Resolución de problemas de falla de autenticación basada en certificados de punto de acceso mediante FTD

Problema

Estos síntomas se notifican después de la migración del Cisco Adaptive Security Appliance 5508 a Cisco Secure Firewall (CSF) Threat Defence (FTD) 1230 en la sucursal principal (HQ):

1. Los puntos de acceso (AP) ubicados en las sucursales no pueden autenticarse en el servidor RADIUS en HQ mediante la autenticación de certificados.

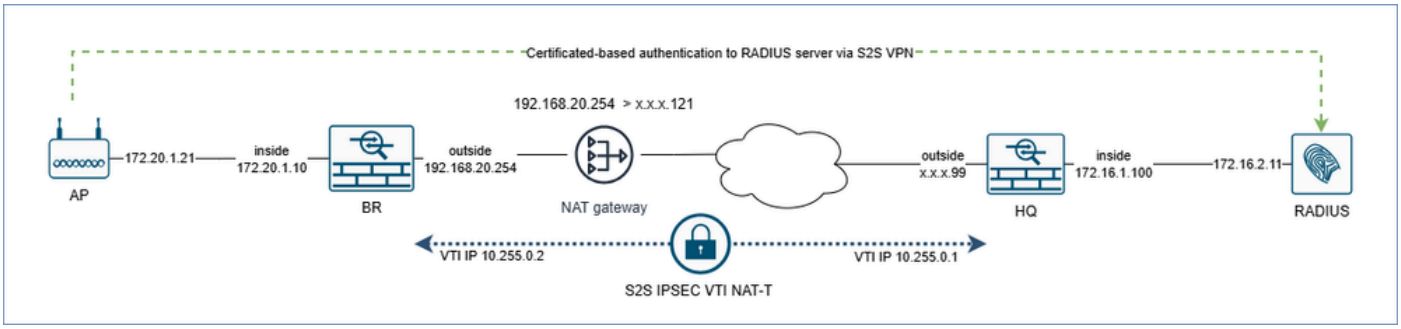
2. La autenticación con nombre de usuario y contraseña se ha realizado correctamente.

Los síntomas se observan en los puntos de acceso de todas las ramas.

Entorno

CSF 1230 gestionado por FMC en configuración de alta disponibilidad que ejecuta la versión 7.7.10.1 en HQ y varios Firepower 1010 independientes que ejecutan la versión 7.4.2.4 en sucursales; también pueden verse afectadas otras versiones de software. Los síntomas en este caso son independientes del hardware.

Topología



inline_image_0.png

Puntos clave sobre la topología:

- En la capa de red, el punto de acceso se encuentra en la subred de la interfaz interior del firewall BR (sucursal).
- El router como gateway NAT traduce la dirección IP de la interfaz exterior del firewall BR a una dirección pública x.x.x.121. Esto significa que el firewall BR está al menos a 1 salto del firewall HQ.
- Los firewalls HQ y BR se conectan mediante redes privadas virtuales de sitio a sitio (VPN S2S) mediante la seguridad de protocolo de Internet (IPsec) con carga de seguridad de encapsulación (ESP) y la interfaz de túnel virtual (VTI) a través de NAT.
- En el nivel de red, el servidor RADIUS se encuentra en la subred de la interfaz interior del firewall de HQ.

Resolución

Para el análisis técnico, las capturas de paquetes se recopilaron de los firewalls HQ y BR.

En las capturas de entrada/salida del plano de datos del firewall de HQ y BR en las interfaces físicas, captura en las interfaces VTI, captura de caídas ASP para el tráfico interno y externo según la dirección IP del par:

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
```

Observe que x.x.x.99 se sustituye por una dirección IP real.

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 172.16.2.1
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
```

Observe que x.x.x.121 se sustituye por una dirección IP real.

Además, en el firewall de HQ, recopile capturas de switch internas bidireccionales en interfaces de chasis basadas en el nombre externo si y en todas las interfaces de enlace ascendente:

```
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.
```

Análisis técnico

Firewall HQ

1. Las capturas de caídas de la ruta de seguridad acelerada (ASP) en el firewall de HQ indican que los fragmentos se descartan con la razón 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. El contador Timeout para la interfaz VTI en la salida del comando show fragment en el firewall HQ 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
```

Según la referencia de comandos (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), el tiempo de espera es "El número máximo de segundos a esperar para que llegue un paquete fragmentado completo". El valor predeterminado es de 5 segundos. Esto significa que si la cadena de fragmentos completa no llega al firewall en 5 segundos, los fragmentos recibidos se descartan y el reensamblado de fragmentos falla.

3. Según el punto anterior, el firewall de HQ no recibe la cadena completa de fragmentos que provoca un error de reensamblado de fragmentos.

Firewall BR

1. Según las capturas, el AP envía una solicitud de autenticación basada en certificados RADIUS en 2 fragmentos separados al firewall BR. La captura br_inside muestra 2 fragmentos de ingreso de 1514 bytes y 475 bytes respectivamente. Los mismos paquetes

se ven en las capturas de la interfaz BR VTI que muestran el paquete antes del cifrado:

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 unidad de transmisión máxima (MTU) de la interfaz exterior BR es de 1500 bytes. Debido a esta razón, el fragmento de 1514 bytes debe fragmentarse en 2 paquetes antes del cifrado.

2. Las capturas de descarte ASP br_asp para el tráfico RADIUS interno en el firewall BR no muestran los paquetes descartados. Mientras tanto, para el tráfico exterior, hay caídas de paquetes de 226 bytes con la razón inactive-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

Observe que la salida del comando show capture br_asp muestra 184 bytes de longitud de carga útil, mientras que la longitud total de cada paquete es de 226 bytes.

3. Para verificar si los paquetes ESP descartados de 226 bytes son relevantes para el tráfico afectado entre el AP y el servidor RADIUS, la captura br_inside se reprodujo en el laboratorio interno utilizando las mismas configuraciones de política de seguridad de los

firewalls HQ y BR. La captura br_vti del dispositivo de laboratorio muestra los fragmentos de 1514 bytes y 475 bytes, es decir, antes del cifrado:

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. Las capturas br_outside muestran la falta de paquetes de 226 bytes y la brecha en los números de secuencia ESP entre los paquetes de 562 bytes y 1506 bytes:

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

Puntos clave:

- Falta un byte de 226 bytes en la captura br_outside, porque se descarta en el firewall de BR ASP con el motivo de caída de paquete inesperado ASP.
- La caída de paquetes explica la brecha en los números de secuencia ESP.
- Además, el número de secuencia faltante en el rango significa que el paquete ESP de 226 bytes fue generado por el firewall BR pero no se transmitió fuera de la interfaz externa.
- Dado que el paquete de 226 bytes no se envió a la interfaz exterior del firewall BR, el firewall HQ nunca lo recibió.
- La falta del paquete de 226 bytes en el firewall HQ provocó el fallo de reensamblado del fragmento, como se muestra en la sección "Firewall HQ".

Explicación

Los hallazgos de la sección de análisis técnico coinciden con los síntomas del Id. de bug Cisco CSCwp10123.

Descripción general de alto nivel de las acciones del firewall para generar paquetes ESP y transmitirlos a través de la interfaz de salida:

1. El firewall recibe paquetes fragmentados que se supone que deben enviarse a través del túnel VTI.
2. Si la longitud del paquete interno es mayor que el tamaño de la MTU de la interfaz menos la sobrecarga de IPSEC, el paquete se fragmenta.
3. De acuerdo con la búsqueda de la tabla de ruteo, se encuentra el siguiente salto. En el caso del VTI, el salto siguiente es la dirección IP del VTI par.
4. En función de la dirección de destino del túnel, se identifican la interfaz de salida y el siguiente salto (por ejemplo, la interfaz externa).
5. Los paquetes originales se encapsulan dentro de los paquetes ESP.
6. Se realiza la búsqueda de adyacencia para el salto siguiente del paso 3 y los paquetes se envían a la interfaz de salida.

Debido al ID de bug de Cisco CSCwp10123, para los fragmentos encapsulados ESP subsiguientes (no iniciales) paquetes en el paso 4 se realiza una nueva búsqueda de ruta. Si el firewall tiene rutas más específicas a la dirección IP del par (o subred), se utiliza la nueva ruta en lugar de la ruta para el paquete inicial. En este ejemplo, la dirección IP de la interfaz de firewall de HQ es x.x.x.99. El firewall de HQ anuncia su subred externa al firewall BR a través del protocolo de gateway fronterizo (BGP) que se ejecuta en el 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
…

El paquete ESP de 1514 bytes se envía por la interfaz externa. Sin embargo, para los 226 bytes, el firewall del paso 3 realiza una búsqueda de ruta y encuentra una ruta específica hacia la

dirección IP del par a través del VTI. En otras palabras, en lugar de enviar los paquetes fuera de la interfaz de terminación de VPN, el firewall utiliza la interfaz VTI e intenta resolver la adyacencia en la interfaz VTI. Dado que las interfaces VTI no tienen un concepto de adyacencia, los paquetes se descartan eventualmente con la razón de la caída de paquetes inesperada.

Como solución alternativa, en CSF1230 el usuario incluyó la lista de acceso (ACL) en el route-map. Después de la implementación de políticas, la ACL denegó la subred externa de HQ, eliminando de forma efectiva la propagación de la subred externa de HQ del ruteo BGP. Debido a este cambio, los firewalls BR no reciben el prefijo de subred externa de HQ a través de la interfaz de túnel.

¿Por qué se descartan los paquetes de 266 bytes después de la migración de ASA a Secure Firewall?

La configuración del firewall ASA bloqueó explícitamente la propagación de la subred de la interfaz externa de HQ a las sucursales:

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
```

Causa

El problema fue provocado por una diferencia de configuración en la redistribución de rutas BGP entre el ASA 5508 original y el nuevo FTD 1230. El ASA 5508 tenía una lista de control de acceso que denegaba la redistribución de la subred x.x.x.96/27, mientras que el FTD 1230 estaba

configurado para redistribuir todas las rutas conectadas. Esta diferencia de configuración activó el ID de bug de Cisco CSCwp10123.

Contenido relacionado

- ID de bug de Cisco CSCwp10123

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).