보안 액세스와 FortiGate 방화벽 간에 IPSec 터널 인증 실패

문제

Cisco Secure Access와 FortiGate 방화벽 간에 인증 오류가 발생하여 IPSec 터널 설정이 실패했습니다. PSK(Pre-Shared Keys)가 양쪽에서 일치하는지 확인했음에도 불구하고 FortiGate 방화벽 디버그 로그에 "인증 실패" 메시지가 표시됩니다. 1단계 협상이 INVALID_KE_PAYLOAD 오류로 인해 실패하여 터널이 시작되지 않습니다. 연결 제안이 두 엔드포인트 간에 일치하는 것처럼 보이지만 터널 설정 프로세스가 성공적으로 완료되지 않습니다.

환경

- Cisco 보안 액세스
- FortiGate 방화벽(서드파티에서 관리)
- 예비 기본 및 백업 엔드포인트를 사용한 IPSec 터널 구성

해결

INVALID_KE_PAYLOAD 오류 및 인증 문제를 해결하기 위해 특정 컨피그레이션을 조정하여 IPSec 터널 연결 문제를 해결했습니다.

1단계 DH 그룹 컨피그레이션

1단계 협상을 위해 DH(Diffie-Hellman) 그룹을 하나만 구성합니다. 여러 DH 그룹 또는 이전에 구성한 DH 그룹 14를 사용하는 대신 1단계에서 DH 그룹 20을 설정합니다.

구성 수정

```
config vpn ipsec phase1-interface
    edit "sse-tunnel"
        set dhgrp 20
    next
end
```

NAT 통과 컨피그레이션

IPSec 터널 컨피그레이션에서 NAT-T(NAT Traversal)를 활성화합니다. 이 기능은 이전에 비활성화되었지만 적절한 터널 설정을 위해 활성화해야 합니다.

PFS(Perfect Forward Secrecy) 컨피그레이션

2단계 컨피그레이션에서 PFS(Perfect Forward Secrecy)를 비활성화하여 잠재적인 협상 충돌을 제거합니다.

원인

IPSec 터널 실패는 여러 컨피그레이션 불일치 및 비호환성 때문에 발생했습니다.

- INVALID_KE_PAYLOAD 오류: Cisco Secure Access와 FortiGate 엔드포인트 간의 Diffie-Hellman 그룹 협상 충돌로 인해 1단계 오류가 발생했습니다
- DH 그룹 불일치: 원래 구성에서 DH 그룹 14를 사용하고 구성된 여러 DH 그룹이 Cisco Secure Access 요구 사항과 호환되지 않았습니다.
- NAT 통과 설정: NAT 통과가 비활성화되어 네트워크 환경에서 터널을 제대로 설정하지 못했습니다

관련 콘텐츠

- FortiGate 방화벽으로 보안 액세스 구성
- 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.