

Secure Access에서 개인 앱에 대한 APP_UNREACHABLE 오류 troubleshooting

목차

문제

Cisco Secure Access를 통해 ZTNA(Zero Trust Network Access) 애플리케이션에 액세스하려고 하면 "애플리케이션 도달 불가" 오류 메시지가 표시됩니다.

- Connector는 대시보드에 정상/활성 상태로 표시되며, 애플리케이션 소유자에 의해 실행 중인 것으로 확인됩니다.
- 이 오류는 동일한 커넥터에서 제공하는 다른 애플리케이션이 정상적으로 작동하는 동안 한 애플리케이션의 모든 사용자에게 영향을 미칠 수 있습니다.
- 커넥터 풀 구축에서는 장애가 간헐적으로 나타날 수 있습니다. 풀의 어떤 커넥터가 선택되었는지에 따라 세션이 성공하거나 실패합니다.

환경

- ZTNA를 통한 Cisco Secure Private Access 구축
- ZTNA 액세스를 위해 구성된 프라이빗 리소스
- 개인 리소스 액세스를 위한 리소스 커넥터 배포

해결

1단계. 커넥터 네트워크 세그먼트에서 직접 연결 가능성 테스트

- 리소스 커넥터는 잠긴 어플라이언스이며 curl 또는 nc와 같은 명령을 직접 실행하기 위한 셀 액세스를 제공하지 않습니다. 그 대신, 커넥터와 동일한 서브넷/VLAN에 있는 테스트 호스트 (또는 임시 VM)에서 연결성 테스트를 수행하여, 애플리케이션에 대한 동일한 네트워크 경로, 라우팅 및 방화벽 규칙을 준수합니다.

```
curl -v http://APP_IP:PORT/health
nc -zv APP_IP PORT
```

- 이 작업이 실패하면 네트워크 경로 또는 애플리케이션 서버에서 문제가 확인됩니다. Secure Access 구성을 검토하기 전에 이 문제를 먼저 해결해야 합니다.



참고: 다른 서브넷의 테스트는 확실하지 않습니다. 테스트 소스가 커넥터의 IP 배치를 최대한 가깝게 미러링해야 하므로 방화벽 규칙 및 라우팅은 소스별로 평가됩니다.

2단계. 프라이빗 리소스 컨피그레이션 확인

- Secure Access 대시보드에서 Resources(리소스) > Private Resources(개인 리소스)로 이동하고, 영향을 받는 개인 리소스를 열고, 구성된 IP, FQDN 및 포트 문자 대 문자를 실행 중인 애플리케이션의 실제 바인드 주소 및 포트와 비교합니다.
- 불일치(서버 마이그레이션 후 부실 IP, 잘못된 포트, HTTP 대 HTTPS)는 완벽하게 정상적인 네트워크 경로에서도 APP_UNREACHABLE을 생성합니다.

3단계. 커넥터에 대한 DNS 확인 검증

- 개인 리소스가 FQDN으로 정의된 경우 커넥터에 할당된 DNS 서버가 이를 확인할 수 있는지 확인합니다. 리소스 커넥터 CLI(VM 구축에서는 지원되는 표준 Linux 문제 해결 명령이 포함된 진단 CLI 제공)에서 다음을 실행합니다.

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- 올바른 프라이빗 IP가 반환되는지 확인합니다. 커넥터의 네트워크 컨피그레이션 포인트가 사실 애플리케이션 FQDN을 확인할 수 있는 내부 DNS 서버인지 확인합니다. 공용 확인기로 구

성된 커넥터에서 내부 영역을 확인할 수 없습니다.

4단계. 방화벽 경로 검토

- 방화벽 규칙(네트워크 방화벽 및 애플리케이션 서버의 호스트 방화벽)이 커넥터의 IP 주소에서 필요한 포트의 애플리케이션 서버 IP로의 트래픽을 허용하는지 확인합니다.

5단계. 리소스 커넥터에서 tcpdump로 트래픽 캡처

- 리소스 커넥터에서 패킷 캡처를 실행하여 애플리케이션에 대한 마지막 마일 연결 시도를 관찰합니다. tcpdump 유틸리티는 리소스 커넥터에서 사용할 수 있습니다. 리소스 커넥터에서 tcpdump [실행 설명서를](#) 참조하십시오.



팁: 커넥터 그룹 구축에서 캡처를 결정적으로 만들려면 리소스에 대한 모든 세션이 이동할 수 있도록 그룹에서 한 개의 리소스 커넥터만 사용하도록 임시로 설정한 다음 애플리케이션 서버 및 포트에서 필터링된 캡처를 실행합니다.

- 예를 들면 다음과 같습니다.

```
tcpdump 'host x.x.x.x and tcp port 443'
```

(여기서 x.x.x.x는 애플리케이션 서버 IP이고 443은 애플리케이션의 포트임)

- 결과를 해석합니다. SYN-ACK가 없는 아웃바운드 SYN은 방화벽 삭제 또는 앱이 수신 대기하지 않음을 나타냅니다. immediate RST는 호스트에 연결할 수 있지만 포트에 바인딩된 항목이 없음을 나타냅니다. 앱으로 향하는 패킷이 전혀 없는 경우 세션이 이 커넥터에 도달하지 않거나 예기치 않은 주소로 확인된 DNS를 나타냅니다.
- 캡처가 완료되면 그룹의 나머지 커넥터를 다시 활성화합니다.

원인

- 커넥터-앱 트래픽을 차단하는 방화벽: 네트워크 또는 호스트 기반 방화벽은 커넥터 호스트 IP와 애플리케이션 서버 IP 간의 필수 포트를 차단합니다.
- 보안 액세스에서 개인 리소스 구성 불일치: 프라이빗 리소스 정의(Resources > Private Resources)에 구성된 IP, FQDN 또는 포트가 애플리케이션이 실제로 수신하는 것과 일치하지 않습니다(예: 앱이 새 IP로 이동했거나 8443에서 수신하지만 443은 구성됨).
- 커넥터에 대한 DNS 확인 실패: 프라이빗 리소스는 FQDN으로 정의되지만 커넥터 DNS 서버가 프라이빗 애플리케이션 FQDN을 확인하지 않습니다.
- 응용 프로그램 서버 작동 중지 또는 수신 안 함: 서버가 다른 방법으로 정상으로 표시되지만 예상 포트에 바인딩되지 않았거나 호스트가 작동 중인 동안 서비스가 중단되었습니다.
- 커넥터 풀에서 부분적으로 연결 가능: 풀에 있는 하나 이상의 커넥터가 애플리케이션에 도달할 수 없는 네트워크 세그먼트에 있으므로 해당 커넥터에 할당된 세션만 실패합니다.

관련 콘텐츠

- [Cisco Secure Access에 대한 기본 정보 트러블슈팅 및 수집](#)
- [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.