透過FTD解決存取點憑證型驗證失敗問題

問題

將思科調適型安全裝置5508遷移到主分支(HQ)中的思科安全防火牆(CSF)威脅防禦(FTD)1230後會報告以下症狀：

1. 位於分支機構中的接入點(AP)無法使用證書身份驗證向HQ中的RADIUS伺服器進行身份驗證。

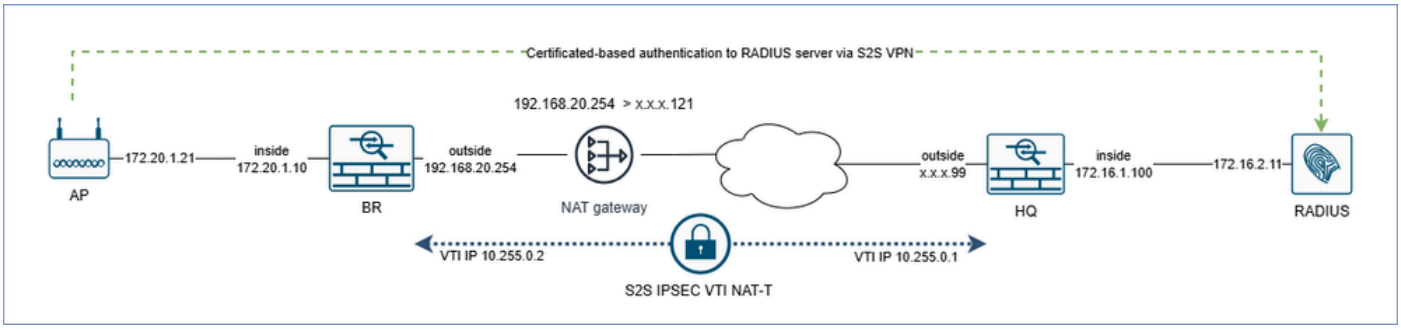
2. 使用使用者名稱和密碼的身份驗證成功。

觀察所有分支中的接入點症狀。

環境

FMC管理的CSF 1230在高可用性配置中運行版本7.7.10.1（總部），多個獨立Firepower 1010運行版本7.4.2.4（分支），其他軟體版本也可能受到影響。此案例中的症狀與硬體無關。

拓撲



inline_image_0.png

有關拓撲的關鍵點：

- 在網路層，接入點位於BR（分支）防火牆內部介面的子網中。

- 作為NAT網關的路由器將BR防火牆外部介面IP地址轉換為公共地址x.x.x.121。這表示BR防火牆與HQ防火牆至少相距1跳。
- HQ和BR防火牆使用點對點虛擬專用網路(S2S VPN)連線，使用具有封裝安全負載(ESP)的網際網路協定安全(IPsec)和通過NAT的虛擬隧道介面(VTI)。
- 在網路級別，RADIUS伺服器位於HQ防火牆內部介面的子網中。

解析

為進行技術分析，從HQ和BR防火牆收集資料包捕獲。

在HQ和BR防火牆資料平面上，物理介面上的輸入/輸出捕獲、VTI介面上的捕獲、基於對等IP地址的內部和外部流量的ASP丟棄捕獲：

BR防火牆：

```
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
```

請注意，x.x.x.99已替換為實際IP地址。

總部防火牆：

```
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
```

請注意，x.x.x.121將替換為實際IP地址。

此外，在HQ防火牆上，根據outside nameif和所有上行鏈路介面收集機箱介面中的雙向內部交換機捕獲：

```
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.
```

技術分析

總部防火牆

1. HQ防火牆中的加速安全路徑(ASP)丟棄捕獲指示丟棄了碎片，原因為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防火牆的show fragment命令輸出中的VTI介面的Timeout計數器增加：

<#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
```

根據命令參考(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「等待整個分段資料包到達的最大秒數」。 預設值為 5 秒.這表示如果整個片段鏈在5秒內未到達防火牆，則系統會捨棄接收的片段，且片段重組失敗。

3. 根據上一點，HQ防火牆不會收到導致分段重組失敗的完整分段鏈。

BR防火牆

1. 根據擷取，AP會將2個獨立的片段中的RADIUS憑證型驗證要求傳送到BR防火牆。br_inside擷取顯示2個輸入片段，分別為1514位元組和475位元組。BR VTI介面擷取中顯示的封包在加密前相同：

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外部介面最大傳輸單元(MTU)為1500位元組。因此，在加密之前，1514位元組的片段必須分段為2個封包。

2. ASP drop captures br_asp（針對BR防火牆上的內部RADIUS流量）不會顯示丟棄的資料包。同時，對於外部流量，會丟棄226位元組的封包，原因為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

請注意，show capture br_asp命令的輸出顯示184位元組的負載長度，而每個封包的總長度為226位元組。

3. 為了驗證226位元組丟棄的ESP封包是否與AP和RADIUS伺服器之間的受影響流量相關，已在內部實驗室使用來自HQ和BR防火牆的相同安全原則設定重播br_inside擷取。來自實驗裝置的br_vti捕獲顯示1514位元組和475位元組的片段，即在加密之前：

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擷取顯示缺少226位元組封包，且562位元組和1506位元組封包之間的ESP序號差異：

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

重點：

- br_outside捕獲中缺少226位元組，因為它在BR防火牆ASP中因意外包ASP丟棄原因被丟棄。
- 資料包丟棄說明了ESP序列號中的差距。
- 此外，此範圍中缺少序列號意味著226位元組的ESP資料包由BR防火牆生成，但未從外部介面傳輸。
- 由於226位元組的資料包沒有從介面外部的BR防火牆發出，因此HQ防火牆從未收到該資料包。
- HQ防火牆中缺少226位元組的資料包會導致分段重組失敗，如「HQ防火牆部分」中所示。

說明

技術分析一節中的發現結果與Cisco錯誤ID CSCwp10123的症狀相符。

有關生成ESP資料包並將其從輸出介面傳輸的防火牆操作的高級概述：

1. 防火牆收到應該透過VTI通道傳送的零碎封包。
2. 如果內部封包的長度大於介面MTU大小減去IPSEC額外負荷，則會將封包分段。
3. 根據路由表查詢，找到下一跳。對於VTI，下一跳是對等VTI IP地址。
4. 根據通道目的地位址，識別輸出介面和下一躍點（例如外部介面）。
5. 原始資料包將封裝在ESP資料包中。
6. 從步驟3開始執行下一躍點的鄰接查詢，並將資料包從輸出介面傳送出去。

由於Cisco錯誤ID CSCwp10123，因此對於後續的ESP封裝片段（非初始）封包，會在步驟4執行新路由查詢。如果防火牆具有到對等體IP地址（或子網）的更具體的路由，則使用新路由而不是初始資料包的路由。在本示例中，HQ防火牆介面IP地址為x.x.x.99。HQ防火牆通過在VTI上運行的邊界網關協定(BGP)向BR防火牆通告其外部子網：

<#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位元組的ESP資料包從外部介面發出。但是對於長度為226位元組的IP，防火牆在步驟3執行路由查詢，並找到通過VTI到達對等IP地址的特定路由。換句話說，防火牆使用VTI介面並嘗試解析VTI介面上的鄰接關係，而不是從VPN終端介面傳送資料包。由於VTI介面沒有鄰接概念，因此最終會使用意外資料包丟棄原因來丟棄資料包。

因應措施是，在CSF1230上，使用者在路由對映中包含存取清單(ACL)。在策略部署之後，ACL拒絕了HQ外部子網，從而有效地從BGP路由中刪除HQ外部子網的傳播。由於此更改，BR防火牆不會通過隧道介面接收HQ外部子網字首。

從ASA遷移至安全防火牆後，為什麼會丟棄266位元組的資料包？

ASA防火牆配置明確阻止了HQ外部介面子網向分支的傳播：

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

問題是由原始ASA 5508和新的FTD 1230之間的BGP路由重分佈配置差異觸發的。ASA 5508有一個訪問控制清單，該清單拒絕重分發x.x.x.96/27子網，而FTD 1230配置為重分發所有連線的路由。此組態差異已觸發思科錯誤ID CSCwp10123。

相關內容

- 思科錯誤ID CSCwp10123

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。