FMC에서 FTD로 업그레이드 구축 실패 후 sftunnel 통신 문제 해결

목차

문제

여러 FTD(Firewall Threat Defense) 디바이스에 구축을 푸시하려는 시도가 실패하며, 구축 실패는 8%에서 20% 사이에서 발생합니다. FMC 로그는 이러한 실패의 명확한 이유를 제공하지 않습니다.

환경

- Cisco FMC(Secure Firewall Firepower)
- FMC와 FTD는 MPLS 경로를 통해 통신합니다
- FMC와 FTD 간의 sftunnel/management 트래픽에 대한 방화벽 검사 없음
- sftunnel 통신을 위한 FMC와 FTD 간의 대역폭이 충분합니다.
- 배포 실패 기록됨

해결

이 워크플로에서는 sftunnel 프로세스 통신 문제와 관련된 FMC에서 FTD 장치로의 배치 실패를 식별하고 해결하기 위한 포괄적이고 자세한 절차를 제공합니다. 각 단계에 대해서는 설명을 위한 명령 출력 예를 포함하여 자세히 설명합니다.

FTD CLI를 루트 수퍼 유저로 액세스

고급 진단 및 프로세스 작업을 수행하려면 FTD 디바이스 CLI에 로그인하고 권한을 루트로 에스컬레이션합니다.

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

FTD sftunnel 상태 확인

sftunnel 프로세스의 상태와 통신 상태를 확인하려면 sftunnel_status.pl 스크립트를 실행합니다.

```
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
```

RPC 상태 실패를 나타내는 출력의 예:

```
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
```

변경이 필요한 디바이스에 따라 FMC System/Configuration/Management Interfaces(FMC 시스템/컨피그레이션/관리 인터페이스) 페이지 또는 FTD CLISH에서 IP 주소를 수동으로 변경해야 하므로 FMC 또는 FTD 관리에 최근 IP 주소 또는 네트워크 변경이 없었는지 확인합니다.

FTD CLISH의 관리 IP 주소 변경 예:

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

sftunnel 프로세스의 현재 프로세스 ID(PID) 식별

sftunnel 프로세스를 모니터링하고 확인하려면 pmtool을 사용하여 PID를 검색합니다.

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

출력 예:

```
sftunnel       Running     PID: 12345
```

sftunnel 프로세스를 다시 시작하고 PID 변경 사항을 확인합니다.

sftunnel 프로세스를 다시 시작하여 통신 상태를 재설정합니다. 다시 시작한 후 PID 검사를 다시 실행하여 새 프로세스가 활성 상태인지 확인하십시오.

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

잠시 후에 프로세스 상태를 다시 확인합니다.

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

출력 예(PID는 이전과 달라야 함):

```
sftunnel       Running     PID: 67890
```

sftunnel 프로세스가 안정화될 때까지 2분 정도 기다린 후 FMC에서 영향받는 FTD로 새 구축을 시도합니다.

sftunnel 프로세스가 완전히 다시 초기화하고 통신을 다시 설정할 때까지 약 2분 정도 기다립니다. 그런 다음 FMC에서 FTD로 새 배포를 시작합니다.

구축 스크립트 예:

```
===============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Out-of-date policy group list: Access Control Policy, Intrusion Policy, Network Analysis Policy, Intrus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
================================================================
```

성공적으로 구축되면 오류 없이 완료되며 FTD에서 정책이 업데이트됩니다.

sftunnel 및 RPC 통신 사후 다시 시작 확인

성공적으로 배포한 후 sftunnel _status.pl을 다시 사용하여 sftunnel 프로세스 및 RPC 상태가 정상 상태인지 확인합니다.

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

성공을 나타내는 출력의 예:

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

영향을 받는 모든 FTD에 대해 sftunnel 재시작 절차를 반복합니다

여러 FTD가 영향을 받는 경우 영향을 받는 각 디바이스에 대해 앞서 설명한 단계를 수행하여 구축 기능을 복원합니다.

대역폭 및 연결 검증

bandwidth_analyzer.pl —size SIZEINMB -p PEERIP를 실행하여 FMC와 FTD 간에 적절한 대역폭과 기본 네트워크 연결이 이루어지도록 합니다. Cisco 문서에서는 안정적인 관리 연결을 위해 최소 5Mbps의 처리량을 제안합니다.

대역폭 분석 출력의 예:

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

원인

구축 실패의 근본 원인은 다음과 같습니다.

- 특정 FTD 또는 FMC 장치의 sftunnel 프로세스가 작동하지 않습니다.
- 중간 방화벽 검사와 같은 관리 TLS 트래픽에 대한 간섭으로 인해 RPC 상태 확인에 대한 잘못된 응답이 발생합니다.
- IP 주소 변경, 마이그레이션 또는 디바이스 추가와 같은 네트워크 변경으로 인해 디바이스 간 연결이 불가능합니다.

영향받는 FTD/FMC에서 sftunnel 프로세스를 다시 시작하면 올바른 통신이 복원되고 FMC에서 성공적으로 정책을 구축할 수 있습니다.

그렇지 않으면 IP 주소와 명확한 네트워크 경로를 검증하여 디바이스 간의 올바른 연결을 보장합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.