

RAVPN Geolocation-Based Policy Configuration for Secure Firewall FTD Version Anforderungen

Inhalt

[Problem](#)

[Umwelt](#)

[Auflösung](#)

[Ursache](#)

[Verwandte Inhalte](#)

- [Problem](#)
 - [Umwelt](#)
 - [Auflösung](#)
 - [Ursache](#)
 - [Verwandte Inhalte](#)
-

Problem

Eine Zugriffskontrollrichtlinie, die mit geolokationsbasierten Filterregeln für AnyConnect Secure Sockets Layer Virtual Private Network (SSL VPN)-Verbindungen konfiguriert wurde, funktioniert nicht wie erwartet. Die Richtlinie enthält eine Regel, die speziell entwickelt wurde, um AnyConnect SSL VPN-Verbindungen ausschließlich von Saudi-Arabien aus zuzulassen. Die Funktion für eine ortsabhängige Zugriffskontrolle, von der diese Regeln abhängen, um Datenverkehr basierend auf dem Ursprungsland zu identifizieren und zu filtern, funktioniert nicht mit der aktuellen Version 7.0.9 von Cisco Secure Firewall Threat Defense (FTD).

Umwelt

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD) Version 7.0.9
- FirePOWER-Anwendungssteuerung mit Standortbestimmungsdiensten
- AnyConnect SSL VPN-Konfiguration mit standortbezogenen Zugriffskontrollregeln

- Zugriffskontrollrichtlinie mit länderspezifischer Filterung konfiguriert

Auflösung

Die Geolocation-basierte Zugriffskontrollrichtlinie für die RAVPN-Funktion erfordert die FTD-Version 7.7 oder höher, um ordnungsgemäß zu funktionieren. Da in der aktuellen Umgebung FTD Version 7.0.9 ausgeführt wird, ist ein Upgrade erforderlich, um dieses Problem zu beheben.

- FMC-Upgrade-Priorität: Das FMC muss zuerst aktualisiert werden und eine Version ausführen, die der FTD-Zielversion entspricht oder höher ist. Stellen Sie vor dem FTD-Upgrade sicher, dass das FMC entsprechend aktualisiert wird.
- Konfigurations-Backup: Erstellen Sie eine vollständige Sicherung der FMC- und FTD-Konfigurationen, bevor Sie den Upgrade-Prozess starten.
- Wartungsfenster: Planen Sie ein Wartungsfenster ein, da der Upgrade-Prozess einen Neustart des Geräts erfordert und zu einer vorübergehenden Unterbrechung des Datenverkehrs führen kann.
- Prüfung der Versionshinweise: Lesen Sie die Versionshinweise für jede Zwischenversion und die Zielversion, um bekannte Probleme oder Probleme zu identifizieren.

Ursache

Die Funktion für eine ortsabhängige Zugriffskontrollrichtlinie für RAVPN (Remote Access Virtual Private Network) wird erst ab FTD Version 7.7 und höher unterstützt. Die aktuelle FTD-Version 7.0.9 bietet keine Unterstützung für diese Funktion, wodurch verhindert wird, dass die Geolokations-basierten Filterregeln in der Zugriffskontrollrichtlinie ordnungsgemäß funktionieren.

Verwandte Inhalte

- [Konfigurieren von standortbasierten Richtlinien für einen sicheren Schutz vor Bedrohungen durch Firewalls](#)
- [Cisco Secure Firewall Threat Defense - Softwaredownload - Version 7.7.11](#)

- [Upgrade-Planungsleitfaden für Cisco Secure Firewall Management Center](#)
- [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.