

Resolución de problemas de comunicación sftunnel tras fallo de implementación de actualización de FMC a FTD

Contenido

Problema

Los intentos de enviar implementaciones a varios dispositivos de defensa frente a amenazas de firewall (FTD) fallan y los errores de implementación se producen entre el 8% y el 20%. Los registros de FMC no proporcionan una razón clara para estos errores.

Entorno

- Cisco Secure Firewall Firepower (FMC)
- Los FMC y los FTD se comunican a través de una ruta MPLS
- Sin inspección de firewall en el tráfico de gestión/túnel seguro entre FMC y FTD
- Ancho de banda suficiente entre FMC y FTD para comunicaciones de túnel seguro
- Errores de implementación detectados

Resolución

Este flujo de trabajo proporciona un procedimiento completo y detallado para identificar y resolver los fallos de despliegue de FMC a los dispositivos FTD asociados con problemas de comunicación de proceso sftunnel. Cada paso se explica en detalle, incluidas salidas de comandos de ejemplo para la ilustración.

Acceso a la CLI de FTD como superusuario raíz

Para realizar diagnósticos avanzados y operaciones de proceso, inicie sesión en la CLI del dispositivo FTD y escale los privilegios a root.

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

Compruebe el estado del túnel seguro de FTD

Ejecute el script `sftunnel_status.pl` para verificar el estado y el estado de la comunicación del proceso `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
```

Ejemplo de salida que indica errores de estado 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
```

Asegúrese de que no se han producido cambios recientes en la dirección IP o en la red, ni en la gestión de FMC ni en la de FTD, ya que esto requeriría un cambio manual de la dirección IP en la página Sistema/Configuración/Interfaces de gestión de FMC o en FTD CLISH, en función del dispositivo en el que se requiera el cambio.

Ejemplo de cambio de dirección IP de administración en FTD CLISH:

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

Identifique el ID de proceso actual (PID) para el proceso `sftunnel`

Para monitorear y verificar el proceso `sftunnel`, recupere su PID usando `pmtool`.

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

Ejemplo de salida:

```
sftunnel      Running      PID: 12345
```

Reinicie el proceso sftunnel y verifique el cambio de PID

Reinicie el proceso sftunnel para restablecer su estado de comunicación. Después de reiniciar, vuelva a ejecutar la comprobación de PID para confirmar que hay un nuevo proceso activo.

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

Tras un breve período, vuelva a comprobar el estado del proceso:

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

Ejemplo de salida (PID debe ser diferente de la anterior):

```
sftunnel      Running      PID: 67890
```

Espere 2 minutos hasta que el proceso sftunnel se estabilice e intente una nueva implementación desde FMC hasta el FTD afectado

Espere aproximadamente dos minutos para que el proceso sftunnel se reinicialice por completo y restablezca la comunicación. A continuación, inicie una nueva implementación desde FMC al FTD.

Ejemplo de transcripción de implementación:

```
=====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
```

```
=====
```

Si se realiza correctamente, la implementación se completa sin errores y las políticas se actualizan en el FTD.

Validar sftunnel y comunicación RPC después del reinicio

Después de una implementación exitosa, confirme que el proceso sftunnel y el estado RPC se

encuentren en buen estado usando de nuevo `sftunnel_status.pl`.

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

Ejemplo de resultado que indica éxito:

```
**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 el procedimiento de reinicio de `sftunnel` para todos los FTD afectados

Si se ven afectados varios FTD, lleve a cabo los pasos anteriores para cada dispositivo afectado con el fin de restaurar la funcionalidad de implementación.

Validación de ancho de banda y conectividad

Ejecute `bandwidth_analyzer.pl —size SIZEINMB -p PEERIP` para asegurarse de que haya un ancho de banda adecuado y conectividad de red básica entre FMC y FTD. La documentación de Cisco sugiere un rendimiento de al menos 5 Mbps para una conexión de administración estable.

Ejemplo de resultado del análisis de ancho de banda:

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

Causa

Las causas principales de los errores de implementación pueden deberse a:

- Un mal funcionamiento en el proceso sftunnel en dispositivos FTD o FMC específicos.
- Interferencia en la administración del tráfico TLS, como por las inspecciones intermedias del firewall, causando respuestas erróneas a las verificaciones de estado RPC.
- Los cambios en la red, como los cambios en la dirección IP, las migraciones o las adiciones de dispositivos, causan inaccesibilidad entre dispositivos.

El reinicio del proceso sftunnel en el FTD/FMC afectado puede restaurar la comunicación adecuada y permitir una implementación correcta de la política desde FMC.

De lo contrario, asegúrese de que haya una conectividad adecuada entre los dispositivos validando las direcciones IP y una ruta de red clara.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).