FTD를 통한 액세스 포인트 인증서 기반 인증 실패 문제 해결

문제

이러한 증상은 HQ(Main Branch)에서 Cisco CSF(Secure Firewall) FTD(Threat Defense) 1230으로 Cisco Adaptive Security Appliance 5508을 마이그레이션한 후에 보고됩니다.

1. 지사에 있는 액세스 포인트(AP)가 인증서 인증을 사용하여 HQ의 RADIUS 서버에 인증하지 못합니다.

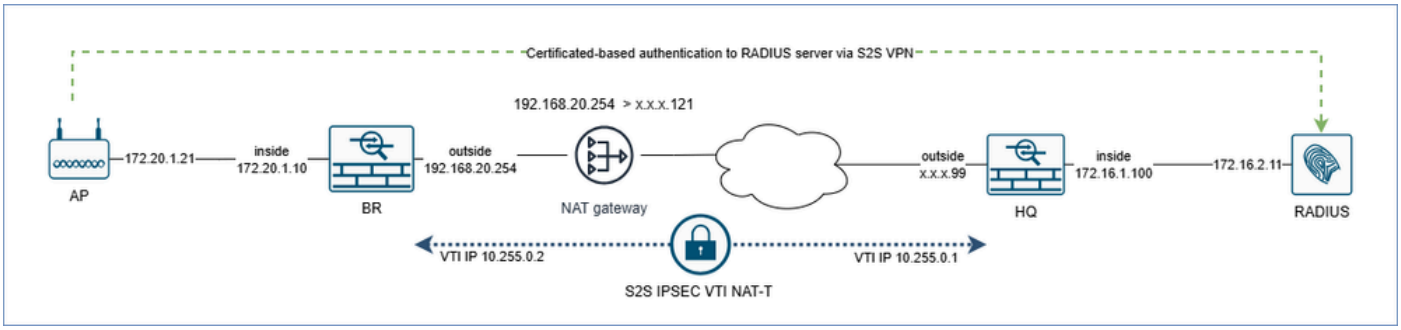
2 . 사용자 이름 및 비밀번호로 인증했습니다.

모든 지사의 액세스 포인트에서 증상이 관찰됩니다.

환경

HQ에서 버전 7.7.10.1을 실행하는 고가용성 구성의 FMC 관리 CSF 1230 및 브랜치에서 버전 7.4.2.4를 실행하는 여러 독립형 Firepower 1010, 다른 소프트웨어 버전도 영향을 받을 수 있습니다 . 이 경우 증상은 하드웨어에 구애받지 않습니다.

토폴로지



inline_image_0.png

토폴로지에 대한 주요 내용:

- 네트워크 레이어에서 액세스 포인트는 BR(브랜치) 방화벽 내부 인터페이스의 서브넷에 있습니다.
- NAT 게이트웨이로서의 라우터는 BR 방화벽 외부 인터페이스 IP 주소를 공용 주소 x.x.x.121로 변환합니다. 즉, BR 방화벽이 HQ 방화벽에서 최소 1홉 떨어져 있습니다.
- HQ와 BR 방화벽은 IPsec(Internet Protocol Security)과 ESP(Encapsulating Security Payload) 및 VTI(Virtual Tunnel Interface)를 통해 NAT를 통해 사이트 간 S2S VPN(Virtual Private Network)을 사용하여 연결됩니다.
- 네트워크 레벨에서 RADIUS 서버는 HQ 방화벽 내부 인터페이스의 서브넷에 있습니다.

해결

기술 분석을 위해 패킷 캡처를 HQ 및 BR 방화벽에서 수집했습니다.

HQ 및 BR 방화벽 데이터 플레인 인그레스/이그레스 캡처에서 물리적 인터페이스의 캡처, VTI 인터페이스의 캡처, 피어 IP 주소를 기반으로 내부 및 외부 트래픽에 대한 ASP 드롭 캡처:

BR 방화벽:

```
cap br_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap br_vti interface vti-hq packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap br_asp match ip host x.x.x.99 any
cap br_asp match ip host 172.20.1.21 host 172.16.2.11
cap br_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.99 any
```

x.x.x.99는 실제 IP 주소로 대체됩니다.

HQ 방화벽

```
cap hq_inside interface inside packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16
cap hq_vti interface vti-br packet-length 9000 buffer 33554400 match ip host 172.20.1.21 host 172.16.2.
cap hq_asp match ip host x.x.x.121 any
cap hq_asp match ip host 172.20.1.21 host 172.16.2.11
cap hq_outside interface outside packet-length 9000 buffer 33554400 match ip host x.x.x.121 any
```

x.x.x.121은 실제 IP 주소로 대체됩니다.

또한 HQ 방화벽에서는 외부 이름과 모든 업링크 인터페이스를 기반으로 섀시 인터페이스의 양방향 내부 스위치 캡처를 수집합니다.

```
cap hqfxos switch interface outside direction both packet-length 2048 match ip x.x.177.121
cap hqfxos switch interface in_data_uplink1 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink2 direction both packet-length 2048 match ip x.x.x.121
cap hqfxos switch interface in_data_uplink3 direction both packet-length 2048 match ip x.x.x.121
no cap hqfxos switch stop.
```

기술 분석

HQ 방화벽

1. HQ 방화벽의 ASP(Accelerated Security Path) 삭제 캡처는 fragment-reassembly-failed의 이유로 프래그먼트가 삭제되었음을 나타냅니다.

<#root>

>

show capture hq_asp

```
Target:     OTHER
Hardware:   CSF-1230
Cisco Adaptive Security Appliance Software Version 99.23(37)127
ASLR enabled, text region aaaae5d50000-aaaae902d504
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.38676 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
172.20.1.21.56952 > 172.16.2.11.1812:  udp 1913 Drop-reason: (fragment-reassembly-failed) Fragment reas
Drop-reason: (
```

fragment-reassembly-failed

```
) Fragment reassembly failed, Drop-location: frame snp_fh_destroy:1055 flow (NA)/NA
```

2. HQ 방화벽에서 show fragment 명령의 출력에 있는 VTI 인터페이스에 대한 Timeout 카운터가

증가합니다.

<#root>

>

show fragment

```
Interface: vti-br
    Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Run-time stats: Queue: 0, Full assembly: 0
    Drops: Size overflow: 0,
```

Timeout: 1217

```
,
            Chain overflow: 0, Fragment queue threshold exceeded: 0,
            Small fragments: 0, Invalid IP len: 0,
            Reassembly overlap: 0, Fraghead alloc failed: 0,
            SGT mismatch: 0, Block alloc failed: 0,
            Invalid IPV6 header: 0, Passenger flow assembly failed: 0
            Cluster reinsert collision: 0
```

명령 참조(https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html#wp4144096608)에 따르면 Timeout은 "프래그먼트화된 전체 패킷이 도착할 때까지 기다리는 최대 시간(초)입니다. 기본값은 5초입니다. 즉, 전체 프래그먼트 체인이 5초 이내에 방화벽에 도착하지 않으면 수신된 프래그먼트가 삭제되고 프래그먼트 리어셈블리가 실패합니다.

3. 이전 시점을 기준으로 HQ 방화벽은 프래그먼트 재결합 실패의 원인이 되는 프래그먼트의 완전한 체인을 수신하지 않습니다.

BR 방화벽

1. 캡처를 기반으로 AP는 BR 방화벽에 2개의 프래그먼트로 RADIUS 인증서 기반 인증 요청을 전송합니다. br_inside 캡처는 각각 1514바이트와 475바이트의 인그레스 프래그먼트 2개를 보여줍니다. 암호화 전에 패킷을 표시하는 BR VTI 인터페이스 캡처에도 동일한 패킷이 표시됩니다.

172.20.1.21	172.16.2.11	IPv4			1514	0xf20b (61963)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20b) [Reassembled in #9]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20b (61963)	64	Access-Request id=255
172.20.1.21	172.16.2.11	IPv4			1514	0xf20c (61964)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20c) [Reassembled in #11]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20c (61964)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20d (61965)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20d) [Reassembled in #13]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20d (61965)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20e (61966)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20e) [Reassembled in #15]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20e (61966)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf20f (61967)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f20f) [Reassembled in #17]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf20f (61967)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf210 (61968)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f210) [Reassembled in #19]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf210 (61968)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf211 (61969)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f211) [Reassembled in #21]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf211 (61969)	64	Access-Request id=255, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xf212 (61970)	64	Fragmented IP protocol (proto=UDP 17, off=0, ID=f212) [Reassembled in #23]
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xf212 (61970)	64	Access-Request id=255, Duplicate Request

inline_image_0.png

BR 외부 인터페이스 MTU(Maximum Transmission Unit)는 1500바이트입니다. 따라서 1514바이트 프래그먼트는 암호화 전에 2개의 패킷으로 프래그먼트화되어야 합니다.

2. ASP 삭제 캡처는 BR 방화벽의 내부 RADIUS 트래픽에 대해 삭제된 패킷을 표시하지 않습니다. 한편, 외부 트래픽의 경우 예기치 않은 패킷을 이유로 226바이트 패킷이 삭제됩니다.

<#root>

```
firepower#

show capture br_asp

Target:     OTHER
Hardware:   FPR-1010
Cisco Adaptive Security Appliance Software Version 9.20(2)121
ASLR enabled, text region 560817d6b000-56081d1ae26d
103 packets captured
   1: 10:13:22.160239       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
   2: 10:13:23.160727       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
   3: 10:13:24.161200       192.168.20.254.4500 > x.x.x.99.4500:  udp 184 Drop-reason: (unexpected-pack
```

192.168.20.254	.99	ESP	4500	4500	226	0x7254 (29268)	64	6275	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x7e97 (32407)	64	6278 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x0fc6 (4038)	64	6281 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x3511 (13585)	64	6284 ✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	226	0x5868 (22632)	64	6287 ✓	ESP (SPI=0x1592a843)

인라인 이미지_1.png

show capture br_asp 명령의 출력에는 184바이트의 페이로드 길이가 표시되지만 각 패킷의 총 길이는 226바이트입니다.

3. 226바이트 삭제 ESP 패킷이 AP와 RADIUS 서버 간의 영향을 받는 트래픽과 관련이 있는지 확인하기 위해 HQ 및 BR 방화벽의 동일한 보안 정책 컨피그레이션을 사용하여 내부 랩에서 br_inside 캡처를 재생했습니다. 랩 디바이스에서 br_vti 캡처는 1514바이트 및 475바이트 프래그먼트를 보여주는데, 이는 암호화 이전입니다.

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	Info
172.20.1.21	172.16.2.11	IPv4			1514	0xe69d (59037)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69d) [Reassembled in #9
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69d (59037)	63	Access-Request id=218
172.20.1.21	172.16.2.11	IPv4			1514	0xe69e (59038)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69e) [Reassembled in #11
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69e (59038)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe69f (59039)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e69f) [Reassembled in #13
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe69f (59039)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a0 (59040)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a0) [Reassembled in #15
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a0 (59040)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a1 (59041)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a1) [Reassembled in #17
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a1 (59041)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a2 (59042)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a2) [Reassembled in #19
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a2 (59042)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a3 (59043)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a3) [Reassembled in #21
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a3 (59043)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a4 (59044)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a4) [Reassembled in #23
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a4 (59044)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a5 (59045)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a5) [Reassembled in #25
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a5 (59045)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a6 (59046)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a6) [Reassembled in #27
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a6 (59046)	63	Access-Request id=218, Duplicate Request
172.20.1.21	172.16.2.11	IPv4			1514	0xe6a7 (59047)	63	Fragmented IP protocol (proto=UDP 17, off=0, ID=e6a7) [Reassembled in #29
172.20.1.21	172.16.2.11	RADIUS	56952	1812	475	0xe6a7 (59047)	63	Access-Request id=218, Duplicate Request

inline_image_2.png

4. br_outside 캡처는 226바이트 패킷의 부족 및 562바이트와 1506바이트 패킷 간의 ESP 시퀀스 번호의 간격을 보여줍니다.

Source	Destination	Protocol	Sport	Dport	Length	IP ID	IP TTL	ESP Sequence	Wrong Sequence Number	Info
192.168.20.254	.99	ESP	4500	4500	1506	0x2d7e (11646)	64	6448		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x0b2c (2860)	64	6450	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x6ca9 (27817)	64	6451		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x51cf (20943)	64	6453	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x7d60 (32096)	64	6454		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x42de (17118)	64	6456	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x4553 (17747)	64	6457		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x7389 (29577)	64	6459	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	1506	0x50f9 (20729)	64	6460		ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	562	0x169f (5791)	64	6462	✓	ESP (SPI=0x1592a843)
192.168.20.254	.99	ESP	4500	4500	178	0x32d8 (13016)	64	6463		ESP (SPI=0x1592a843)

inline_image_3.png

요점:

- 226바이트가 br_outside 캡처에 없습니다. 예기치 않은 패킷 ASP 삭제 이유로 BR 방화벽 ASP에서 삭제되기 때문입니다.
- 패킷 삭제는 ESP 시퀀스 번호의 간격을 설명합니다.
- 또한, 범위에서 누락된 시퀀스 번호는 226바이트 ESP 패킷이 BR 방화벽에 의해 생성되었지만 외부 인터페이스 외부로 전송되지 않았음을 의미합니다.
- 226바이트 패킷이 BR 방화벽 외부 인터페이스 외부로 전송되지 않았기 때문에 HQ 방화벽은 이를 수신하지 못했습니다.
- HQ 방화벽에 226바이트 패킷이 없기 때문에 "HQ 방화벽 섹션"에 표시된 프래그먼트 리어셈블리 오류가 발생했습니다.

설명

기술 분석 섹션의 결과는 Cisco 버그 ID CSCwp10123의 증상과 일치합니다.

ESP 패킷을 생성하여 이그레스 인터페이스 외부로 전송하기 위한 방화벽 작업에 대한 대략적인 개요:

1. 방화벽은 VTI 터널을 통해 전송되어야 하는 프래그먼트된 패킷을 수신합니다.
2. 내부 패킷의 길이가 인터페이스 MTU 크기에서 IPSEC 오버헤드를 뺀 값보다 크면 패킷이 프래그먼트화됩니다.
3. 라우팅 테이블 조회를 기반으로 다음 홉을 찾습니다. VTI의 경우 다음 홉은 피어 VTI IP 주소입니다.

4. 터널 대상 주소에 따라 이그레스 인터페이스와 다음 홉이 식별됩니다(예: 외부 인터페이스).
5. 원래 패킷은 ESP 패킷 내부에서 캡슐화됩니다.
6. 3단계의 다음 홉에 대한 인접성 조회가 수행되며 패킷은 이그레스(egress) 인터페이스로 전송됩니다.

Cisco 버그 ID CSCwp10123으로 인해, 4단계에서 후속 ESP 캡슐화 조각(비초기) 패킷에 대해 새 경로 조회가 수행됩니다. 방화벽에 피어 IP 주소(또는 서브넷)에 대한 더 구체적인 경로가 있으면 초기 패킷의 경로 대신 새 경로가 사용됩니다. 이 예에서 HQ 방화벽 인터페이스 IP 주소는 x.x.x.99입니다. HQ 방화벽은 VTI를 통해 실행되는 BGP(Border Gateway Protocol)를 통해 BR 방화벽에 외부 서브넷을 광고합니다.

```
<#root>

>

show route bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRFGateway of last resort is 192.168.20.1 to network 0.0.0.0

B        x.x.x.96 255.255.255.224 [20/0] via 10.255.0.1, 13:57:43

<--BR firewall learns /27 route via BGP over VTI
```

```
<#root>

>

show bgp summary

BGP router identifier 192.168.179.10, local AS number 65001
BGP table version is 25, main routing table version 25
23 network entries using 4600 bytes of memory
24 path entries using 1920 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6960 total bytes of memory
BGP activity 23/0 prefixes, 24/0 paths, scan interval 60 secs
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

10.255.0.1      4        65000 762     761          25    0    0 13:59:01  18
```

```
>

show ip

…
Tunnel1                    vti-hq                  10.255.0.2      255.255.255.252 CONFIG <--

10.255.0.1

 is the peer VTI IP
…
```

```
<#root>

>

show ip

…
Tunnel1                    vti-hq                  10.255.0.2      255.255.255.252 CONFIG <--

10.255.0.1

 is the peer VTI IP in the same subnet
…
```

1514바이트 ESP 패킷이 외부 인터페이스로 전송됩니다. 그러나 226바이트의 경우 3단계의 방화벽이 경로 조회를 수행하고 VTI를 통해 피어 IP 주소로 향하는 특정 경로를 찾습니다. 즉, 방화벽은 VPN 종단 인터페이스에서 패킷을 전송하는 대신 VTI 인터페이스를 사용하여 VTI 인터페이스의 인접성을 확인합니다. VTI 인터페이스에는 인접성의 개념이 없으므로 예기치 않은 패킷 삭제 이유와 함께 패킷이 삭제됩니다.

이를 해결하기 위해 CSF1230에서 사용자가 경로 맵에 ACL(access-list)을 포함했습니다. 정책 구축 후 ACL이 HQ 외부 서브넷을 거부하여 BGP 라우팅에서 HQ 외부 서브넷의 전파를 효과적으로 제거합니다. 이러한 변경으로 인해 BR 방화벽은 터널 인터페이스를 통해 HQ 외부 서브넷 접두사를 수신하지 않습니다.

ASA에서 보안 방화벽으로 마이그레이션한 후 266바이트 패킷이 삭제되는 이유는 무엇입니까?

ASA 방화벽 컨피그레이션은 HQ 외부 인터페이스 서브넷이 브랜치로 전파되는 것을 명시적으로 차단했습니다.

ASA5508

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 10
 match ip address bgp-connected-routes
access-list bgp-connected-routes standard deny x.x.x.96 255.255.255.224 <-- deny = do not redistribute
```

CSF1230

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 40 <-- No match, means redistribute all connected routes
```

원인

이 문제는 원래 ASA 5508과 새 FTD 1230 간의 BGP 경로 재배포의 컨피그레이션 차이로 인해 발생했습니다. ASA 5508에는 x.x.x.96/27 서브넷의 재배포를 거부하는 액세스 제어 목록이 있는 반면, FTD 1230은 연결된 모든 경로를 재배포하도록 구성되었습니다. 이러한 컨피그레이션 차이로 인해 Cisco 버그 ID CSCwp10123이 트리거되었습니다.

관련 콘텐츠

- Cisco 버그 ID CSCwp10123

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.