Mensagem de Erro do Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" com perda do sibilo sobre o Troubleshooting do túnel de IPsec

Índice

Introdução

Este documento descreve como resolver a perda do sibilo sobre um túnel de IPsec acoplado com mensagens de "%CRYPTO-4-RECVD_PKT_MAC_ERR" no Syslog segundo as indicações da caixa:

```
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
```

Uma porcentagem pequena de tais gotas é considerada normal. Contudo, uma taxa alta da gota devido a este problema pode impactar o serviço e pôde exigir a atenção do operador de rede. Note que estas mensagens relatadas nos Syslog são taxa limitada em 30 segundos intervalos, assim que um único mensagem de registro não indica sempre que somente um pacote único obtido deixou cair. A fim obter uma contagem exata destas gotas, emita o comando show crypto ipsec sa detail, e o olhar no SA ao lado do identificador de conexão visto nos logs. Entre os contadores SA, os **pacotes verificam que o** contador de erros **falhado** esclarece a gota do pacote total devido à falha de verificação do código de autenticação de mensagens (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
```

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada nos testes feitos com liberação 15.1(4)M4 do ® do Cisco IOS. Embora testados não ainda, os scripts e a configuração devem trabalhar com versões de Cisco IOS Software mais adiantadas também desde que ambos os applet usam o 3.0 da versão EEM (que é apoiada na Versão do IOS 12.4(22)T ou acima).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Caracterize a informação

O “%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: ” implica que um pacote criptografado esteve recebido que falhe a verificação MAC. Esta verificação é um resultado da autenticação transforma o grupo configurado:

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

No exemplo acima, o *“ESP-aes 256"* define o algoritmo de criptografia como o 256-bit AES, e *"esp-md5"* define o MD5 (variação HMAC) como o algoritmo de hash usado para a autenticação. Os algoritmos de hash como o MD5 são usados tipicamente para fornecer uma impressão digital digital dos índices de um arquivo. A impressão digital digitial é usada frequentemente assegurar-se de que o arquivo não esteja alterado por um intruso ou por um vírus. Assim a ocorrência deste Mensagem de Erro implica geralmente qualquer um:

- A chave errada foi usada para cifrar ou decifrar o pacote. Este erro é muito raro e poderia ser causado por um Bug de Software.

- OU

- O pacote foi alterado durante o trânsito. Este erro podia ser devido a um circuito sujo ou a um evento hostil.

Metodologia de Troubleshooting

Desde que este Mensagem de Erro é causado tipicamente pela corrupção de pacote, a única maneira de fazer uma análise de causa de raiz é usar o EPC a fim obter capturas de pacote de informação completas do lado WAN em ambos os pontos finais do túnel e compará-los. Antes que você obtenha as captações, é o melhor identificar que tipo do tráfego provoca estes logs. Em alguns casos, pode ser um tipo específico do tráfego; em outros casos, pôde ser aleatório mas reproduziu facilmente (como 5-7 deixa cair cada 100 sibilos). Em tais situações, a edição torna-se levemente mais fácil de identificar. A melhor maneira de identificar o disparador é marcar o tráfego de teste com marcações DSCP e capturar os pacotes. O valor DSCP é copiado ao cabeçalho de ESP e pode então ser filtrado com Wireshark. Esta configuração, que supõe um teste com 100 sibilos, pode ser usada para marcar os pacotes ICMP:

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

Esta política deve agora ser aplicada à interface de ingresso onde o tráfego claro é recebido no roteador de criptografia:

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

Alternativamente, você pôde querer executar este teste com tráfego roteador-gerado. Para isto, você não pode usar o Qualidade de Serviço (QoS) para marcar os pacotes, mas você pode o Use Policy-Based Routing (PBR).

> Nota: A fim encontrar (5) marcações críticas DSCP, use o **== 0x28 do** filtro **ip.dsfield.dscp de** Wireshark**.**

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

Uma vez que a marcação de QoS é configurada para seu tráfego ICMP, você pode configurar a captura de pacote de informação encaixada:

```
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"
```

Nota: esta característica foi introduzida no Cisco IOS Release 12.4(20)T. Refira a captura de pacote de informação encaixada para obter mais informações sobre dos epc.

O uso de uma captura de pacote de informação pesquisar defeitos este tipo de problema exige que o pacote inteiro esteja capturado, não apenas uma parcela dele. A característica do EPC em liberações do Cisco IOS antes de 15.0(1)M tem um limite de buffer de 512K e um limite máximo do tamanho do pacote de 1024 bytes. A fim evitar esta limitação, elevação a 15.0(1)M ou o código mais novo, que apoia agora um tamanho de buffer da captação de 100M com um tamanho do pacote máximo de 9500 bytes.

Se a edição pode confiantemente ser reproduzida com cada sibilo de 100 contagens, o cenário de caso pior é programar uma janela de manutenção a fim permitir somente o tráfego de ping como um teste controlado e tomar as captações. Este processo deve tomar somente alguns minutos, mas interrompe o tráfego de produção por esse tempo. Se você usa a marcação de QoS, você pode eliminar a exigência restringir pacotes somente aos sibilos. A fim capturar todos os pacotes de ping em um buffer, você deve assegurar-se de que o teste não esteja conduzido durante horas de pico.

Se a edição não é reproduzida facilmente, você pode usar um script EEM para automatizar a captura de pacote de informação. A teoria é que você começa as captações em ambos os lados em um buffer circular e usa EEM para parar a captação em um lado. Ao mesmo tempo o EEM para a captação, manda-a enviar uma armadilha SNMP ao par, que para sua captação. Este processo pôde trabalhar. Mas se a carga é pesada, o segundo roteador não pôde reagir rapidamente bastante para parar sua captação. Um teste controlado é preferido. Estão aqui os scripts EEM que executarão o processo:

```
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"
```

```
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"
```

Note que o código na caixa precedente é uma configuração testada com 15.0(1)M. Você pôde querer testá-lo com a versão do Cisco IOS específica seus usos do cliente antes que você a execute no ambiente de cliente.

Análise de dados

1. Uma vez as captações foram terminadas, usam o TFTP para exportá-los para um PC.
2. Abra as captações com um analisador do protocolo de rede (tal como Wireshark).
3. Se a marcação de QoS foi usada, filtre para fora os pacotes respectivos.

```
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"
```

   "0x08" é específico para o valor AF21 DSCP. Se um valor diferente DSCP é usado, o valor correto pode ser obtido da captura de pacote de informação próprio ou da lista de gráfico de conversão dos valores DSCP. Refira o DSCP e os valores de precedência para mais informação.
4. Identifique o sibilo deixado cair nas captações do remetente, e encontre esse pacote em captações no lado do receptor e no lado do remetente.
5. Exporte esse pacote de ambas as captações segundo as indicações desta imagem:
6. Conduza uma comparação binária dos dois. Se são idênticos, a seguir não havia nenhum erro no trânsito e o Cisco IOS jogou um falso negativo na extremidade de recepção ou usou a chave errada na extremidade do remetente. Em qualquer dos casos, a edição é um erro do Cisco IOS. Se os pacotes são diferentes, a seguir os pacotes estiveram alterados dentro transmitem.

   Está aqui o pacote como ele deixou a crypto-engine no FC:

```
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"
```

   Está aqui o mesmo pacote que foi recebido no par:

```
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"
```

Neste momento, é mais provável um problema ISP, e esse grupo deve ser envolvido no Troubleshooting.

Problemas comuns

- A identificação de bug Cisco CSCed87408 descreve um problema de hardware com a crypto-engine no 83xs onde os pacotes de saída aleatórios são corrompidos durante a criptografia, que conduz aos erros de autenticação (nos casos onde a autenticação é usada) e às quedas de pacote de informação na extremidade de recepção. É importante realizar que você não verá estes erros no 83x próprios, mas no dispositivo receptor.

- Às vezes Roteadores que executa a mostra velha do código este erro. Você pode promover a mais versões do código recente tais como 15.1(4) M4 para resolver a edição.

- A fim verificar se o problema é um problema de hardware ou software, desabilite a criptografia de hardware. Se os mensagens de registro continuam, é uma questão de software. Se não, então um RMA deve resolver o problema.
  Recorde que se você desabilita a criptografia de hardware, pode causar a degradação severa da rede para túneis pesadamente carregados VPN. Consequentemente, Cisco recomenda-o tentativa que os procedimentos descreveram neste documento durante uma janela de manutenção.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems