Troubleshoot sftunnel Communication Issues after Upgrade Deployment Failure from FMC to FTD

Contents

Issue

Attempts to push deployments to multiple Firewall Threat Defense (FTD) devices fail, with deployment failures occ

Environment

- Cisco Secure Firewall Firepower (FMC)
- FMC and FTDs communicate over an MPLS path
- No firewall inspection on sftunnel/management traffic between FMC and FTDs
- Sufficient bandwidth between FMC and FTDs for sftunnel communications
- Deployment failures noted

Resolution

This workflow provides a comprehensive and detailed procedure for identifying and resolving deployment failures f

Access the FTD CLI as the Root Super User

To perform advanced diagnostics and process operations, log in to the FTD device CLI and escalate privileges to roo

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

Check the FTD sftunnel Status

Run the `sftunnel_status.pl` script to check the health and communication status of the sftunnel process.

```
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
```

Example output indicating RPC status failures:

```
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
```

Ensure that there have been no recent IP address or network changes to either the FMC or FTD management as this

Example management IP address change on FTD CLISH:

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

Identify the Current Process ID (PID) for the sftunnel Process

To monitor and verify the sftunnel process, retrieve its PID using `pmtool`.

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

Example output:

```
sftunnel      Running     PID: 12345
```

Restart the sftunnel Process and Verify the PID Change

Restart the sftunnel process to reset its communication state. After restarting, re-run the PID check to confirm a new process is active.

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

After a brief period, check the process status again:

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

Example output (PID has to be different from the previous):

```
sftunnel      Running     PID: 67890
```

Wait 2 Minutes for the sftunnel Process to Stabilize and Attempt a New deployment from FM

Allow approximately two minutes for the sftunnel process to fully re-initialize and re-establish communication. Then, initiate a new deployment from FMC to the FTD.

Example deployment transcript:

```
===============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
================================================================
```

If successful, the deployment completes without error and policies are updated on the FTD.

Validate sftunnel and RPC Communication Post-Restart

After a successful deployment, confirm that the sftunnel process and RPC status are healthy using `sftunnel_status.` again.

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

Example output indicating success:

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

Repeat the sftunnel Restart Procedure for all Impacted FTDs

If multiple FTDs are impacted, perform the aforementioned steps for each affected device to restore deployment fun

Bandwidth and Connectivity Validation

Run **bandwidth_analyzer.pl --size SIZEINMB -**

p PEERIP to ensure that there is adequate bandwidth and basic network connectivity between FMC and FTDs. Cisc

Example bandwidth analysis output:

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

Cause

The root causes of the deployment failures can be due to:

- A malfunction in the sftunnel process on specific FTD or FMC devices.
- Interference to management TLS traffic, such as from intermediary firewall inspections, causing bad response
- Network changes such as IP address changes, migrations, or device additions causing unreachability between

Restarting the sftunnel process on the affected FTD/FMC can restore proper communication and allow successful po

Otherwise, ensure proper connectivity between devices by validating IP addresses and a clear network path.

Related Content

- Cisco Technical Support & Downloads