FMCからFTDへのアップグレード導入失敗後のsftunnel通信問題のトラブルシューティング

内容

お問い合わせ内容

複数のファイアウォール脅威対策(FTD)デバイスに導入をプッシュしようとすると失敗し、8 %から20 %の間で導入の失敗が発生します。 FMCのログには、これらの障害の明確な理由は示されていません。

環境

- Cisco Secure Firewall Firepower(FMC)
- FMCとFTDはMPLSパス経由で通信します
- FMCとFTD間のsftunnel/managementトラフィックに対するファイアウォール検査はありません。
- sftunnel通信用のFMCとFTD間の十分な帯域幅
- 導入の失敗を記録

解決策

このワークフローでは、sftunnelプロセスの通信の問題に関連するFMCからFTDデバイスへの展開の失敗を識別し、解決するための包括的で詳細な手順を提供します。 各ステップについて、説明用のコマンド出力例を含めて詳細に説明します。

ルートスーパーユーザとしてFTD CLIにアクセスします。

高度な診断とプロセス操作を実行するには、FTDデバイスのCLIにログインし、特権をrootに昇格させます。

```
> expert
device$ sudo su
Password:
root@device:/Volume/home/admin#
```

FTDのsftunnelステータスの確認

`sftunnel_status.pl`スクリプトを実行して、sftunnelプロセスの健全性と通信状態を確認します。

```
root@device:/Volume/home/admin# sftunnel_status.pl
OR
root@device:/Volume/home/admin# sftunnel_status.pl PEERIPADDRESS
OR
root@device:/Volume/home/admin# sftunnel_status.pl PEERUUID
```

RPCステータス障害を示す出力例：

```
peer UUID did not reply at /ngfw/usr/local/sf/bin/sftunnel_status.pl line 309.
Retry rpc status poll at /ngfw/usr/local/sf/bin/sftunnel_status.pl line 315.
**RPC STATUS****PEERIP*************
RPC status :Failed
**RPC STATUS****PEERIP*************
RPC status :Failed
```

変更が必要なデバイスに応じて、FMCの「システム/設定/管理インターフェイス」ページまたはFTDのCLISHでIPアドレスを手動で変更する必要があるため、FMC管理またはFTD管理のいずれかに対して最近、IPアドレスまたはネットワークの変更が行われていないことを確認します。

FTD CLISHでの管理IPアドレス変更の例：

```
> configure network ipv4 manual IPADDRESS NETMASK GATEWAYIP
> show network
```

sftunnelプロセスの現在のプロセスID(PID)の特定

sftunnelプロセスを監視および確認するには、pmtoolを使用してそのPIDを取得します。

```
root@device:/Volume/home/admin# pmtool status | grep sftunnel
```

出力例：

```
sftunnel       Running     PID: 12345
```

sftunnelプロセスを再起動し、PIDの変更を確認する

sftunnelプロセスを再起動して、通信状態をリセットします。 再起動後、PIDチェックを再実行し

て、新しいプロセスがアクティブであることを確認します。

```
root@device:/Volume/home/admin# pmtool restartbyid sftunnel
```

しばらくしてから、プロセスのステータスを再び確認します。

```
root@device:/Volume/home/admin# pmtool status | grep sftunnel
```

出力例 (PIDは前のものと異なる必要があります) :

```
sftunnel      Running     PID: 67890
```

sftunnelプロセスが安定するまで2分間待機し、FMCから影響を受けるFTDへの新しい展開を試行します

sftunnelプロセスが完全に再初期化され、通信が再確立されるまで約2分間待機します。 次に、FMCからFTDへの新しい導入を開始します。

導入記録の例：

```
===============TRANSACTION INFO===============
Device UUID: PEERUUID
Transaction ID: 4075925334520
Selected policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrusion
Out-of-date policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrus
Deployment Type: Full Deployment
================================================================
```

成功すると、導入はエラーなしで完了し、ポリシーはFTDで更新されます。

再起動後のsftunnelとRPC通信の検証

導入が成功したら、`sftunnel_status.pl`を使用して、sftunnelプロセスとRPCステータスが正常であることを再度確認します。

```
root@device:/Volume/home/admin# sftunnel_status.pl
```

成功を示す出力例：

```
**RPC STATUS****PEERIP*************
  'ipv4_1' => 'PEERIP',
  'uuid' => 'PEERUUID',
  'ipv6' => 'IPv6 is not configured for management',
  'active' => 1,
  'ip' => 'PEERIP',
  'last_changed' => 'Thu Nov 13 23:22:43 2025',
  'name' => 'PEERNAME',
  'uuid_gw' => ''
```

影響を受けるすべてのFTDでsftunnel再起動手順を繰り返します。

複数のFTDが影響を受ける場合は、影響を受けるデバイスごとに前述の手順を実行して、展開機能を復元します。

帯域幅と接続の検証

bandwidth_analyzer.pl —size SIZEINMB -p PEERIPを実行して、FMCとFTD間に適切な帯域幅と基本的なネットワーク接続があることを確認します。 シスコのドキュメントでは、安定した管理接続のために少なくとも5 Mbpsのスループットを推奨しています。

帯域幅分析の出力例：

```
======== Bandwidth Analysis Result  ========
$VAR1 = {
          'PEERIP' => [
                                {
                                  'download' => '3.81 Mbps'
                                },
                                {
                                  'upload' => '4.24 Mbps'
                                },
                                {
                                  'rpcStatus' => 'Up'
                                }
                              ]
        };
```

原因

展開の失敗の根本原因には、次の原因が考えられます。

- 特定のFTDまたはFMCデバイスのsftunnelプロセスの誤動作。
- 中間ファイアウォールインスペクションなどの管理TLSトラフィックへの干渉が原因で、

RPCステータスチェックに対する応答が正しくありません。
- IPアドレスの変更、移行、デバイスの追加などのネットワークの変更により、デバイス間で到達不能が発生する。

影響を受けるFTD/FMCでsftunnelプロセスを再起動すると、適切な通信が復元され、FMCからポリシーを正常に展開できるようになります。

それ以外の場合は、IPアドレスと明確なネットワークパスを検証して、デバイス間の接続が適切であることを確認します。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

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。