Troubleshoot Access Point Certificate-Based Authentication Failure Through FTD

Contents

Issue

These symptoms are reported after the migration of Cisco Adaptive Security Appliance 5508 to Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 in the main branch (HQ):

1. The access points (AP) located in the branch offices fail to authenticate to the RADIUS server in HQ using certificate authentication.

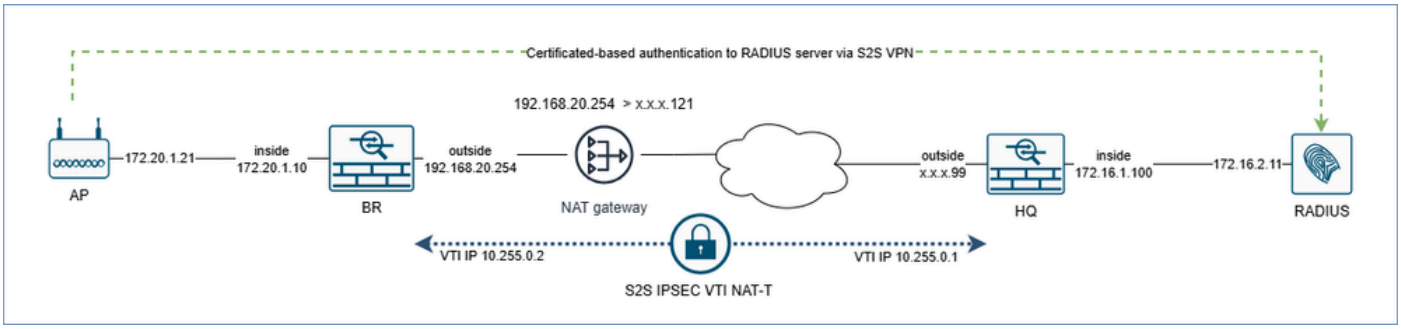
2. Authentication with username and password is successful.

The symptoms are observed for access points in all branches.

Environment

FMC-managed CSF 1230 in high availability configuration running version 7.7.10.1 in HQ and multiple standalone Firepower 1010 running version 7.4.2.4 in branches, other software version can also be affected. The symptoms in this case are hardware agnostic.

Topology



inline_image_0.png

Key points about the topology:

- At network layer, the access point is in the subnet of the BR (branch) firewall inside interface.
- The router as a NAT gateway translates the BR firewall outside interface IP address to a public address **x.x.x.121.** This means the BR firewall is at least 1 hop away from the HQ firewall.
- HQ and BR firewalls are connected using Site-to-Site Virtual Private Networks (S2S VPN) using Internet Protocol Security (IPsec) with Encapsulating Security Payload (ESP) and the Virtual Tunnel Interface (VTI) over NAT.
- At the network level, the RADIUS server is in the subnet of the HQ firewall inside interface.

Resolution

For technical analysis the packet captures were collected from the HQ and BR firewalls.

On HQ and BR firewall data plane ingress/egress captures on physical interfaces, capture on VTI interfaces, ASP drop captures for inner and outer traffic based on the peer IP address:

BR firewall:

```
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
```

Note that **x.x.x.99** is substituted with an actual IP address.

HQ firewall:

```
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
```

Note that **x.x.x.121** is substituted with an actual IP address.

Additionally, on HQ firewall collect bidirectional internal switch captures in chassis interfaces based on the

outside nameif and all uplink interfaces:

```
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.
```

Technical Analysis

HQ Firewall

1. The Accelerated Security Path (ASP) drop captures in HQ firewall indicate that fragments are dropped with the reason **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. The **Timeout** counter for the VTI interface in the output of the **show fragment** command in HQ firewall increases:

<#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
```

According to the command reference (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), the **Timeout** is "The maximum number of seconds to **wait for an entire fragmented packet to arrive"**. The default value is 5 seconds. This means if the entire fragment chain does not arrive at the firewall within **5** seconds, the received fragments are dropped, and fragment reassembly fails.

3. Based on the previous point, the HQ firewall does not receive the complete chain of fragment that results in fragment reassembly failure.

BR Firewall

1. Based on the captures, the AP sends RADIUS certificate-based authentication request in 2 separate fragments to the BR firewall. The **br_inside** capture shows 2 ingress fragments of **1514** bytes and **475** bytes respectively. The same packets are seen in the BR VTI interface captures that show packet before encryption:

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

The BR outside interface Maximum Transmission Unit (MTU) is 1500 bytes. Due to this reason, the 1514-byte fragment must be fragmented into 2 packets before encryption.

2. ASP drop captures **br_asp** for inner RADIUS traffic on BR firewall do not show dropped packets. Meanwhile, for outer traffic, there are drops of 226-byte packets with the reason **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

Note that the output of the **show capture br_asp** command shows **184** bytes of payload length, while the total length of each packet is **226** bytes.

3. To verify if 226-byte dropped ESP packets are relevant to the affected traffic between AP and the RADIUS server, the **br_inside** capture was replayed in the internal lab using same security policy configurations from HQ and BR firewalls. The **br_vti** capture from the lab device shows **1514**-byte and **475**-byte fragments, that is before encryption:

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. The **br_outside** captures show the lack of 226-byte packets and the gap in ESP sequence numbers between the 562-byte and 1506-byte packets:

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

Key Points

- 226-byte is missing in the **br_outside** capture, because it is dropped in the BR firewall ASP with the **unexpected-packet** ASP drop reason.
- The packet drop explains the gap in the ESP sequence numbers.
- Additionally, the missing sequence number in the range means that the 226-byte ESP packet was generated by the BR firewall but not transmitted out the outside interface.
- Since the 226-byte packet was not sent out the BR firewall outside interface, the HQ firewall never received it.
- The lack of the 226-byte packet in the HQ firewall resulted in the fragment reassembly failure as show in the “HQ firewall section”.

Explanation

The findings from the technical analysis section match the symptoms of the Cisco bug ID CSCwp10123.

High lever overview of the firewall actions to generate ESP packets and transmitted them out the egress interface:

1. The firewall receives fragmented packets that are supposed to be sent via the VTI tunnel.
2. If the length of the inner packet is greater than the interface MTU size minus the IPSEC overhead, then the packet is fragmented.
3. Based on the routing table lookup the next hop is found. In the case of the VTI, the next hop is the peer VTI IP address.
4. Based on the tunnel destination address the egress interface and the next hop are identified (for example, outside interface).
5. The original packets are encapsulated inside ESP packets.
6. Adjacency lookup for the next hop from step 3 is performed and packets are sent out the egress interface.

Due to Cisco bug ID CSCwp10123, for subsequent ESP-encapsulated fragments (non-initial) packets at step

4 new route-lookup is performed. If the firewall has more specific routes to the peer IP address (or subnet), then the new route are used instead of the route for the initial packet. In this example, the HQ firewall interface IP address is x.x.x.99. The HQ firewall advertises its outside subnet to the BR firewall via the Border Gateway Protocol (BGP) running over the VTI:

<#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
…
```

The 1514-byte ESP packet is sent out the outside interface. But for the 226-byte the firewall at step 3 performs a route-lookup and finds specific route toward the peer IP address via the VTI. In other words, instead of sending the packets out the VPN-terminating interface, the firewall uses VTI interface and tries to resolve the adjacency on the VTI interface. Since the VTI interfaces do not have a concept of adjacency, the packets are eventually be dropped with the unexpected-packet drop reason.

As a workaround, on CSF1230 the user included the access-list (ACL) in the route-map. After policy deployment, the ACL denied HQ outside subnet, effectively removing the propagation of HQ outside subnet from BGP routing. Due to this change, the BR firewalls do not receive HQ outside subnet prefix over the tunnel interface.

Q: Why are 266-byte packets dropped after the migration from ASA to Secure Firewall?

A: The ASA firewall configuration explicitly blocked the propagation of the HQ outside interface subnet to the branches.

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
```

Cause

The issue was triggered by a configuration difference in BGP route redistribution between the original ASA 5508 and the new FTD 1230. The ASA 5508 had an access control list that denied redistribution of the x.x.x.96/27 subnet, while the FTD 1230 was configured to redistribute all connected routes. This configuration difference triggered Cisco bug ID CSCwp10123.

Related Content

- Cisco bug ID CSCwp10123