IPSec-Tunnelauthentifizierung schlägt fehl zwischen sicherem Zugriff und FortiGate-Firewall

Problem

Der IPSec-Tunnelaufbau zwischen Cisco Secure Access und einer FortiGate-Firewall ist fehlgeschlagen, und es sind Authentifizierungsfehler aufgetreten. In den FortiGate-Firewall-Debug-Protokollen wird trotz Überprüfung, ob die Pre-Shared Keys (PSKs) auf beiden Seiten übereinstimmen, die Meldung "authentication failed" (Authentifizierung fehlgeschlagen) angezeigt. Die Phase-1-Aushandlung schlägt mit einem INVALID_KE_PAYLOAD-Fehler fehl, wodurch der Tunnel nicht hochgefahren werden kann. Die Vorschläge für die Verbindung scheinen zwischen beiden Endpunkten zu stimmen, der Tunnelherstellungsprozess wurde jedoch nicht erfolgreich abgeschlossen.

Umwelt

- Sicherer Zugriff von Cisco
- FortiGate-Firewall (von Drittanbieter verwaltet)
- IPSec-Tunnelkonfiguration mit redundanten primären und Backup-Endpunkten

Auflösung

Das Problem mit der IPSec-Tunnelverbindung wurde durch spezifische Konfigurationsanpassungen behoben, um den Fehler INVALID_KE_PAYLOAD und die Authentifizierungsprobleme zu beheben.

Konfiguration der DH-Gruppe in Phase 1

Konfigurieren Sie nur eine Diffie-Hellman-Gruppe (DH) für die Phase-1-Aushandlung. Legen Sie

die DH-Gruppe 20 auf Phase 1 fest, anstatt mehrere DH-Gruppen oder die zuvor konfigurierte DH-Gruppe 14 zu verwenden.

Konfigurationsreparatur

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

NAT-Überbrückungskonfiguration

Aktivieren Sie NAT-Traversal (NAT-T) in der IPSec-Tunnelkonfiguration. Diese Funktion war zuvor deaktiviert, muss jedoch aktiviert werden, damit der Tunnel ordnungsgemäß eingerichtet werden kann.

Perfekte geheime Weiterleitungskonfiguration

Deaktivieren Sie Perfect Forward Secrecy (PFS) in der Phase 2-Konfiguration, um potenzielle Verhandlungskonflikte zu vermeiden.

Ursache

Der IPSec-Tunnelausfall wurde durch mehrere Konfigurationskonflikte und Inkompatibilitäten verursacht:

- UNGÜLTIGER_KE_PAYLOAD-Fehler: Dieser Fehler in Phase 1 ist auf Diffie-Hellman-Gruppenaushandlungskonflikte zwischen den Cisco Secure Access- und FortiGate-Endpunkten zurückzuführen.
- DH-Gruppen-Diskrepanz: Mehrere konfigurierte DH-Gruppen; die Verwendung der DH-Gruppe 14 in der ursprünglichen Konfiguration war nicht mit den Cisco Secure Access-Anforderungen kompatibel.
- NAT-Überbrückungseinstellungen: NAT Traversal wurde deaktiviert, wodurch die ordnungsgemäße Tunneleinrichtung in der Netzwerkumgebung verhindert wurde.

Verwandte Inhalte

- Konfigurieren des sicheren Zugriffs mit der FortiGate-Firewall
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.