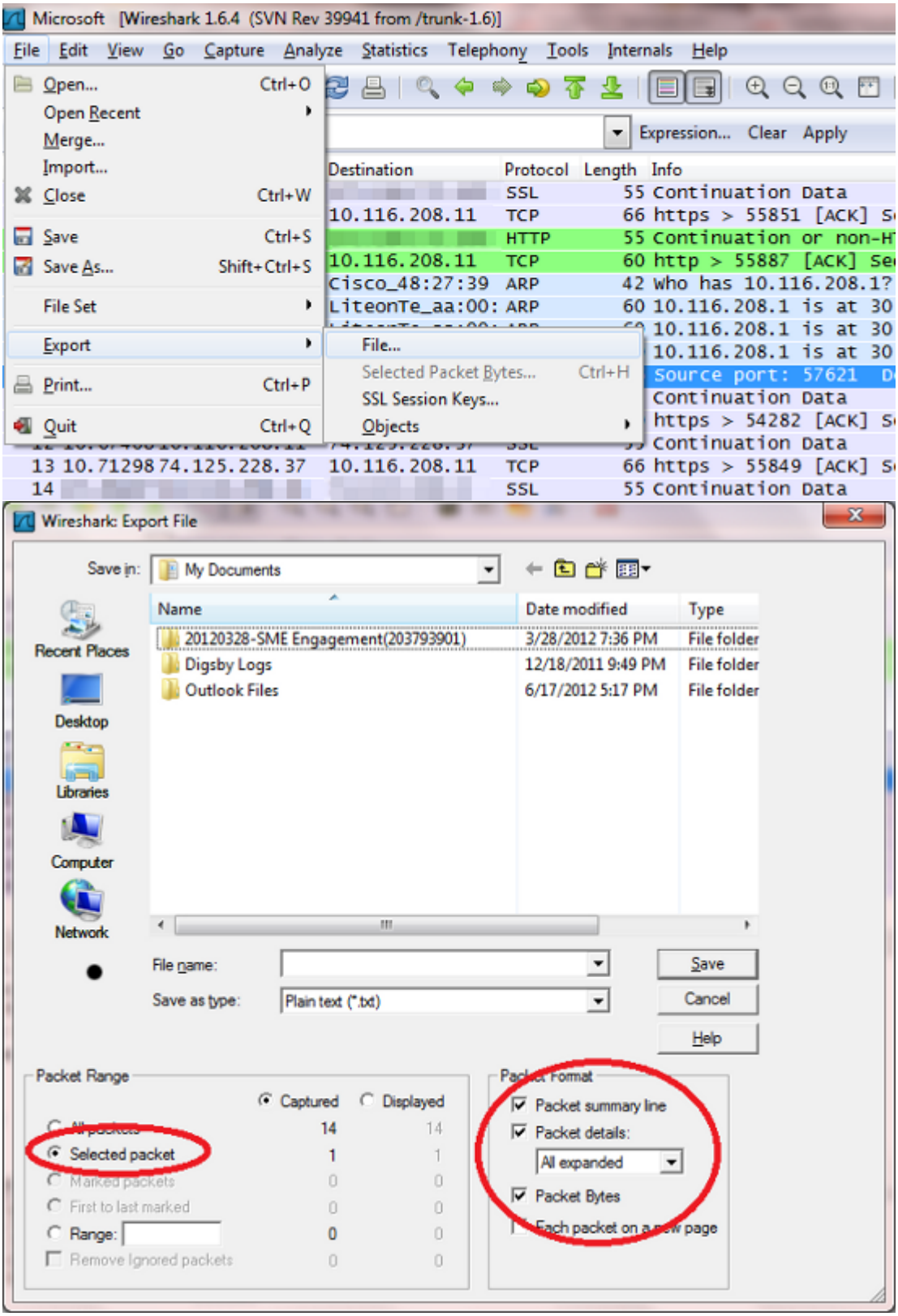
Notez que le code de la zone précédente est une configuration testée avec 15.0(1)M. Vous pouvez le tester avec la version spécifique de Cisco IOS que votre client utilise avant de l'implémenter dans l'environnement du client.

Analyse des données

1. Une fois les captures effectuées, utilisez TFTP pour les exporter vers un PC.
2. Ouvrez les captures avec un analyseur de protocole réseau (tel que Wireshark).
3. Si le marquage QoS a été utilisé, filtrez les paquets respectifs.

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

   «0x08 » est spécifique à la valeur DSCP AF21. Si une autre valeur DSCP est utilisée, la valeur correcte peut être obtenue à partir de la capture de paquets elle-même ou de la liste du graphique de conversion des valeurs DSCP. Référez-vous à Valeurs DSCP et de priorité pour plus d'informations.
4. Identifiez la requête ping abandonnée sur les captures de l'expéditeur et localisez ce paquet sur les captures à la fois du côté du récepteur et du côté de l'expéditeur.
5. Exportez ce paquet à partir des deux captures, comme illustré dans cette image :



6. Effectuez une comparaison binaire des deux. S'ils sont identiques, il n'y a pas eu d'erreur de transit et Cisco IOS a soit lancé un faux négatif sur l'extrémité de réception, soit utilisé la mauvaise clé sur l'extrémité de l'expéditeur. Dans les deux cas, le problème est un bogue Cisco IOS. Si les paquets sont différents, alors les paquets ont été falsifiés dans la transmission.

   Voici le paquet alors qu'il quittait 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 l'homologue :

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

Àce stade, il s'agit probablement d'un problème de FAI et ce groupe doit être impliqué dans le dépannage.

Problèmes courants

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

- Parfois, les routeurs qui exécutent un ancien code affichent cette erreur. Vous pouvez effectuer une mise à niveau vers les versions de code les plus récentes, 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 du journal continuent, il s'agit d'un problème logiciel. Dans le cas contraire, une RMA doit résoudre le problème.
  N'oubliez pas que si vous désactivez le cryptage matériel, il peut entraîner une grave dégradation du réseau pour les tunnels VPN lourdement chargés. Par conséquent, Cisco vous recommande d'essayer les procédures décrites dans ce document pendant une fenêtre de maintenance.

Informations connexes

- Support et documentation techniques - Cisco Systems