

Solucionar problemas de fragmentação: Afetando o c9800 Wireless Controller com o Azure

Contents

[Introdução](#)

[Sintomas](#)

[Erro no servidor ISE](#)

[Análise detalhada de log:](#)

[Controlador sem fio EPC:](#)

[Despejos de TCP ISE](#)

[Captura Lateral do Azure com análise:](#)

[Sugestão de solução alternativa da extremidade do controlador sem fio:](#)

[Solução:](#)

Introdução

Este documento descreve um problema conhecido com a plataforma Azure que leva à perda de pacotes devido ao manuseio incorreto de fragmentos fora de sequência.

Sintomas

Produtos afetados: O Catalyst 9800-CL Wireless Controller hospedado no Azure ou o Identity Service Engine hospedado no Azure.

Configuração de SSID: Configurado para EAP-TLS 802.1x com autenticação central.

Conduta: Ao utilizar o 9800-CL hospedado na plataforma Azure com um SSID baseado em EAP-TLS, você pode encontrar problemas de conectividade. Os clientes podem encontrar dificuldades durante a fase de autenticação.

Erro no servidor ISE

Código de erro 5411 indicando que o requerente parou de se comunicar com o ISE durante a troca de certificado EAP-TLS.

Análise detalhada de log:

Aqui está uma ilustração de uma das configurações afetadas: No controlador sem fio 9800, o SSID é configurado para 802.1x e o servidor AAA é configurado para EAP-TLS. Quando um cliente tenta a autenticação, particularmente durante a fase de troca de certificado, o cliente envia um certificado que excede o tamanho da unidade de transmissão máxima (MTU) no controlador sem fio. Em seguida, o controlador sem fio 9800 fragmenta esse grande pacote e envia os fragmentos sequencialmente para o servidor AAA. No entanto, esses fragmentos não chegam na ordem correta no host físico, levando à queda do pacote.

Aqui estão os rastreamentos de RA do controlador sem fio quando o cliente está tentando se conectar:

O cliente entrando no estado de autenticação L2 e o processo EAP é iniciado

```
04/2023/12 16:51:27.606414 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_90000004] Entrando no estado de  
solicitação  
04/2023/12 16:51:27.606425 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [0000.0000.0000:capwap_90000004] Enviando pacote EAPOL  
04/2023/12 16:51:27.606494 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_90000004] Pacote EAPOL enviado -  
Versão: 3,Tipo EAPOL : EAP, Comprimento do payload: 1008, Tipo de EAP =  
EAP-TLS  
04/2023/12 16:51:27.606496 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_90000004] Pacote EAP - SOLICITAÇÃO,  
ID: 0x25  
04/2023/12 16:51:27.606536 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_90000004] Pacote EAPOL enviado ao  
cliente  
04/2023/12 16:51:27.640768 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_90000004] Pacote EAPOL recebido -  
Versão: 1,Tipo EAPOL : EAP, Comprimento do payload: 6, Tipo de EAP =  
EAP-TLS  
04/2023/12 16:51:27.640781 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_90000004] Pacote EAP - RESPOSTA, ID:  
0x25
```

Quando o controlador Wireless envia a solicitação de acesso ao servidor AAA e o tamanho do pacote está abaixo de 1500 bytes (que é o MTU padrão no controlador Wireless), o desafio de acesso é recebido sem complicações.

```
04/2023/12 16:51:27.641094 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Enviar solicitação de acesso para  
172.16.26.235:1812 id 0/6, len 552  
04/2023/12 16:51:27.644693 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Recebido de id 1812/6 172.16.26.235:0, Access-  
Challenge, len 1141
```

Às vezes, um cliente pode enviar seu certificado para autenticação. Se o tamanho do pacote exceder a MTU, ele será fragmentado antes de ser enviado posteriormente.

```
04/2023/12 16:51:27.758366 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Enviar solicitação de acesso para  
172.16.26.235:1812 id 0/8, len 2048  
04/2023/12 16:51:37.761885 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Iniciado o tempo limite de 5 segundos  
04/2023/12 16:51:42.762096 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Retransmitir para (172.16.26.235:1812,1813) para  
id 0/8  
04/2023/12 16:51:32.759255 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Retransmitir para (172.16.26.235:1812,1813) para  
id 0/8  
04/2023/12 16:51:32.760328 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Iniciado o tempo limite de 5 segundos  
04/2023/12 16:51:37.760552 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Retransmitir para (172.16.26.235:1812,1813) para  
id 0/8  
04/2023/12 16:51:42.762096 {wncd_x_R0-0}{1}: [raio] [19224]:  
(informações): RADIUS: Retransmitir para (172.16.26.235:1812,1813) para  
id 0/8
```

Observamos que o tamanho do pacote é 2048, o que ultrapassa o MTU padrão. Consequentemente, não houve resposta do servidor AAA. A controladora Wireless reenviará persistentemente a solicitação de acesso até atingir o número máximo de tentativas. Devido à ausência de resposta, o controlador sem fio reiniciará o processo EAPOL.

```
04/2023/12 16:51:45.762890 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_900000004] Publicando EAPOL_START no  
cliente  
04/2023/12 16:51:45.762956 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_900000004] Entrando no estado init  
04/2023/12 16:51:45.762965 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_900000004] Publicação !AUTH_ABORT no  
cliente  
04/2023/12 16:51:45.762969 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(informações): [Client_MAC:capwap_900000004] Entrando no estado de  
reinicialização
```

Esse processo entra em loop e o cliente fica preso somente na fase de autenticação.

A Captura de pacotes incorporada capturada no controlador sem fio mostra que, após várias solicitações de acesso e trocas de desafio com uma MTU menor que 1500 bytes, o controlador sem fio envia uma solicitação de acesso superior a 1500 bytes, que contém o certificado do

cliente. Esse pacote maior sofre fragmentação. No entanto, não há resposta a essa solicitação de acesso específica. O controlador sem fio continua a reenviar essa solicitação até atingir o número máximo de novas tentativas, após o qual a sessão EAP-TLS será reiniciada. Essa sequência de eventos continua se repetindo, indicando que há um loop EAP-TLS ocorrendo quando o cliente tenta se autenticar. Consulte as capturas de pacotes simultâneos da controladora Wireless e do ISE fornecidas abaixo para obter uma compreensão mais clara.

Controlador sem fio EPC:

radius.code == 1				
No.	Time	Protocol	Length	Info
109	12:21:27.510959	RADIUS	594	Access-Request id=3
110	12:21:27.510959	RADIUS	594	Access-Request id=3, Duplicate Request
117	12:21:27.554963	RADIUS	594	Access-Request id=4
118	12:21:27.554963	RADIUS	594	Access-Request id=4, Duplicate Request
125	12:21:27.599959	RADIUS	594	Access-Request id=5
126	12:21:27.599959	RADIUS	594	Access-Request id=5, Duplicate Request
135	12:21:27.640958	RADIUS	594	Access-Request id=6
136	12:21:27.640958	RADIUS	594	Access-Request id=6, Duplicate Request
143	12:21:27.676951	RADIUS	594	Access-Request id=7
144	12:21:27.676951	RADIUS	594	Access-Request id=7, Duplicate Request
154	12:21:27.758948	RADIUS	714	Access-Request id=8
796	12:21:32.759955	RADIUS	714	Access-Request id=8, Duplicate Request
1130	12:21:37.761954	RADIUS	714	Access-Request id=8, Duplicate Request
1868	12:21:42.762945	RADIUS	714	Access-Request id=8, Duplicate Request
2132	12:21:45.796955	RADIUS	538	Access-Request id=9
2133	12:21:45.796955	RADIUS	538	Access-Request id=9, Duplicate Request
2144	12:21:45.854951	RADIUS	760	Access-Request id=10
2145	12:21:45.854951	RADIUS	760	Access-Request id=10, Duplicate Request
2168	12:21:45.914945	RADIUS	594	Access-Request id=11
2169	12:21:45.914945	RADIUS	594	Access-Request id=11, Duplicate Request
2176	12:21:45.959941	RADIUS	594	Access-Request id=12

Captura de pacotes na WLC

Observamos que o controlador sem fio está enviando várias solicitações duplicadas para um ID de solicitação de acesso específico = 8



Note: No que respeita ao EPC, verificamos também que existe uma única solicitação em duplicado para outros ID. Isso faz com que a pergunta: Espera-se uma tal duplicação? A resposta à questão de saber se esta duplicação é esperada é sim, é. O motivo é que a captura foi feita na GUI do controlador sem fio com a opção "Monitor Control Plane" selecionada. Como resultado, é normal observar várias instâncias de pacotes RADIUS desde que estejam sendo direcionados para a CPU. Nesses casos, as solicitações de Acesso devem ser vistas com os endereços MAC origem e destino definidos como 00:00:00.

No.	Time	Protocol	Length	Info
109	12:21:27.510959	RADIUS	594	Access-Request id=3
110	12:21:27.510959	RADIUS	594	Access-Request id=3, Duplicate Request
117	12:21:27.554963	RADIUS	594	Access-Request id=4
118	12:21:27.554963	RADIUS	594	Access-Request id=4, Duplicate Request

> Frame 109: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits)

> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Source: 00:00:00_00:00:00 (00:00:00:00:00:00)

Type: IPv4 (0x0800)

Somente as solicitações de Acesso com os endereços MAC origem e destino especificados devem realmente ser enviadas para fora do controlador Wireless.

No.	Time	Protocol	Length	Info
109	12:21:27.510959	RADIUS	594	Access-Request id=3
110	12:21:27.510959	RADIUS	594	Access-Request id=3, Duplicate Request
117	12:21:27.554963	RADIUS	594	Access-Request id=4
118	12:21:27.554963	RADIUS	594	Access-Request id=4, Duplicate Request

> Frame 110: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits)

> Ethernet II, Src: Microsoft [redacted], Dst: [redacted]

> Destination: 12:34:56:78:9a:bc (12:34:56:78:9a:bc)

> Source: Microsoft_95:42:9e (00:22:48:95:42:9e)

Type: IPv4 (0x0800)

Solicitação de Acesso Radius Enviada ao Servidor AAA

As solicitações de Acesso em questão, identificadas pelo ID = 8, que são enviadas várias vezes e para as quais nenhuma resposta foi vista do servidor AAA. Após investigação adicional, observamos que para o ID de solicitação de acesso=8, a fragmentação de UDP está ocorrendo devido ao tamanho que ultrapassa o MTU, conforme ilustrado abaixo:

147	12:21:27.683955	TLSv1.2	104	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
148	12:21:27.683955	EAP	104	Request, TLS EAP (EAP-TLS)
149	12:21:27.756949	CAPWAP-Data	1450	CAPWAP-Data (Fragment ID: 50383, Fragment Offset: 0)
150	12:21:27.756949	EAP	188	Response, TLS EAP (EAP-TLS)
151	12:21:27.756949	EAP	1580	Response, TLS EAP (EAP-TLS)
152	12:21:27.758948	IPv4	1410	Fragmented IP protocol (proto=UDP 17, off=0, ID=b156) [Reassembled in #154]
153	12:21:27.758948	IPv4	1410	Fragmented IP protocol (proto=UDP 17, off=0, ID=b156) [Reassembled in #154]
154	12:21:27.758948	RADIUS	714	Access-Request id=8
155	12:21:27.758948	IPv4	714	Fragmented IP protocol (proto=UDP 17, off=1376, ID=b156)
156	12:21:28.084987	TLSv1.2	1070	Application Data

Fragmentação ocorrendo na captura de pacotes de WLC

> Frame 152: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits)

> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Source: 00:00:00_00:00:00 (00:00:00:00:00:00)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1396

Identification: 0xb156 (45398)

> 001. = Flags: 0x1, More fragments

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: UDP (17)

Header Checksum: 0xc9b4 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.100.9.15

Destination Address: 172.16.26.235

[Reassembled IPv4 in frame: 154]

> Data (1376 bytes)

Pacote Fragmentado - I

```

> Frame 153: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits)
v Ethernet II, Src: Microsoft_ [REDACTED], Dst: [REDACTED]
  > Destination: 12:34:56:78:9a:bc (12:34:56:78:9a:bc)
  > Source: Microsoft_95:42:9e (00:22:48:95:42:9e)
  Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1396
  Identification: 0xb156 (45398)
  > 001. .... = Flags: 0x1, More fragments
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xc9b4 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.100.9.15
  Destination Address: 172.16.26.235
  [Reassembled IPv4 in frame: 154]

```

Pacote Fragmentado - II

152	12:21:27.758948	IPv4	1410	Fragmented IP protocol (proto=UDP 17, off=0, ID=b156) [Reassembled in #154]
153	12:21:27.758948	IPv4	1410	Fragmented IP protocol (proto=UDP 17, off=0, ID=b156) [Reassembled in #154]
154	12:21:27.758948	RADIUS	714	Access-Request id=8
155	12:21:27.758948	IPv4	714	Fragmented IP protocol (proto=UDP 17, off=1376, ID=b156)

```

> Frame 154: 714 bytes on wire (5712 bits), 714 bytes captured (5712 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
v Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 700
  Identification: 0xb156 (45398)
  > 000. .... = Flags: 0x0
  ...0 0000 1010 1100 = Fragment Offset: 1376
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xebc0 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.100.9.15
  Destination Address: 172.16.26.235
v [3 IPv4 Fragments (2056 bytes): #152(1376), #153(1376), #154(680)]
  [Frame: 152, payload: 0-1375 (1376 bytes)]
  > [Frame: 153, payload: 0-1375 (1376 bytes)]
  [Frame: 154, payload: 1376-2055 (680 bytes)]
  [Fragment count: 3]
  [Reassembled IPv4 length: 2056]

```

Pacote remontado

Para verificar, revisamos os registros do ISE e descobrimos que a solicitação de acesso, que havia sido fragmentada no controlador sem fio, não estava sendo recebida pelo ISE.

Despejos de TCP ISE

radius.code == 1

o.	Time	Protocol	Length	Info
1	12:21:27.387158	RADIUS	538	Access-Request id=0
3	12:21:27.428304	RADIUS	760	Access-Request id=1
5	12:21:27.492019	RADIUS	594	Access-Request id=2
7	12:21:27.527949	RADIUS	594	Access-Request id=3
9	12:21:27.572272	RADIUS	594	Access-Request id=4
11	12:21:27.617147	RADIUS	594	Access-Request id=5
13	12:21:27.657917	RADIUS	594	Access-Request id=6
15	12:21:27.694381	RADIUS	594	Access-Request id=7
17	12:21:45.814195	RADIUS	538	Access-Request id=9
19	12:21:45.871163	RADIUS	760	Access-Request id=10
21	12:21:45.932076	RADIUS	594	Access-Request id=11
23	12:21:45.977012	RADIUS	594	Access-Request id=12
25	12:21:46.018562	RADIUS	594	Access-Request id=13

Capturas no final do ISE

Captura Lateral do Azure com análise:

A equipe do Azure realizou uma captura no host físico dentro do Azure. Os dados capturados no vSwitch dentro do host Azure indicam que os pacotes UDP estão chegando fora de sequência. Como esses fragmentos UDP não estão na ordem correta, o Azure os está descartando. Abaixo estão as capturas da extremidade do Azure e da controladora Wireless, tiradas simultaneamente para ID de solicitação de acesso = 255, onde o problema de pacotes fora de ordem é claramente evidente:

O Encapsulated Packet Capture (EPC) no controlador Wireless exibe a sequência em que os pacotes fragmentados saem do controlador Wireless.

0619_AURAUENRAWLC01_source.pcap

File Edit View Go Capture Analyze **Filter** Telephony Wireless Tools Help

ip.addr == 10.100.9.15 && ip.addr == 172.16.26.235 && (p.id == 33004 or p.id == 35253)

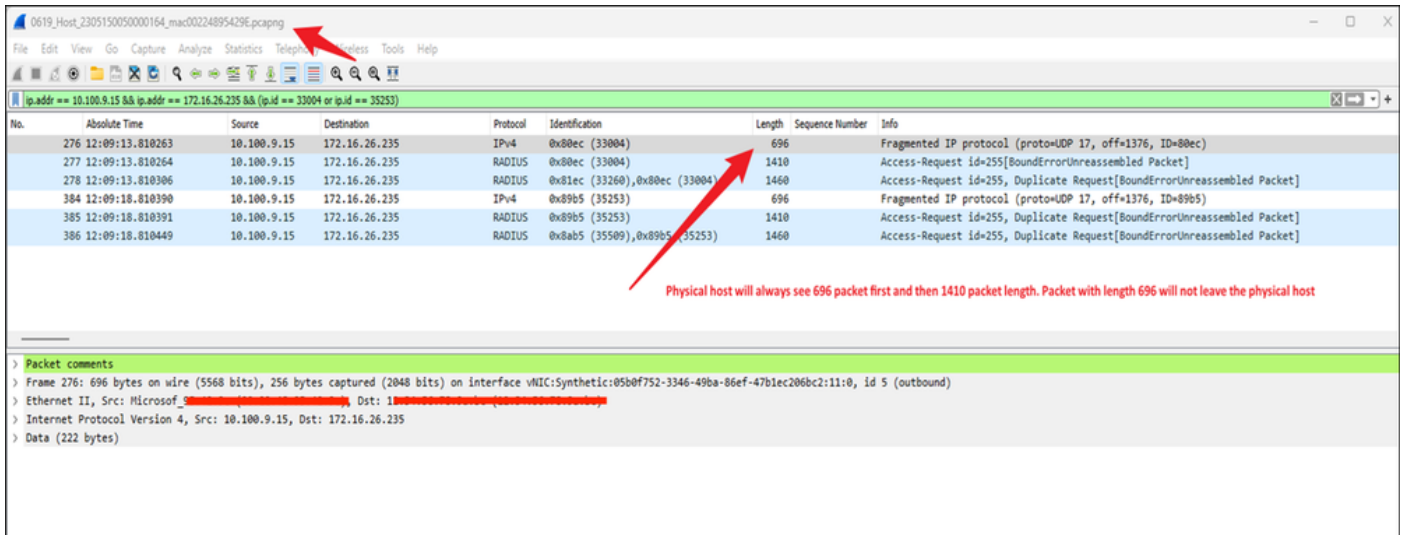
No.	Absolute Time	Source	Destination	Protocol	Identification	Length	Sequence Number	Info
5629	12:09:05.029997	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=80ec) [Reassembled in #5631]
5630	12:09:05.029997	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=80ec) [Reassembled in #5631]
5631	12:09:05.029997	10.100.9.15	172.16.26.235	RADIUS	0x80ec (33004)	696		Access-Request id=255
5632	12:09:05.029997	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=80ec)
5721	12:09:10.029997	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=89b5) [Reassembled in #5723]
5722	12:09:10.029997	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=89b5) [Reassembled in #5723]
5723	12:09:10.029997	10.100.9.15	172.16.26.235	RADIUS	0x89b5 (35253)	696		Access-Request id=255, Duplicate Request
5724	12:09:10.029997	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=89b5)

VM Capture will see packet length of 1410 is sent first, then 696

Frame 5721: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 19, 2023 12:09:10.029997000 AUS Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1687140550.029997000 seconds
[Time delta from previous captured frame: 0.525034000 seconds]
[Time delta from previous displayed frame: 5.000000000 seconds]
[Time since reference or first frame: 94.285041000 seconds]
Frame Number: 5721
Frame Length: 1410 bytes (11280 bits)
Capture Length: 1410 bytes (11280 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:data]

Sequência de pacotes fragmentados no WLC

No host físico, os pacotes não estão chegando na sequência correta



0619_Host_2305150050000164_mac00224895429E.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.100.9.15 && ip.addr == 172.16.26.235 && (p.id == 33004 or ip.id == 35253)

No.	Absolute Time	Source	Destination	Protocol	Identification	Length	Sequence Number	Info
276	12:09:13.810263	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=80ec)
277	12:09:13.810264	10.100.9.15	172.16.26.235	RADIUS	0x80ec (33004)	1410		Access-Request id=255[BoundErrorUnreassembled Packet]
278	12:09:13.810306	10.100.9.15	172.16.26.235	RADIUS	0x81ec (33260), 0x80ec (33004)	1460		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]
384	12:09:18.810390	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=89b5)
385	12:09:18.810391	10.100.9.15	172.16.26.235	RADIUS	0x89b5 (35253)	1410		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]
386	12:09:18.810449	10.100.9.15	172.16.26.235	RADIUS	0x8ab5 (35509), 0x89b5 (35253)	1460		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]

Physical host will always see 696 packet first and then 1410 packet length. Packet with length 696 will not leave the physical host

Packet comments

- > Frame 276: 696 bytes on wire (5568 bits), 256 bytes captured (2048 bits) on interface vNIC:Synthetic:05b0f752-3346-49ba-86ef-47b1ec206bc2:11:0, id 5 (outbound)
- > Ethernet II, Src: Microsof..., Dst: 1...
- > Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
- > Data (222 bytes)

Capturas no Fim do Azure

Como os pacotes estão chegando na ordem errada e o nó físico está programado para rejeitar quadros fora de ordem, os pacotes são descartados imediatamente. Essa interrupção faz com que o processo de autenticação falhe, deixando o cliente incapaz de progredir além da fase de autenticação.

Sugestão de solução alternativa da extremidade do controlador sem fio:

Começando com a versão 17.11.1, estamos implementando suporte para Jumbo Frames em pacotes Radius/AAA. Esse recurso permite que o controlador c9800 evite a fragmentação de pacotes AAA, desde que a seguinte configuração seja definida no controlador. Observe que, para evitar a fragmentação total desses pacotes, é essencial garantir que cada salto de rede, incluindo o servidor AAA, seja compatível com pacotes de Jumbo Frame. Para o ISE, o suporte a Jumbo Frame começa com a versão 3.1 em diante.

Configuração da interface no controlador sem fio:

```
C9800-CL(config)#interface
```

```
C9800-CL(config-if) # mtu
```

```
C9800-CL(config-if) # ip mtu
```

```
[1500 to 9000]
```

Configuração do servidor AAA no controlador sem fio:

```
C9800-CL(config)# aaa group server radius
```

```
C9800-CL(config-sg-radius) # server name
```

```
C9800-CL(config-sg-radius) # ip radius source-interface
```

Aqui está uma breve visão de um pacote Radius quando a MTU (Unidade Máxima de Transmissão) é configurada para 3000 bytes em um Controller de LAN Wireless (WLC). Pacotes menores que 3000 bytes foram enviados perfeitamente sem a necessidade de fragmentação:

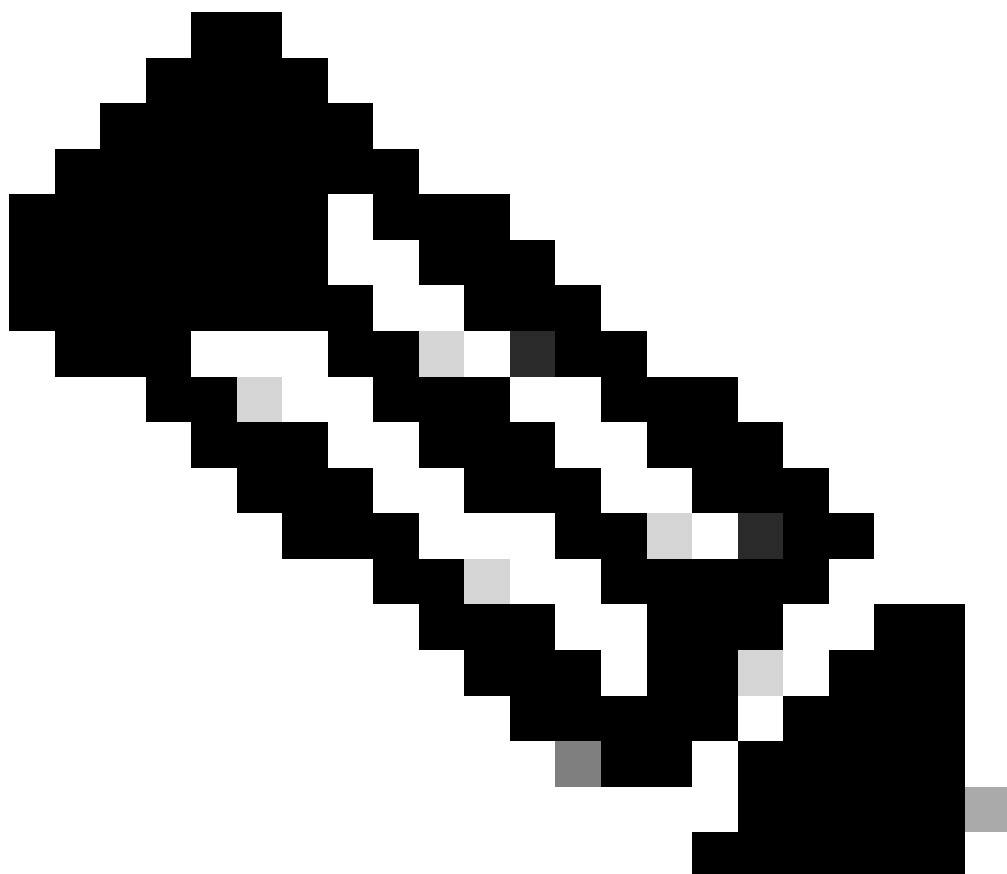
1020	10:08:11.177984	RADIUS	2075	Access-Request id=199
1021	10:08:11.177984	RADIUS	2075	Access-Request id=199, Duplicate Request
1119	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1120	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1223	10:08:21.179983	RADIUS	2075	Access-Request id=199, Duplicate Request
1224	10:08:21.179983	RADIUS	2075	Access-Request id=199, Duplicate Request
1451	10:08:26.180990	RADIUS	2075	Access-Request id=199, Duplicate Request
1452	10:08:26.180990	RADIUS	2075	Access-Request id=199, Duplicate Request
2470	10:08:31.181982	RADIUS	2075	Access-Request id=199, Duplicate Request

Captura de pacotes em WLC com aumento de MTU

Definindo a configuração dessa maneira, o controlador sem fio transmite pacotes sem fragmentá-los, enviando-os intactos. No entanto, como a nuvem do Azure não oferece suporte a quadros jumbo, essa solução não pode ser implementada.

Solução:

- A partir do Encapsulated Packet Capture (EPC) da controladora Wireless, observamos que os pacotes estão sendo enviados na ordem correta. Em seguida, é responsabilidade do host receptor remontá-los corretamente e continuar com o processamento, o que, neste caso, não ocorre no Azure.
- Para resolver o problema de pacotes UDP fora de ordem, a `enable-udp-fragment-reordering` opção precisa ser ativada no Azure.
- Você deve entrar em contato com a equipe de suporte do Azure para obter assistência sobre este assunto. A Microsoft reconheceu este problema.



Note: Deve-se observar que esse problema não é exclusivo da controladora Wireless LAN (WLC). Problemas semelhantes com pacotes UDP fora de ordem foram encontrados em diferentes servidores radius, incluindo ISE, Forti Authenticator e servidores RTSP, particularmente quando eles operam dentro do ambiente Azure.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.