FTDを介したアクセスポイントの証明書ベースの認証失敗のトラブルシューティング

お問い合わせ内容

これらの症状は、Cisco適応型セキュリティアプライアンス(ASA)5508をメインブランチ(HQ)のCisco Secure Firewall(CSF)Threat Defense(FTD)1230に移行した後に報告されます。

1. ブランチオフィスにあるアクセスポイント(AP)が、証明書認証を使用したHQのRADIUSサーバへの認証に失敗する。

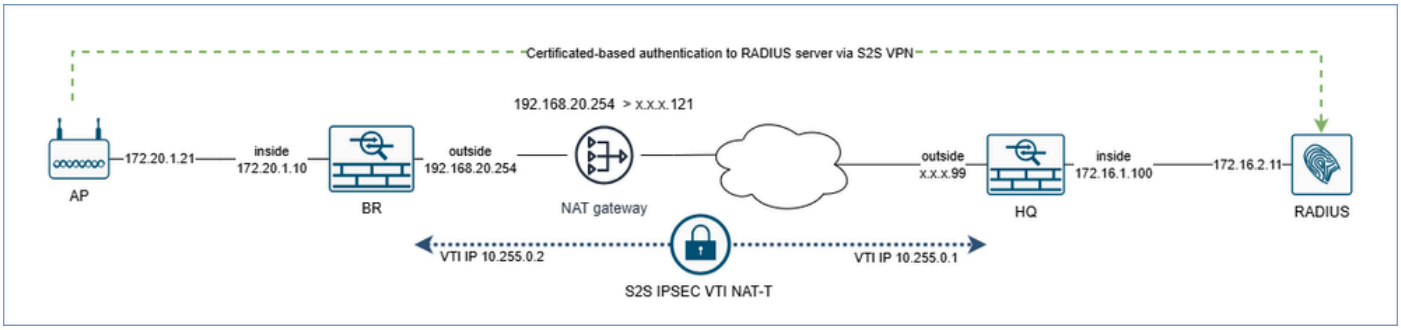
2. ユーザ名とパスワードを使用した認証が成功します。

症状は、すべてのブランチのアクセスポイントで見られます。

環境

HQでバージョン7.7.10.1を実行する高可用性構成のFMC管理対象CSF 1230と、ブランチでバージョン7.4.2.4を実行する複数のスタンドアロンFirepower 1010では、他のソフトウェアバージョンも影響を受ける可能性があります。この場合の症状は、ハードウェアに依存しません。

トポロジ



inline_image_0.png (インラインイメージ_0.png)

トポロジに関する要点：

- ネットワーク層では、アクセスポイントはBR（ブランチ）ファイアウォールの内部インターフェイスのサブネットにあります。
- NATゲートウェイとしてのルータは、BRファイアウォールの外部インターフェイスのIPアドレスを、パブリックアドレスx.x.x.121に変換します。つまり、BRファイアウォールはHQファイアウォールから少なくとも1ホップ離れていることになります。
- HQファイアウォールとBRファイアウォールは、Encapsulating Security Payload(ESP)を備えたインターネットプロトコルセキュリティ(IPsec)とNAT経由の仮想トンネルインターフェイス(VTI)を使用するサイト間バーチャルプライベートネットワーク(S2S VPN)を使用して接続されます。
- ネットワークレベルでは、RADIUSサーバはHQファイアウォールの内部インターフェイスのサブネットにあります。

解決策

技術的な分析のために、パケットキャプチャはHQおよびBRファイアウォールから収集されました。

物理インターフェイス上のHQおよびBRファイアウォールデータプレーンの入力/出力キャプチャ、VTIインターフェイス上のキャプチャ、ピアIPアドレスに基づく内部および外部トラフィックのASPドロップキャプチャ：

BRファイアウォール：

```
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
```

x.x.x.99は実際のIPアドレスに置き換えられることに注意してください。

本社のファイアウォール：

```
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
```

x.x.x.121は実際のIPアドレスに置き換えられることに注意してください。

さらに、HQファイアウォールで、outside nameifとすべてのアップリンクインターフェイスに基づいて、シャーシインターフェイス内の双方向の内部スイッチキャプチャを収集します。

```
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.
```

技術分析

HQファイアウォール

1. HQファイアウォール内のAccelerated Security Path（ASP；高速セキュリティパス）dropキャプチャは、fragment-reassembly-failed:という理由でフラグメントがドロップされたことを示しています。

<#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. HQファイアウォールでのshow fragmentコマンドの出力に含まれる、VTIインターフェイスのTimeoutカウンタは、

```
<#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
```

コマンドリファレンス(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)によると、Timeoutは「フラグメント化されたパケット全体が到着するのを待機する最大秒数」です。 デフォルト値は 5 秒です。つまり、フラグメントチェーン全体が5秒以内にファイアウォールに到達しなかった場合、受信したフラグメントは廃棄され、フラグメントの再構成は失敗します。

3. 前述のポイントに基づくと、HQファイアウォールは、フラグメントのリアセンブル障害を引き起こすフラグメントの完全なチェーンを受信しません。

BRファイアウォール

1. キャプチャに基づいて、APはRADIUS証明書ベースの認証要求を2つのフラグメントに分割してBRファイアウォールに送信します。br_insideキャプチャは、それぞれ1514バイトと475バイトの2つの入力フラグメントを示します。同じパケットが、暗号化前のパケットを示すBR VTIインターフェイスキャプチャに表示されます。

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 (インラインイメージ_0.png)

BR外部インターフェイスの最大伝送ユニット(MTU)は1500バイトです。このため、1514バイトのフラグメントは、暗号化の前に2つのパケットにフラグメント化する必要があります。

2. BRファイアウォールの内側RADIUSトラフィックに対するASPドロップキャプチャ
   br_aspでは、ドロップされたパケットは表示されません。一方、外部トラフィックの場合、unexpected-packet:という理由で、226バイトのパケットが廃棄されます。

<#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ファイル

show capture br_aspコマンドの出力では、ペイロード長が184バイトなのに対し、各パケットの全長は226バイトになっていることに注意してください。

3. 226バイトのドロップされたESPパケットが、APとRADIUSサーバ間の影響を受けるトラフィックに関連するかどうかを確認するため、内部のラボでbr_insideキャプチャがHQとBRファイアウォールからの同じセキュリティポリシー設定を使用して再実行されました。ラボデバイスからのbr_vtiキャプチャには、暗号化前の1514バイトおよび475バイトのフラグメントが示されています。

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ファイル

4. br_outsideのキャプチャでは、226バイトのパケットが不足しており、562バイトと1506バイトのパケット間にESPシーケンス番号のギャップがあることが示されています。

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 (インラインイメージ_3.png)

キー ポイント：

- br_outsideキャプチャでは、226バイトが欠落しています。これは、unexpected-packet ASPドロップの理由でBRファイアウォールASPでドロップされるためです。
- パケットドロップは、ESPシーケンス番号のギャップを説明します。
- さらに、この範囲内にシーケンス番号が含まれていないことは、226バイトのESPパケットがBRファイアウォールによって生成されたものの、外部インターフェイスには送信されなかったことを意味します。
- 226バイトのパケットはBRファイアウォールの外部インターフェイスから送信されていないため、HQファイアウォールはそれを受信しませんでした。
- HQファイアウォールで226バイトのパケットが欠落していたため、「HQファイアウォール」セクションで示したように、フラグメントのリアセンブルに失敗しました。

説明

技術分析セクションの結果は、Cisco Bug ID CSCwp10123の症状と一致します。

ESPパケットを生成し、出力インターフェイスに送信するファイアウォールアクションの概要を説明します。

1. ファイアウォールは、VTIトンネル経由で送信されると想定されるフラグメント化されたパケットを受信します。
2. 内部パケットの長さが、インターフェイスのMTUサイズからIPSECオーバーヘッドを引いたサイズよりも大きい場合、パケットはフラグメント化されます。
3. ルーティングテーブルのルックアップに基づいて、ネクストホップが見つかります。VTIの場合、ネクストホップはピアVTIのIPアドレスです。
4. トンネルの宛先アドレスに基づいて、出力インターフェイスとネクストホップ（外部インターフェイスなど）が識別されます。
5. 元のパケットはESPパケット内にカプセル化されます。
6. 手順3で取得したネクストホップの隣接関係ルックアップが実行され、パケットが出力インターフェイスから送信されます。

Cisco Bug ID CSCwp10123により、手順4で後続のESP力プセル化フラグメント（先頭以外）のパケットに対して、新しいルートルックアップが実行されます。ファイアウォールにピアIPアドレス（またはサブネット）への特定のルートがある場合、最初のパケットのルートではなく新しいルートが使用されます。この例では、HQファイアウォールインターフェイスのIPアドレスはx.x.x.99です。HQファイアウォールは、VTI上で実行されているボーダーゲートウェイプロトコル(BGP)を介して、外部サブネットをBRファイアウォールにアドバタイズします。

<#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
…
```

1514バイトのESPパケットが外部インターフェイスから送信されます。ただし、226バイトの場合、ステップ3のファイアウォールはルートルックアップを実行し、VTIを介したピアIPアドレスへの特定のルートを見つけます。つまり、ファイアウォールは、VPN終端インターフェイスからパケットを送信する代わりに、VTIインターフェイスを使用して、VTIインターフェイスの隣接関係の解決を試みます。VTIインターフェイスには隣接関係の概念がないため、パケットは最終的に

、予期しないパケットのドロップの理由でドロップされます。

回避策として、CSF1230でユーザがルートマップにアクセスリスト(ACL)を含めました。ポリシーの導入後、ACLはHQ外部サブネットを拒否し、BGPルーティングからHQ外部サブネットの伝搬を効果的に削除しました。この変更により、BRファイアウォールはトンネルインターフェイス経由でHQ外部サブネットプレフィクスを受信しません。

ASAからセキュアファイアウォールに移行した後、266バイトのパケットがドロップされるのはなぜですか。

ASAファイアウォールの設定により、ブランチへのHQ外部インターフェイスサブネットの伝搬が明示的にブロックされました。

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
```

原因

この問題は、元のASA 5508と新しいFTD 1230の間のBGPルート再配布の設定の違いによって引き起こされました。ASA 5508には、x.x.x.96/27サブネットの再配布を拒否するアクセスコントロールリスト(ACL)が設定されていましたが、FTD 1230は接続されたすべてのルートを再配布するように設定されていました。この設定の違いにより、Cisco Bug ID CSCwp10123が発生しました。

関連コンテンツ

- Cisco Bug ID CSCwp10123

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。