Problemen met op certificaten gebaseerde verificatie van toegangspunten oplossen via FTD

uitgeven

Deze symptomen worden gemeld na de migratie van Cisco Adaptive Security Appliance 5508 naar Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 in de hoofdvestiging (HQ):

1. De toegangspunten (AP's) in de filialen kunnen zich niet met behulp van certificaatverificatie verifiëren bij de RADIUS-server in het hoofdkantoor.

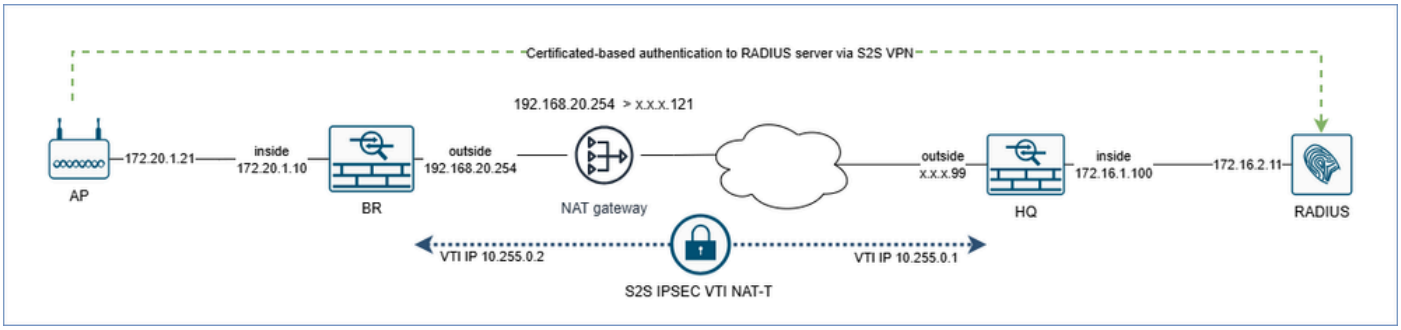
2. De verificatie met gebruikersnaam en wachtwoord is geslaagd.

De symptomen worden waargenomen voor toegangspunten in alle takken.

milieu

FMC-beheerde CSF 1230 in configuratie met hoge beschikbaarheid met versie 7.7.10.1 in hoofdkwartier en meerdere zelfstandige Firepower 1010 met versie 7.4.2.4 in filialen, kan ook van invloed zijn op andere softwareversies. De symptomen zijn in dit geval hardware-agnostisch.

Topologie



inline_image_0.png

Belangrijkste punten over de topologie:

- Op de netwerklaag bevindt het toegangspunt zich in het subnet van de BR (branch) firewall inside interface.
- De router als een NAT-gateway vertaalt de BR-firewall buiten het IP-adres naar een openbaar adres x.x.x.121. Dit betekent dat de BR-firewall ten minste 1 stap verwijderd is van de HQ-firewall.
- HQ- en BR-firewalls zijn verbonden via Site-to-Site Virtual Private Networks (S2S VPN) met behulp van Internet Protocol Security (IPsec) met Encapsulating Security Payload (ESP) en de Virtual Tunnel Interface (VTI) via NAT.
- Op netwerkniveau bevindt de RADIUS-server zich in het subnet van de HQ-firewall in de interface.

resolutie

Voor technische analyse werden de pakketopnames verzameld van de HQ- en BR-firewalls.

Op HQ en BR firewall data plane ingress/egress captures op fysieke interfaces, capture op VTI interfaces, ASP drop captures voor binnen- en buitenverkeer op basis van het peer IP-adres:

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
```

Merk op dat x.x.x.99 wordt vervangen door een echt IP-adres.

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
```

Merk op dat x.x.x.121 wordt vervangen door een echt IP-adres.

Bovendien kunt u op de HQ-firewall bidirectionele interne switch-opnames verzamelen in chassisinterfaces op basis van de naam van de buitenkant en alle uplinkinterfaces:

```
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.
```

technische analyse

HQ Firewall

1. De vervolgopnamen van het versnelde beveiligingspad (ASP) in de firewall van het hoofdkwartier geven aan dat fragmenten zijn weggelaten, met als reden dat het opnieuw samenstellen van fragmenten is mislukt:

<#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. De time-outteller voor de VTI-interface in de uitvoer van de opdracht fragment weergeven in de HQ-firewall wordt verhoogd:

<#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
```

Volgens de opdrachtverwijzing (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) is de Timeout "het maximale aantal seconden dat moet wachten voordat een volledig gefragmenteerd pakket arriveert". De standaardwaarde is 5 seconden. Dit betekent dat als de gehele fragmentketen niet binnen 5 seconden bij de firewall aankomt, de ontvangen fragmenten worden verwijderd en de fragmenthermontage mislukt.

3. Op basis van het vorige punt ontvangt de HQ-firewall niet de volledige fragmentatieketen die resulteert in een mislukte hermontage van fragmenten.

BR Firewall

1. Op basis van de vastgelegde gegevens verzendt het toegangspunt een op RADIUS-certificaten gebaseerd verificatieverzoek in twee afzonderlijke fragmenten naar de BR-firewall. De br_inside opname toont 2 ingress fragmenten van respectievelijk 1514 bytes en 475 bytes. Dezelfde pakketten zijn te zien in de BR VTI-interfaceopnames die pakketversleuteling tonen:

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

De BR outside interface Maximum Transmission Unit (MTU) is 1500 bytes. Om deze reden moet het 1514-byte-fragment worden gefragmenteerd in 2 pakketten voordat codering plaatsvindt.

2. ASP drop captures br_asp voor binnenste RADIUS verkeer op BR firewall tonen geen gedropte pakketten. Ondertussen zijn er voor buitenverkeer druppels van 226-byte-pakketten met de reden onverwacht-pakket:

<#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

Merk op dat de uitvoer van de opdracht show capture br_asp 184 bytes aan payloadlengte toont, terwijl de totale lengte van elk pakket 226 bytes is.

3. Om te controleren of 226-byte gevallen ESP-pakketten relevant zijn voor het getroffen verkeer tussen AP en de RADIUS-server, werd de br_inside-opname opnieuw afgespeeld in het interne lab met dezelfde configuraties voor het beveiligingsbeleid van HQ- en BR-firewalls. De br_vti-opname van het laboratoriumapparaat toont 1514-byte- en 475-byte-fragmenten, dat wil zeggen vóór de codering:

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. De br_outside-opnames tonen het ontbreken van 226-byte-pakketten en de kloof in ESP-volgnummers tussen de 562-byte- en 1506-byte-pakketten:

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

Belangrijkste punten:

- 226-byte ontbreekt in de br_outside-opname, omdat deze in de BR-firewall ASP is gedropt met de onverwachte ASP-dropreden voor het pakket.
- De pakketdrop verklaart de kloof in de ESP-volgnummers.
- Bovendien betekent het ontbrekende volgnummer in het bereik dat het 226-byte ESP-pakket is gegenereerd door de BR-firewall, maar niet is verzonden via de externe interface.
- Aangezien het pakket van 226 bytes niet buiten de interface van de BR-firewall werd verzonden, heeft de HQ-firewall het nooit ontvangen.
- Het ontbreken van het 226-byte pakket in de HQ firewall resulteerde in de fragment reassembly mislukking zoals te zien in de "HQ firewall sectie".

verklaring

De bevindingen uit de sectie technische analyse komen overeen met de symptomen van de Cisco-bug ID CSCwp10123.

Hefboomoverzicht van de firewallacties om ESP-pakketten te genereren en deze via de uitgang-interface te verzenden:

1. De firewall ontvangt gefragmenteerde pakketten die via de VTI-tunnel zouden moeten worden verzonden.
2. Als de lengte van het binnenste pakket groter is dan de grootte van de interface MTU minus de IPSEC-overhead, dan is het pakket gefragmenteerd.
3. Op basis van de routeringstabel wordt de volgende hop gevonden. In het geval van de VTI is de volgende stap het peer-VTI IP-adres.
4. Op basis van het tunnelbestemmingsadres worden de uitgang en de volgende hop geïdentificeerd (bijvoorbeeld de buiteninterface).
5. De originele pakketten zijn ingekapseld in ESP-pakketten.
6. Adjacency lookup voor de volgende hop van stap 3 wordt uitgevoerd en pakketten worden verzonden uit de uitgang interface.

Vanwege Cisco bug ID CSCwp10123, wordt voor volgende ESP-ingekapselde fragmenten (niet-initiële) pakketten bij stap 4 een nieuwe route-opzoeking uitgevoerd. Als de firewall meer specifieke routes heeft naar het peer-IP-adres (of subnet), wordt de nieuwe route gebruikt in plaats van de route voor het eerste pakket. In dit voorbeeld is het IP-adres van de HQ-firewallinterface x.x.x.99. De HQ-firewall adverteert zijn externe subnet via het Border Gateway Protocol (BGP) dat over de VTI loopt, naar de BR-firewall:

<#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
…
```

Het 1514-byte ESP-pakket wordt verzonden naar de buiteninterface. Maar voor de 226-byte voert de firewall bij stap 3 een route-opzoeking uit en vindt een specifieke route naar het peer-IP-adres via de VTI. Met andere woorden, in plaats van de pakketten uit de VPN-terminating interface te sturen, gebruikt de firewall de VTI-interface en probeert hij de nabijheid van de VTI-interface op te lossen. Aangezien de VTI-interfaces geen concept van nabijheid hebben, worden de pakketten

uiteindelijk gedropt met de onverwachte reden voor het vallen van pakketten.

Als tijdelijke oplossing nam de gebruiker op CSF1230 de toegangslijst (ACL) op in de routekaart. Na beleidsimplementatie weigerde de ACL het hoofdkwartier buiten het subnet, waardoor de verspreiding van het hoofdkwartier buiten het subnet effectief werd verwijderd van de BGP-routering. Vanwege deze wijziging ontvangen de BR-firewalls geen HQ-prefix buiten het subnet over de tunnelinterface.

Waarom worden 266-byte pakketten verwijderd na de migratie van ASA naar Secure Firewall?

De ASA-firewallconfiguratie blokkeerde expliciet de verspreiding van de HQ-interface buiten het subnet naar de vertakkingen:

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
```

Oorzaak

Het probleem werd veroorzaakt door een configuratieverschil in BGP-routeherverdeling tussen de oorspronkelijke ASA 5508 en de nieuwe FTD 1230. De ASA 5508 had een toegangscontrolelijst die herverdeling van het x.x.x.96/27-subnet ontkende, terwijl de FTD 1230 was geconfigureerd om alle verbonden routes te herverdelen. Dit configuratieverschil leidde tot Cisco bug ID CSCwp10123.

Verwante inhoud

- Cisco bug ID CSCwp10123

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.