Risoluzione dei problemi relativi all'autenticazione basata sui certificati del punto di accesso tramite FTD

Problema

Questi sintomi vengono segnalati dopo la migrazione di Cisco Adaptive Security Appliance 5508 a Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 nella sezione principale (HQ):

1. I punti di accesso (AP) situati nelle succursali non sono in grado di eseguire l'autenticazione al server RADIUS nella sede centrale utilizzando l'autenticazione del certificato.

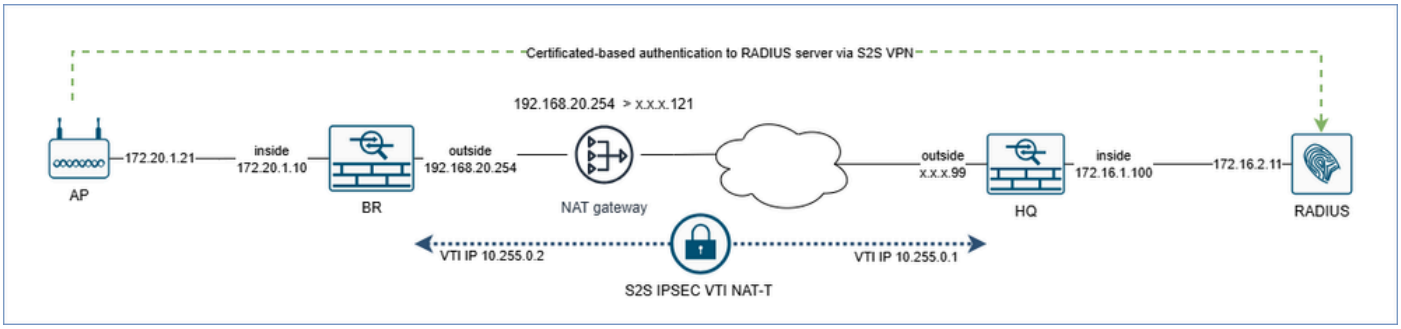
2. Autenticazione con nome utente e password riuscita.

I sintomi vengono osservati nei punti di accesso di tutti i rami.

Ambiente

Il problema può riguardare anche il CSF 1230 gestito da FMC in una configurazione ad alta disponibilità con versione 7.7.10.1 in HQ e più Firepower 1010 standalone con versione 7.4.2.4 in filiali. I sintomi in questo caso sono indipendenti dall'hardware.

Topologia



inline_image_0.png

Punti chiave sulla topologia:

- A livello di rete, il punto di accesso si trova nella subnet del firewall BR (branch) all'interno dell'interfaccia.
- Il router come gateway NAT converte l'indirizzo IP dell'interfaccia esterna BR in un indirizzo pubblico x.x.x.121. Ciò significa che il firewall BR è ad almeno 1 hop di distanza dal firewall HQ.
- I firewall HQ e BR sono connessi tramite reti VPN da sito a sito (Virtual Private Network, S2S VPN) tramite IPsec (Internet Protocol Security) con ESP (Encapsulating Security Payload) e VTI (Virtual Tunnel Interface) su NAT.
- A livello di rete, il server RADIUS si trova nella subnet del firewall HQ all'interno dell'interfaccia.

Risoluzione

Per l'analisi tecnica, le acquisizioni dei pacchetti sono state raccolte dai firewall HQ e BR.

Sul firewall HQ e BR, le acquisizioni di dati in entrata/uscita sulle interfacce fisiche, l'acquisizione sulle interfacce VTI, le acquisizioni di drop ASP per il traffico interno ed esterno basate sull'indirizzo IP del peer:

Firewall BR:

```
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
```

Si noti che x.x.x.99 viene sostituito con un indirizzo IP effettivo.

Firewall HQ:

```
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
```

Si noti che x.x.x.121 viene sostituito con un indirizzo IP effettivo.

Inoltre, sul firewall della sede centrale, lo switch interno bidirezionale acquisisce le interfacce dello chassis in base al nome esterno se e a tutte le interfacce uplink:

```
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.
```

Analisi tecnica

Firewall HQ

1. Le acquisizioni di Accelerated Security Path (ASP) nel firewall della sede centrale indicano che i frammenti vengono scartati e questo è il motivo per cui 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. Il contatore Timeout per l'interfaccia VTI nell'output del comando show fragment nel firewall della sede centrale aumenta:

<#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
```

In base alla guida di riferimento del comando (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), il timeout è "il numero massimo di secondi di attesa per l'arrivo di un intero pacchetto frammentato". Il valore predefinito è 5 secondi. Ciò significa che se l'intera catena di frammenti non raggiunge il firewall entro 5 secondi, i frammenti ricevuti vengono scartati e il riassemblaggio non riesce.

3. In base al punto precedente, il firewall della sede centrale non riceve l'intera catena di frammenti che determina un errore di riassemblaggio.

BR Firewall

1. In base alle acquisizioni, il punto di accesso invia al firewall BR una richiesta di autenticazione basata su certificato RADIUS in due frammenti separati. L'acquisizione br_inside visualizza 2 frammenti in ingresso di 1514 byte e 475 byte rispettivamente. Gli stessi pacchetti vengono visualizzati nelle acquisizioni dell'interfaccia VTI di BR che mostrano il pacchetto prima della crittografia:

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

La MTU (Maximum Transmission Unit) dell'interfaccia esterna BR è 1500 byte. Per questo motivo, il frammento da 1514 byte deve essere frammentato in 2 pacchetti prima della crittografia.

2. Il drop ASP acquisisce br_asp per il traffico RADIUS interno sul firewall BR e non visualizza i pacchetti scartati. Nel frattempo, per il traffico esterno, si verificano gocce di pacchetti da 226 byte, con il motivo 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

L'output del comando show capture br_asp visualizza 184 byte di lunghezza del payload, mentre la lunghezza totale di ciascun pacchetto è di 226 byte.

3. Per verificare se i pacchetti ESP scartati da 226 byte sono rilevanti per il traffico interessato tra il punto di accesso e il server RADIUS, l'acquisizione br_inside è stata riprodotta nel laboratorio interno utilizzando le stesse configurazioni dei criteri di sicurezza dai firewall HQ e BR. La funzione br_vti capture dal dispositivo lab visualizza i frammenti da 1514 byte e 475 byte, ossia prima della crittografia:

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. Le clip br_outside mostrano la mancanza di pacchetti da 226 byte e lo spazio tra i numeri di sequenza ESP dei pacchetti da 562 byte e 1506 byte:

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

Considerazioni principali:

- Nell'acquisizione br_outside manca il valore 226 byte, perché viene scartato nell'ASP del firewall di BR con il motivo della perdita di ASP imprevista-packet.
- La perdita di pacchetti spiega il gap nei numeri di sequenza ESP.
- Inoltre, il numero di sequenza mancante nell'intervallo indica che il pacchetto ESP da 226 byte è stato generato dal firewall BR ma non trasmesso dall'interfaccia esterna.
- Poiché il pacchetto da 226 byte non è stato inviato al firewall di BR all'esterno dell'interfaccia, il firewall della sede centrale non lo ha mai ricevuto.
- La mancanza di un pacchetto da 226 byte nel firewall della sede centrale ha causato un errore di riassemblaggio del frammento, come mostrato nella sezione "HQ firewall".

Spiegazione

I risultati restituiti dalla sezione analisi tecnica corrispondono ai sintomi del bug Cisco con ID CSCwp10123.

Panoramica delle azioni del firewall per generare pacchetti ESP e trasmetterli all'esterno dell'interfaccia di uscita:

1. Il firewall riceve i pacchetti frammentati che devono essere inviati tramite il tunnel VTI.
2. Se la lunghezza del pacchetto interno è maggiore delle dimensioni MTU dell'interfaccia meno il sovraccarico dell'IPSEC, il pacchetto viene frammentato.
3. L'hop successivo viene trovato in base alla ricerca nella tabella di routing. Nel caso della VTI, l'hop successivo è l'indirizzo IP VTI del peer.
4. In base all'indirizzo di destinazione del tunnel, vengono identificate l'interfaccia in uscita e l'hop successivo (ad esempio, l'interfaccia esterna).
5. I pacchetti originali sono incapsulati all'interno dei pacchetti ESP.
6. Viene eseguita la ricerca delle adiacenze per l'hop successivo dal passaggio 3 e i pacchetti vengono inviati all'interfaccia di uscita.

A causa dell'ID bug Cisco CSCwp10123, per i successivi pacchetti (non iniziali) incapsulati ESP viene eseguita una nuova ricerca del percorso alla fase 4. Se il firewall dispone di route più specifiche per l'indirizzo IP (o subnet) del peer, viene utilizzata la nuova route anziché la route del pacchetto iniziale. Nell'esempio, l'indirizzo IP dell'interfaccia del firewall HQ è x.x.x.99. Il firewall HQ annuncia la propria subnet esterna al firewall BR tramite il Border Gateway Protocol (BGP) in esecuzione sul 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
…
```

Il pacchetto ESP da 1514 byte viene inviato all'interfaccia esterna. Tuttavia, per i 226 byte, il firewall al passaggio 3 esegue una ricerca dei percorsi e trova il percorso specifico verso l'indirizzo IP del peer tramite la VTI. In altre parole, invece di inviare i pacchetti all'interfaccia che termina la VPN, il firewall utilizza l'interfaccia VTI e cerca di risolvere l'adiacenza sull'interfaccia VTI. Poiché le interfacce VTI non hanno un concetto di adiacenza, i pacchetti possono essere scartati con il motivo della perdita imprevista.

Per ovviare al problema, nel CSF1230 l'utente ha incluso l'elenco degli accessi (ACL) nella mappa dei percorsi. Dopo la distribuzione della policy, l'ACL ha negato la sede centrale all'esterno della subnet, rimuovendo in modo efficace la propagazione della sede centrale all'esterno della subnet dal routing BGP. A causa di questa modifica, i firewall BR non ricevono il prefisso della subnet HQ esterna sull'interfaccia del tunnel.

Perché i pacchetti da 266 byte vengono eliminati dopo la migrazione da ASA a Secure Firewall?

La configurazione del firewall dell'ASA ha bloccato in modo esplicito la propagazione della subnet dell'interfaccia esterna della sede centrale alle diramazioni:

ASA 5508

```
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
```

Causa

Il problema è stato causato da una differenza di configurazione nella ridistribuzione della route BGP tra l'ASA 5508 originale e il nuovo FTD 1230. L'ASA 5508 disponeva di una lista di controllo degli accessi che negava la ridistribuzione della subnet x.x.x.96/27, mentre l'FTD 1230 era configurato per ridistribuire tutte le route connesse. La differenza di configurazione ha attivato l'ID bug Cisco CSCwp10123.

Contenuto correlato

- ID bug Cisco CSCwp10123

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).