

Problemen met sftunnelcommunicatie oplossen na mislukte implementatie van upgrade van FMC naar FTD

Inhoud

uitgeven

Pogingen om implementaties naar meerdere Firewall Threat Defense (FTD)-apparaten te pushen mislukken, waarbij implementatiefouten tussen 8% en 20% optreden. De FMC-logs geven geen duidelijke reden voor deze fouten.

milieu

- Cisco Secure Firewall Firepower (FMC)
- FMC's en FTD's communiceren via een MPLS-pad
- Geen firewallinspectie van de tunnel/het beheer van het verkeer tussen het VCC en de FTD's
- Voldoende bandbreedte tussen FMC en FTD's voor satellietcommunicatie
- Mislukte implementatie opgemerkt

resolutie

Deze workflow biedt een uitgebreide en gedetailleerde procedure voor het identificeren en oplossen van implementatiefouten van FMC naar FTD-apparaten die verband houden met problemen met de communicatie van het aftunnelproces. Elke stap wordt in detail uitgelegd, inclusief voorbeeld commando-uitgangen voor illustratie.

Toegang tot de FTD CLI als de Root Super User

Om geavanceerde diagnoses en procesbewerkingen uit te voeren, meldt u zich aan bij de FTD-apparaatCLI en escaleert u de rechten naar root.

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

Controleer de status van de FTD-tunnel

Voer het script `sftunnel_status.pl` uit om de gezondheids- en communicatiestatus van het `sftunnel`-proces te controleren.

```
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
```

Voorbeeld van uitvoer die aangeeft dat de RPC-status is mislukt:

```
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
```

Zorg ervoor dat er geen recente IP-adres- of netwerkwijzigingen in het FMC- of FTD-beheer zijn opgetreden, aangezien dit handmatige wijziging van het IP-adres op de pagina FMC System / Configuration / Management Interfaces of de FTD CLISH zou vereisen, afhankelijk van het apparaat waarvoor de wijziging vereist is.

Voorbeeld IP-adreswijziging beheer op FTD CLISH:

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

Identificeer de huidige proces-ID (PID) voor het sftunnelproces

Om het `sftunnel`proces te bewaken en te verifiëren, haalt u de PID op met `pmtool`.

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

Voorbeeld van uitvoer:

sftunnel Running PID: 12345

Herstart het stunnel-proces en controleer de PID-wijziging

Start het stunnel-proces opnieuw op om de communicatiestatus te herstellen. Voer na het opnieuw opstarten de PID-controle opnieuw uit om te bevestigen dat een nieuw proces actief is.

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

Controleer na een korte periode de processtatus opnieuw:

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

Voorbeelduitvoer (PID moet anders zijn dan de vorige uitvoer):

sftunnel Running PID: 67890

Wacht 2 minuten totdat het steftunnelproces is gestabiliseerd en probeer een nieuwe inzet van FMC naar de getroffen FTD

Laat ongeveer twee minuten voor de sftunnelproces volledig opnieuw initialiseren en opnieuw tot stand brengen van de communicatie. Start vervolgens een nieuwe implementatie van FMC naar het FTD.

Voorbeeld van implementatietranscript:

```
=====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, Intrusion
Deployment Type: Full Deployment
=====
```

Als dit lukt, wordt de implementatie zonder fouten voltooid en worden de beleidsregels in het FTD bijgewerkt.

Valideren van sftunnel- en RPC-communicatie na herstart

Bevestig na een succesvolle implementatie dat het sftunnel-proces en de RPC-status weer gezond zijn met behulp van `sftunnel_status.pl`.

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

Voorbeeld van uitvoer die succes aangeeft:

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

Herhaal de herstartprocedure voor alle getroffen FTD's

Als meerdere FTD's worden beïnvloed, voert u de bovengenoemde stappen uit voor elk betrokken apparaat om de implementatiefunctie te herstellen.

Bandbreedte- en connectiviteitsvalidatie

Voer `bandwidth_analyzer.pl --size SIZEINMB -p PEERIP` uit om ervoor te zorgen dat er voldoende bandbreedte en basisnetwerkconnectiviteit is tussen FMC en FTD's. Cisco-documentatie suggereert ten minste 5 Mbps doorvoer voor een stabiele beheerverbinding.

Voorbeeld bandbreedte analyse uitvoer:

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

Oorzaak

De hoofdoorzaken van de implementatiefouten kunnen het volgende zijn:

- Een storing in het aftunnelproces op specifieke FTD- of FMC-apparaten.
- Interferentie met het beheer van TLS-verkeer, zoals van intermediaire firewall-inspecties, waardoor slechte reacties op RPC-statuscontroles worden veroorzaakt.
- Netwerkwijzigingen, zoals wijzigingen in het IP-adres, migraties of apparaattoevoegingen die onbereikbaarheid tussen apparaten veroorzaken.

Het opnieuw opstarten van het setunnelproces op de betrokken FTD/FMC kan de juiste communicatie herstellen en een succesvolle beleidsimplementatie van de FMC mogelijk maken.

Zorg anders voor een goede connectiviteit tussen apparaten door IP-adressen en een duidelijk netwerkpad te valideren.

Verwante inhoud

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.