

Risoluzione dei problemi di comunicazione sftunnel dopo l'errore di distribuzione dell'aggiornamento da FMC a FTD

Sommario

Problema

Tentativi di eseguire il push di distribuzioni in più dispositivi Firewall Threat Defense (FTD) non riusciti. Gli errori di distribuzione si verificano tra l'8% e il 20%. I registri FMC non forniscono una motivazione chiara per tali errori.

Ambiente

- Cisco Secure Firewall Firepower (FMC)
- FMC e FTD comunicano su un percorso MPLS
- Nessuna ispezione del firewall sul traffico di gestione/tunnel tra FMC e FTD
- Larghezza di banda sufficiente tra FMC e FTD per le comunicazioni tunnel
- Errori di distribuzione annotati

Risoluzione

Questo flusso di lavoro fornisce una procedura completa e dettagliata per identificare e risolvere gli errori di distribuzione da FMC ai dispositivi FTD associati a problemi di comunicazione del processo sftunnel. Ogni passo viene spiegato in dettaglio, inclusi alcuni output di comandi di esempio per illustrazione.

Accesso alla CLI FTD come utente privilegiato root

Per eseguire operazioni avanzate di diagnostica ed elaborazione, accedere alla CLI del dispositivo FTD ed eseguire l'escalation dei privilegi nella root.

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

Controllare lo stato del tunnel FTD

Eseguire lo script `sftunnel_status.pl` per controllare lo stato di integrità e di comunicazione del 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
```

Output di esempio che indica gli errori di stato 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
```

Accertarsi che non vi siano state modifiche recenti dell'indirizzo IP o della rete nella gestione del FMC o del FTD, in quanto ciò richiederebbe la modifica manuale dell'indirizzo IP nella pagina Sistema/configurazione/Interfacce di gestione del FMC o nel FTD CLISH, a seconda del dispositivo su cui è richiesta la modifica.

Esempio di modifica dell'indirizzo IP di gestione in FTD CLISH:

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

Identificare l'ID processo corrente (PID) per il processo `sftunnel`

Per monitorare e verificare il processo `sftunnel`, recuperare il relativo PID utilizzando `pmtool`.

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

Output di esempio:

```
sftunnel      Running      PID: 12345
```

Riavviare il processo sftunnel e verificare la modifica del PID

Riavviare il processo sftunnel per reimpostarne lo stato di comunicazione. Dopo il riavvio, eseguire nuovamente la verifica PID per confermare che un nuovo processo è attivo.

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

Dopo un breve periodo, verificare nuovamente lo stato del processo:

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

Esempio di output (il PID deve essere diverso dal precedente):

```
sftunnel      Running      PID: 67890
```

Attendere 2 minuti per consentire al processo sftunnel di stabilizzare e tentare una nuova distribuzione da FMC all'FTD interessato

Attendere circa due minuti prima che il processo sftunnel reinizializzi e ristabilisca completamente la comunicazione. Quindi avviare una nuova distribuzione da FMC a FTD.

Esempio di trascrizione della distribuzione:

```
=====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 l'operazione ha esito positivo, la distribuzione viene completata senza errori e i criteri vengono aggiornati nell'FTD.

Convalida dopo il riavvio di sftunnel e comunicazione RPC

Dopo una distribuzione corretta, verificare che il processo sftunnel e lo stato RPC siano integri utilizzando nuovamente `sftunnel_status.pl`.

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

Output di esempio che indica il successo:

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

Ripetere la procedura di riavvio sftunnel per tutti gli FTD interessati

In caso di impatto su più FTD, eseguire i passaggi descritti in precedenza per ciascun dispositivo interessato per ripristinare la funzionalità di distribuzione.

Convalida larghezza di banda e connettività

Eseguire `bandwidth_analyzer.pl —size SIZEINMB -p PEERIP` per verificare che la larghezza di banda e la connettività di rete di base tra FMC e FTD siano adeguate. La documentazione Cisco consiglia almeno 5 Mbps di velocità effettiva per una connessione di gestione stabile.

Esempio di output dell'analisi della larghezza di banda:

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

Causa

Le cause principali degli errori di distribuzione possono essere le seguenti:

- Un malfunzionamento nel processo sftunnel su dispositivi FTD o FMC specifici.
- Interferenza con il traffico TLS di gestione, ad esempio a causa di ispezioni intermedie del firewall, che provoca risposte errate ai controlli dello stato RPC.
- Modifiche alla rete, ad esempio modifiche dell'indirizzo IP, migrazioni o aggiunte di dispositivi, che causano l'irraggiungibilità tra i dispositivi.

Il riavvio del processo sftunnel nell'FTD/FMC interessato può ripristinare la comunicazione corretta e consentire la corretta distribuzione dei criteri da FMC.

In caso contrario, verificare la corretta connettività tra i dispositivi convalidando gli indirizzi IP e specificando chiaramente il percorso di rete.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).