Fehlerbehebung bei zertifiziertem Authentifizierungsfehler des Access Points über FTD

Problem

Diese Symptome treten nach der Migration der Cisco Adaptive Security Appliance 5508 zur Cisco Secure Firewall (CSF) Threat Defense (FTD) 1230 in der Hauptniederlassung auf:

1. Die in den Zweigstellen befindlichen Access Points (APs) können sich beim RADIUS-Server in der Hauptniederlassung nicht mittels Zertifikatsauthentifizierung authentifizieren.

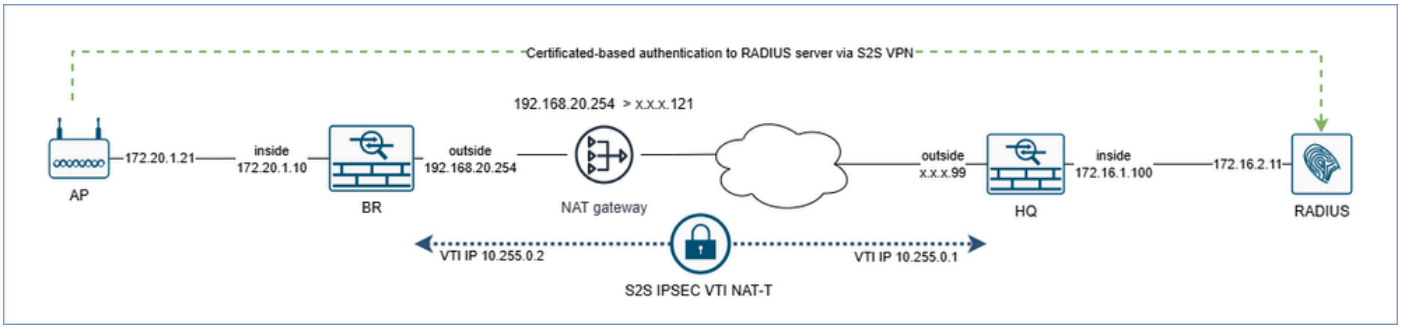
2. Die Authentifizierung mit Benutzername und Kennwort ist erfolgreich.

Die Symptome wurden für Access Points in allen Zweigstellen beobachtet.

Umwelt

FMC-Managed CSF 1230 in hochverfügbarer Konfiguration mit Version 7.7.10.1 im Hauptsitz und mehreren eigenständigen Firepower 1010 mit Version 7.4.2.4 in Zweigstellen, andere Softwareversionen können ebenfalls betroffen sein. Die Symptome in diesem Fall sind hardwareunabhängig.

Topologie



inline_image_0,png

Wichtige Punkte zur Topologie:

- Auf Netzwerkebene befindet sich der Access Point im Subnetz der Firewall innerhalb der BR-Schnittstelle (Außenstelle).
- Der Router als NAT-Gateway übersetzt die IP-Adresse der externen BR-Firewall-Schnittstelle in eine öffentliche Adresse x.x.x.121. Dies bedeutet, dass die BR-Firewall mindestens einen Hop von der Firewall im Hauptsitz entfernt ist.
- Die Verbindung der Firewalls von Hauptsitz und BR erfolgt über Site-to-Site Virtual Private Networks (S2S VPN) unter Verwendung von IPsec (Internet Protocol Security) mit Encapsulating Security Payload (ESP) und VTI (Virtual Tunnel Interface) über NAT.
- Auf Netzwerkebene befindet sich der RADIUS-Server im Subnetz der Firewall im Hauptsitz.

Auflösung

Zur technischen Analyse wurden die Paketerfassungen von den Firewalls im Hauptsitz und im Außendienst erfasst.

Auf der HQ- und BR-Firewall-Datenebene werden Eingangs-/Ausgangserfassungen an physischen Schnittstellen, Erfassung an VTI-Schnittstellen, ASP-Ausgangserfassungen für inneren und äußeren Datenverkehr auf Basis der Peer-IP-Adresse:

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
```

Beachten Sie, dass x.x.x.99 durch eine tatsächliche IP-Adresse ersetzt wird.

Firewall im Hauptsitz:

```
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
```

Beachten Sie, dass x.x.x.121 durch eine tatsächliche IP-Adresse ersetzt wird.

Zusätzlich sammelt die Firewall im Hauptsitz bidirektionale interne Switch-Erfassungen in den Chassis-Schnittstellen, basierend auf dem externen Namen EIF und allen Uplink-Schnittstellen:

```
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

Firewall im Hauptsitz

1. Die ASP-Drop-Captures in der Firewall des Hauptsitzes weisen darauf hin, dass Fragmente aufgrund eines Fehlers bei der Fragmentreassemblierung verworfen werden:

<#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. Der Timeout-Zähler für die VTI-Schnittstelle in der Ausgabe des Befehls show fragment in der HQ-Firewall erhöht sich um:

<#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
```

Gemäß der Befehlsreferenz (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) ist das Timeout "The maximum number of seconds to wait for a complete fragmented packet to arrival". Der Standardwert ist 5 Sekunden. Dies bedeutet, dass die empfangenen Fragmente verworfen werden, wenn die gesamte Fragmentkette nicht innerhalb von 5 Sekunden an der Firewall ankommt und die Fragmenterneuerung fehlschlägt.

3. Ausgehend vom vorherigen Punkt empfängt die Firewall im Hauptsitz nicht die gesamte Fragmentkette, die zu einem Fragmentreassemblierungsfehler führt.

BR-Firewall

1. Basierend auf den Erfassungen sendet der WAP eine RADIUS-zertifikatbasierte Authentifizierungsanforderung in zwei separaten Fragmenten an die BR-Firewall. Der br_inside-Capture-Befehl zeigt 2 Eingangsfragmente mit 1514 Byte bzw. 475 Byte.

Dieselben Pakete werden in der BR VTI-Schnittstelle erkannt, die das Paket vor der Verschlüsselung anzeigt:

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

Die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) der BR-Schnittstelle beträgt 1.500 Byte. Aus diesem Grund muss das 1514 Byte große Fragment vor der Verschlüsselung in 2 Pakete fragmentiert werden.

2. ASP-Drop-Captures br_asp für internen RADIUS-Datenverkehr auf der BR-Firewall zeigen keine verworfenen Pakete an. Gleichzeitig treten beim äußeren Datenverkehr Verluste von 226-Byte-Paketen auf, die den folgenden unerwarteten Grund haben:

<#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

Beachten Sie, dass die Ausgabe des Befehls show capture br_asp 184 Byte Nutzlastlänge anzeigt, während die Gesamtlänge jedes Pakets 226 Byte beträgt.

3. Um zu überprüfen, ob verworfene 226-Byte-ESP-Pakete für den betroffenen Datenverkehr

zwischen dem Access Point und dem RADIUS-Server relevant sind, wurde die br_inside-Erfassung im internen Lab unter Verwendung derselben Sicherheitsrichtlinienkonfigurationen von den Firewalls im Hauptsitz und im BR wiederholt. Der br_vti-Test des Übungsgeräts zeigt 1514-Byte- und 475-Byte-Fragmente, d. h. vor der Verschlüsselung:

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 #11
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 #13
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 #15
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 #17
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 #19
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 #21
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 #23
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 #25
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 #27
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 #29
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. Die br_outside-Aufnahmen zeigen das Fehlen von 226-Byte-Paketen und die Lücke in den ESP-Sequenznummern zwischen den 562-Byte- und 1506-Byte-Paketen:

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

Wichtigste Punkte:

- 226 Byte fehlen bei der br_outside-Erfassung, da sie in der BR-Firewall ASP mit dem Grund für das Verwerfen eines unerwarteten Pakets verworfen werden.
- Der Paketverlust erklärt die Lücke in den ESP-Sequenznummern.
- Darüber hinaus bedeutet die fehlende Sequenznummer im Bereich, dass das 226-Byte-ESP-Paket von der BR-Firewall generiert, aber nicht über die externe Schnittstelle übertragen wurde.
- Da das 226-Byte-Paket nicht über die externe Schnittstelle der BR-Firewall gesendet wurde, hat die Firewall im Hauptsitz es nie empfangen.
- Das Fehlen des 226-Byte-Pakets in der Firewall des Hauptsitzes führte zum Zusammenstellungsfehler des Fragments, wie im Abschnitt "Firewall des Hauptsitzes" gezeigt.

Erläuterung

Die Ergebnisse aus dem Abschnitt zur technischen Analyse stimmen mit den Symptomen des Cisco Bugs "CSCwp10123" überein.

Überblick über die Firewall-Aktionen zum Generieren von ESP-Paketen und deren Übertragung über die Ausgangsschnittstelle:

1. Die Firewall empfängt fragmentierte Pakete, die über den VTI-Tunnel gesendet werden sollen.
2. Wenn die Länge des inneren Pakets größer als die MTU-Größe der Schnittstelle abzüglich des IPSEC-Overheads ist, wird das Paket fragmentiert.
3. Basierend auf der Suche in der Routing-Tabelle wird der nächste Hop gefunden. Im Fall des VTI ist der nächste Hop die VTI-IP-Adresse des Peers.
4. Basierend auf der Tunnel-Zieladresse werden die Egress-Schnittstelle und der nächste Hop identifiziert (z. B. eine externe Schnittstelle).
5. Die ursprünglichen Pakete werden in ESP-Pakete gekapselt.
6. Es wird eine Adjazenzsuche für den nächsten Hop aus Schritt 3 durchgeführt, und Pakete werden an die Ausgangsschnittstelle gesendet.

Aufgrund der Cisco Bug-ID CSCwp10123 wird für nachfolgende ESP-gekapselte Fragmente (nicht-initiale) von Paketen in Schritt 4 eine neue Routensuche durchgeführt. Wenn die Firewall spezifischere Routen zur Peer-IP-Adresse (oder zum Subnetz) hat, wird die neue Route anstelle der Route für das ursprüngliche Paket verwendet. In diesem Beispiel ist die IP-Adresse der Firewall-Schnittstelle des Hauptsitzes x.x.x.99. Die Firewall des Hauptsitzes kündigt der BR-Firewall ihr externes Subnetz über das Border Gateway Protocol (BGP) an, das über den VTI ausgeführt wird:

<#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
…

Das 1514-Byte-ESP-Paket wird von der externen Schnittstelle gesendet. Für die 226 Byte führt die Firewall in Schritt 3 jedoch eine Routensuche durch und findet über den VTI eine bestimmte Route zur Peer-IP-Adresse. Mit anderen Worten: Anstatt die Pakete über die VPN-Terminierungsschnittstelle zu senden, verwendet die Firewall die VTI-Schnittstelle und versucht, die Adjacency an der VTI-Schnittstelle aufzulösen. Da die VTI-Schnittstellen kein Konzept der Adjacency aufweisen, werden die Pakete schließlich verworfen, um unerwartete Paketverluste zu vermeiden.

Als Problemumgehung hat der Benutzer bei CSF1230 die Zugriffsliste (ACL) in die Routenübersicht eingefügt. Nach der Richtlinienbereitstellung verweigerte die ACL den Hauptsitz außerhalb des Subnetzes und entfernte somit effektiv die Übertragung des Hauptsitzes außerhalb des Subnetzes vom BGP-Routing. Aufgrund dieser Änderung erhalten die BR-Firewalls über die Tunnelschnittstelle kein externes Subnetzpräfix für den Hauptsitz.

Warum werden 266-Byte-Pakete nach der Migration von ASA zu Secure Firewall verworfen?

Die ASA-Firewall-Konfiguration blockierte explizit die Weiterleitung des externen Schnittstellen-Subnetzes im Hauptsitz an die Außenstellen:

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
```

GFK 1230

```
router bgp 65000
...
  redistribute connected route-map BGP_RM
route-map BGP_RM permit 40 <-- No match, means redistribute all connected routes
```

Ursache

Das Problem wurde durch einen Konfigurationsunterschied bei der BGP-Routen-Neuverteilung

zwischen der ursprünglichen ASA 5508 und der neuen FTD 1230 ausgelöst. Die ASA 5508 verfügte über eine Zugriffskontrollliste, die die Neuverteilung des Subnetzes x.x.x.96/27 ablehnte, während die FTD 1230 für die Neuverteilung aller verbundenen Routen konfiguriert wurde. Dieser Konfigurationsunterschied löste den Cisco Bug mit der ID CSCwp10123 aus.

Verwandte Inhalte

- Cisco Bug-ID CSCwp10123

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.