通过FTD排除接入点基于证书的身份验证故障

问题

在主分支机构(HQ)将思科自适应安全设备5508迁移到思科安全防火墙(CSF)威胁防御(FTD)1230之后报告以下症状：

1. 位于分支机构的无线接入点(AP)无法使用证书身份验证向HQ中的RADIUS服务器进行身份验证。

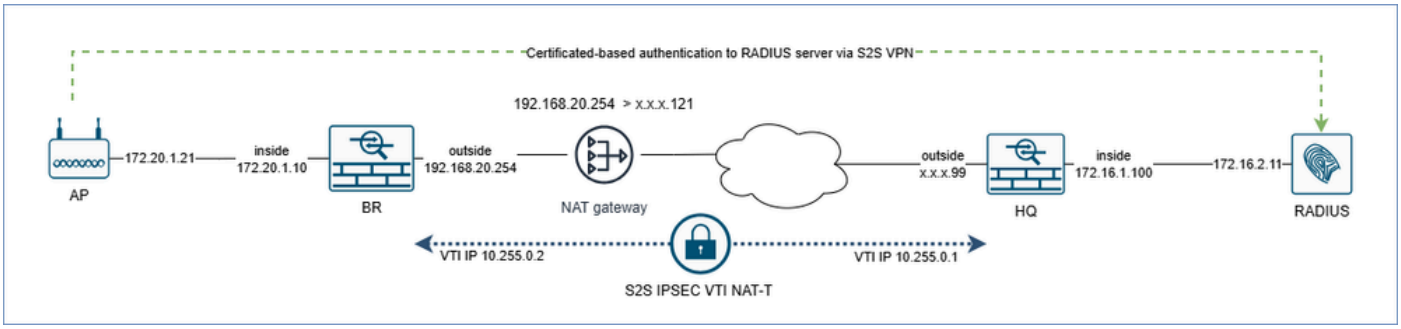
2. 使用用户名和密码的身份验证成功。

观察所有分支机构中接入点的故障症状。

环境

FMC管理的CSF 1230在高可用性配置中运行7.7.10.1版本（总部），多个独立Firepower 1010运行7.4.2.4版本（分支），其他软件版本也可能受到影响。此案例中的症状与硬件无关。

拓扑



inline_image_0.png

有关拓扑的关键点：

- 在网络层，接入点位于BR（分支）防火墙内部接口的子网中。

- 作为NAT网关的路由器将BR防火墙外部接口IP地址转换为公有地址x.x.x.121。这意味着BR防火墙至少与HQ防火墙相距1跳。
- HQ和BR防火墙使用具有封装安全负载(ESP)的互联网协议安全(IPsec)和通过NAT的虚拟隧道接口(VTI)，使用站点到站点虚拟专用网络(S2S VPN)进行连接。
- 在网络级别，RADIUS服务器位于HQ防火墙内部接口的子网中。

分辨率

为进行技术分析，从HQ和BR防火墙收集数据包捕获。

在HQ和BR防火墙上，根据对等IP地址捕获物理接口上的入口/出口捕获、VTI接口上的捕获、内部和外部流量的ASP丢弃捕获：

BR防火墙：

```
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
```

请注意，x.x.x.99替换为实际IP地址。

HQ防火墙：

```
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
```

请注意，x.x.x.121替换为实际IP地址。

此外，在HQ防火墙上，根据outside nameif和所有上行链路接口收集机箱接口中的双向内部交换机捕获：

```
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.
```

技术分析

HQ防火墙

1. HQ防火墙中的加速安全路径(ASP)丢弃捕获表示丢弃分段的原因为fragment-reassembly-failed:

<#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防火墙中的show fragment命令输出中的VTI接口的Timeout计数器增加：

<#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
```

根据命令参考(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),Timeout是“等待整个分段数据包到达的最长秒数”(The maximum number of seconds to wait for a entire fraged packet to reached)。 默认值为 5 秒。这意味着，如果整个分段链在5秒内未到达防火墙，收到的分段将被丢弃，并且分段重组失败。

3. 根据上一点，HQ防火墙不会收到导致分段重组失败的完整分段链。

BR防火墙

1. 根据捕获，AP将分成2个不同的分段向BR防火墙发送基于RADIUS证书的身份验证请求。br_inside捕获显示2个入口分段，分别为1514个字节和475个字节。在BR VTI接口捕获中也会看到相同的数据包，这些数据包在加密之前显示数据包：

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外部接口最大传输单位(MTU)为1500字节。因此，在加密之前，1514字节的分段必须分成2个数据包。

2. ASP丢弃捕获br_asp用于BR防火墙上的内部RADIUS流量，但不会显示丢弃的数据包。同时，对于外部流量，会丢弃226字节的数据包，原因为unexpected-packet:

<#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)

inline_image_1.png

请注意，show capture br_asp命令的输出显示184 bytes of payload length，而每个数据包的总长度为226 bytes。

3. 为了验证226字节丢弃的ESP数据包是否与AP和RADIUS服务器之间受影响的流量相关，在内部实验室中使用来自HQ和BR防火墙的相同安全策略配置重播br_inside捕获。来自实验设备的br_vti捕获显示1514字节和475字节分段，即加密之前：

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 #1
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 #1
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 #1
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 #1
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 #1
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 #2
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 #2
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 #2
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 #2
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 #2
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捕获显示，缺少226字节数据包，并且562字节和1506字节数据包之间的ESP序列号存在间隙：

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

关键点

- br_outside捕获中缺少226字节，因为它在BR防火墙ASP中丢弃，并具有意外数据包ASP丢弃原因。
- 数据包丢弃说明了ESP序列号中的间隙。
- 此外，范围中缺少序列号意味着226字节的ESP数据包由BR防火墙生成，但未从外部接口发送。
- 由于226字节的数据包未从BR防火墙外部接口发出，因此HQ防火墙从未收到过该数据包。
- HQ防火墙中缺少226字节的数据包会导致分片重组失败，如“HQ防火墙部分”所示。

说明

技术分析部分的发现结果与Cisco Bug ID CSCwp10123的症状相符。

有关生成ESP数据包并将其从出口接口传输的防火墙操作的高级概述：

1. 防火墙接收应该通过VTI隧道发送的零碎数据包。
2. 如果内部数据包的长度大于接口MTU大小减去IPSEC开销，则数据包被分段。
3. 根据路由表查找找到下一跳。对于VTI，下一跳是对等VTI IP地址。
4. 根据隧道目的地址，标识出口接口和下一跳（例如，外部接口）。
5. 原始数据包封装在ESP数据包内。
6. 从步骤3开始执行下一跳的邻接查找并将数据包从出口接口发送出去。

由于Cisco Bug ID CSCwp10123，因此在第4步中，对后续ESP封装分段（非初始）数据包执行新的路由查找。如果防火墙有指向对等IP地址（或子网）的更具体的路由，则使用新路由而不是初始数据包的路由。在本示例中，HQ防火墙接口IP地址为x.x.x.99。HQ防火墙通过在VTI上运行的边界网关协议(BGP)向BR防火墙通告其外部子网：

<#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
…
```

1514字节的ESP数据包从外部接口发出。但是，对于长度为226字节的IP，防火墙在步骤3中执行路由查找，并查找通过VTI到达对等IP地址的特定路由。换句话说，防火墙使用VTI接口并尝试解析VTI接口上的邻接关系，而不是从VPN终端接口发送数据包。由于VTI接口没有邻接概念，因此数据包最终会由于意外数据包丢弃原因而被丢弃。

解决方法是，在CSF1230上，用户将访问列表(ACL)包括在路由映射中。在策略部署后，ACL拒绝了HQ外部子网，从而有效地从BGP路由删除HQ外部子网的传播。由于此更改，BR防火墙不会通过隧道接口接收HQ外部子网前缀。

从ASA迁移至安全防火墙后，为什么会丢弃266字节的数据包？

ASA防火墙配置明确阻止了HQ外部接口子网向分支的传播：

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
```

原因

问题是由原始ASA 5508和新的FTD 1230之间的BGP路由重分配配置差异触发的。ASA 5508有一个访问控制列表，该列表拒绝重分发x.x.x.96/27子网，而FTD 1230配置为重分发所有连接的路由。此配置差异触发了Cisco Bug ID CSCwp10123。

相关内容

- Cisco Bug ID CSCwp10123

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。