Dépannage des problèmes de communication sftunnel après l'échec du déploiement de la mise à niveau de FMC à FTD

Table des matières

Problème

Les tentatives d'envoi de déploiements vers plusieurs périphériques Firewall Threat Defense (FTD) échouent, les échecs de déploiement se situant entre 8 % et 20 %. Les journaux FMC ne fournissent pas de raison claire pour ces échecs.

Environnement

- Cisco Secure Firewall Firepower (FMC)
- FMC et FTD communiquent via un chemin MPLS
- Aucune inspection de pare-feu sur le trafic sftunnel/management entre FMC et FTD
- Bande passante suffisante entre FMC et FTD pour les communications sftunnel
- Défaillances de déploiement notées

Résolution

Ce workflow fournit une procédure complète et détaillée pour identifier et résoudre les échecs de déploiement de FMC vers les périphériques FTD associés aux problèmes de communication du processus sftunnel. Chaque étape est expliquée en détail, y compris des exemples de sorties de commande pour illustration.

Accéder à l'interface de ligne de commande FTD en tant que super utilisateur racine

Pour effectuer des diagnostics avancés et des opérations de traitement, connectez-vous à l'interface de ligne de commande du périphérique FTD et transférez les privilèges à la racine.

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

Vérifier l'état du FTD sftunnel

Exécutez le script `sftunnel_status.pl` pour vérifier l'état de santé et de communication du processus sftunnel.

```
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
```

Exemple de résultat indiquant des échecs d'état RPC :

```
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
```

Assurez-vous qu'aucune modification récente de l'adresse IP ou du réseau n'a été apportée à la gestion FMC ou FTD, car cela nécessiterait une modification manuelle de l'adresse IP sur la page Système FMC / Configuration / Interfaces de gestion ou sur l'interface CLISH FTD, selon le périphérique pour lequel la modification est requise.

Exemple de changement d'adresse IP de gestion sur FTD CLISH :

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

Identifier l'ID de processus actuel (PID) pour le processus sftunnel

Pour surveiller et vérifier le processus sftunnel, récupérez son PID à l'aide de `pmtool`.

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

Exemple de rapport :

```
sftunnel      Running     PID: 12345
```

Redémarrez le processus sftunnel et vérifiez la modification du PID

Redémarrez le processus sftunnel pour réinitialiser son état de communication. Après le redémarrage, réexécutez la vérification du PID pour confirmer qu'un nouveau processus est actif.

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

Après une courte période, vérifiez à nouveau l'état du processus :

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

Exemple de résultat (le PID doit être différent du précédent) :

```
sftunnel      Running     PID: 67890
```

Attendez 2 minutes que le processus sftunnel stabilise et tente un nouveau déploiement du FMC au FTD affecté

Attendez environ deux minutes que le processus sftunnel réinitialise et rétablit complètement la communication. Ensuite, lancez un nouveau déploiement de FMC vers FTD.

Exemple de transcription de déploiement :

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

En cas de réussite, le déploiement se termine sans erreur et les stratégies sont mises à jour sur le FTD.

Valider sftunnel et la communication RPC après le redémarrage

Après un déploiement réussi, confirmez que le processus sftunnel et l'état RPC sont sains en utilisant à nouveau `sftunnel_status.pl`.

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

Exemple de résultat indiquant la réussite :

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

Répétez la procédure de redémarrage de sftunnel pour tous les FTD affectés

Si plusieurs FTD sont affectés, exécutez les étapes mentionnées ci-dessus pour chaque périphérique affecté afin de restaurer la fonctionnalité de déploiement.

Validation de bande passante et de connectivité

Exécutez bandwidth_analyzer.pl —size SIZEINMB -p PERIP pour vous assurer que la bande passante et la connectivité réseau de base sont adéquates entre le FMC et les FTD. La documentation Cisco suggère un débit d'au moins 5 Mbits/s pour une connexion de gestion stable.

Exemple de sortie d'analyse de bande passante :

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

Motif

Les causes premières des échecs de déploiement peuvent être les suivantes :

- Un dysfonctionnement dans le processus sftunnel sur des périphériques FTD ou FMC spécifiques.
- Interférence avec le trafic TLS de gestion, par exemple à partir d'inspections de pare-feu intermédiaires, provoquant des réponses incorrectes aux contrôles d'état RPC.
- Les modifications du réseau, telles que les changements d'adresse IP, les migrations ou les ajouts de périphériques, entraînent une inaccessibilité entre les périphériques.

Le redémarrage du processus sftunnel sur le FTD/FMC affecté peut restaurer la communication appropriée et permettre un déploiement de stratégie réussi à partir du FMC.

Dans le cas contraire, assurez-vous d'une connectivité correcte entre les périphériques en validant les adresses IP et un chemin réseau clair.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.