

Solucionar problemas de comunicação do sftunnel após falha na implantação da atualização do FMC para o FTD

Contents

Problema

Falha nas tentativas de enviar implantações para vários dispositivos FTD (Firewall Threat Defense), com falhas de implantação entre 8% e 20%. Os logs FMC não fornecem uma razão clara para essas falhas.

Ambiente

- Cisco Secure Firewall Firepower (FMC)
- O FMC e o FTD comunicam-se através de um canal MPLS
- Sem inspeção de firewall no tráfego de sftunnel/gerenciamento entre FMC e FTDs
- Largura de banda suficiente entre o CVP e o DTF para as comunicações por túnel auxiliar
- Falhas de implantação observadas

Resolução

Este fluxo de trabalho fornece um procedimento abrangente e detalhado para identificar e resolver falhas de implantação de dispositivos FMC para FTD associados a problemas de comunicação do processo sftunnel. Cada etapa é explicada em detalhes, incluindo exemplos de saídas de comando para ilustração.

Acessar a CLI do FTD como superusuário raiz

Para executar diagnósticos avançados e operações de processo, efetue login na CLI do dispositivo FTD e transfira os privilégios para a raiz.

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

Verificar o Status do FTD sftunnel

Execute o script `sftunnel_status.pl` para verificar o status de integridade e de comunicação do processo `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
```

Exemplo de saída indicando falhas de status de 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
```

Assegurar que não houve alterações recentes do endereço IP ou da rede na gestão do FMC ou do FTD, uma vez que tal exigiria a alteração manual do endereço IP na página System / Configuration / Management Interfaces do FMC ou na CLISH do FTD, dependendo do dispositivo em que a alteração é necessária.

Exemplo de alteração de endereço IP de gerenciamento no FTD CLISH:

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

Identificar o ID do processo atual (PID) para o processo `sftunnel`

Para monitorar e verificar o processo `sftunnel`, recupere seu PID usando `pmtool`.

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

Saída de exemplo:

```
sftunnel      Running      PID: 12345
```

Reinicie o processo sftunnel e verifique a alteração do PID

Reinicie o processo sftunnel para redefinir seu estado de comunicação. Depois de reiniciar, execute novamente a verificação de PID para confirmar se um novo processo está ativo.

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

Após um breve período, verifique novamente o status do processo:

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

Saída de exemplo (o PID deve ser diferente do anterior):

```
sftunnel      Running      PID: 67890
```

Aguarde 2 minutos para que o processo de sftunnel seja estabilizado e tente uma nova implantação do FMC para o FTD afetado

Aguarde aproximadamente dois minutos para que o processo sftunnel reinicialize completamente e restabeleça a comunicação. Em seguida, inicie uma nova implantação do FMC para o FTD.

Exemplo de transcrição de implantação:

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

Se obtiver êxito, a implantação será concluída sem erros e as políticas serão atualizadas no FTD.

Validar pós-reinicialização de comunicação sftunnel e RPC

Após uma implantação bem-sucedida, confirme se o processo sftunnel e o status do RPC estão íntegros usando sftunnel_status.pl novamente.

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

Exemplo de saída indicando sucesso:

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

Repita o procedimento de reinicialização de sftunnel para todos os FTDs afetados

Se vários FTDs forem afetados, execute as etapas mencionadas acima para cada dispositivo afetado para restaurar a funcionalidade de implantação.

Validação de largura de banda e conectividade

Execute `bandwidth_analyzer.pl —size SIZEINMB -p PEERIP` para garantir que haja largura de banda adequada e conectividade de rede básica entre o FMC e os FTDs. A documentação da Cisco sugere pelo menos 5 Mbps de throughput para uma conexão de gerenciamento estável.

Exemplo de saída de análise de largura de banda:

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

Causa

As causas raiz das falhas de implantação podem ser:

- Uma anomalia no processo sftunnel em dispositivos específicos do FTD ou do FMC.
- A interferência no gerenciamento do tráfego TLS, como de inspeções intermediárias de firewall, causando respostas incorretas às verificações de status de RPC.
- Alterações de rede, como alterações de endereço IP, migrações ou adições de dispositivos, que causam inacessibilidade entre dispositivos.

Reiniciar o processo sftunnel no FTD/FMC afetado pode restaurar a comunicação apropriada e permitir a implantação bem-sucedida de políticas do FMC.

Caso contrário, assegure a conectividade adequada entre os dispositivos validando os endereços IP e um caminho de rede claro.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.