

Fehlerbehebung bei Problemen mit der Sftunnel-Kommunikation nach einem Bereitstellungsfehler-Upgrade von FMC auf FTD

Inhalt

Problem

Bei Versuchen, Bereitstellungen auf mehrere FTD-Geräte (Firewall Threat Defense) zu übertragen, treten Bereitstellungsfehler zwischen 8 % und 20 % auf. Die FMC-Protokolle liefern keinen klaren Grund für diese Fehler.

Umwelt

- Cisco Secure Firewall FirePOWER (FMC)
- FMC und FTDs kommunizieren über einen MPLS-Pfad
- Keine Firewall-Inspektion für Tunnel-/Management-Datenverkehr zwischen FMC und FTDs
- Ausreichende Bandbreite zwischen FMC und FTD für die Kanalkommunikation
- Festgestellte Bereitstellungsfehler

Auflösung

Dieser Workflow bietet ein umfassendes und detailliertes Verfahren zum Identifizieren und Beheben von Bereitstellungsfehlern von FMC- bis FTD-Geräten, die mit Problemen bei der Kommunikation mit dem Sftunnel-Prozess verbunden sind. Jeder Schritt wird detailliert erläutert, einschließlich Beispielbefehlsausgaben zur Veranschaulichung.

Zugriff auf die FTD-CLI als Super User

Um erweiterte Diagnosen und Prozessabläufe durchzuführen, melden Sie sich bei der FTD-Geräte-CLI an, und eskalieren Sie die Berechtigungen an root.

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

FTD-Sftunnel-Status überprüfen

Führen Sie das Skript `sftunnel_status.pl` aus, um den Zustand und den Kommunikationsstatus des `sftunnel`-Prozesses zu überprüfen.

```
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
```

Beispielausgabe für RPC-Statusfehler:

```
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
```

Vergewissern Sie sich, dass keine Änderungen an der zuletzt verwendeten IP-Adresse oder am Netzwerk vorgenommen wurden, da dies eine manuelle Änderung der IP-Adresse auf der Seite für FMC-System/Konfigurations-/Verwaltungsschnittstellen oder der FTD-CLISH erfordern würde, je nachdem, welches Gerät geändert werden muss.

Beispiel für eine Änderung der Management-IP-Adresse auf FTD CLISH:

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

Identifizieren der aktuellen Prozess-ID (PID) für den Sftunnel-Prozess

Um den Sftunnel-Prozess zu überwachen und zu überprüfen, rufen Sie dessen PID mit `pmtool` ab.

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

Beispiel:

```
sftunnel      Running      PID: 12345
```

Starten Sie den sftunnel-Prozess neu, und überprüfen Sie die PID-Änderung.

Starten Sie den sftunnel-Prozess neu, um seinen Kommunikationsstatus zurückzusetzen. Führen Sie nach dem Neustart die PID-Prüfung erneut aus, um zu bestätigen, dass ein neuer Prozess aktiv ist.

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

Überprüfen Sie nach kurzer Zeit den Prozessstatus erneut:

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

Beispielausgabe (PID muss sich vom vorherigen unterscheiden):

```
sftunnel      Running      PID: 67890
```

Warten Sie 2 Minuten, bis sich der Sftunnel-Prozess stabilisiert hat, und versuchen Sie eine neue Bereitstellung von FMC für das betroffene FTD.

Warten Sie etwa zwei Minuten, bis der Sftunnel-Prozess vollständig neu initialisiert und die Kommunikation wiederhergestellt ist. Starten Sie dann eine neue Bereitstellung von FMC für die FTD.

Beispiel für Bereitstellungsprotokoll:

```
=====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
```

```
=====
```

Wenn die Bereitstellung erfolgreich ist, wird sie fehlerfrei abgeschlossen, und die Richtlinien werden auf dem FTD aktualisiert.

Validierung der Sftunnel- und RPC-Kommunikation nach dem Neustart

Bestätigen Sie nach einer erfolgreichen Bereitstellung mit `sftunnel_status.pl` erneut, dass der Sftunnel-Prozess und der RPC-Status fehlerfrei sind.

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

Beispielausgabe für Erfolg:

```
**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' => ''
```

Wiederholen Sie den sftunnel-Neustart für alle betroffenen FTDs.

Wenn mehrere FTDs betroffen sind, führen Sie die oben genannten Schritte für jedes betroffene Gerät aus, um die Bereitstellungsfunktionalität wiederherzustellen.

Validierung von Bandbreite und Anbindung

Führen Sie `bandwidth_analyser.pl —size SIZEINMB -p PEERIP` aus, um sicherzustellen, dass eine ausreichende Bandbreite und grundlegende Netzwerkverbindungen zwischen FMC und FTDs vorhanden sind. In der Cisco Dokumentation wird ein Durchsatz von mindestens 5 Mbit/s für eine stabile Managementverbindung empfohlen.

Beispiel für Bandbreitenanalyseausgabe:

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

Ursache

Die Ursachen von Bereitstellungsfehlern können folgende sein:

- Eine Fehlfunktion im Sftunnel-Prozess auf bestimmten FTD- oder FMC-Geräten.
- Interferenzen beim TLS-Management-Datenverkehr, z. B. bei zwischengeschalteten Firewall-Analysen, führen zu fehlerhaften Antworten auf RPC-Statusüberprüfungen.
- Netzwerkänderungen wie Änderungen an IP-Adressen, Migrationen oder Geräteerweiterungen führen dazu, dass Geräte nicht mehr erreichbar sind.

Ein Neustart des Sftunnel-Prozesses auf dem betroffenen FTD/FMC kann die ordnungsgemäße Kommunikation wiederherstellen und eine erfolgreiche Richtlinienbereitstellung vom FMC ermöglichen.

Andernfalls stellen Sie eine ordnungsgemäße Verbindung zwischen den Geräten sicher, indem Sie die IP-Adressen und einen eindeutigen Netzwerkpfad validieren.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

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.