

Zieladressen für sicheren Zugriff für Split-Routing-Konfiguration

Inhalt

Problem

Bei der Bereitstellung von Cisco Secure Access (CSA) mit Cisco Secure Client (CSC) auf Windows-Endpunkten in einer Hub-Spoke-Netzwerkarchitektur müssen Unternehmen höchstwahrscheinlich Split-Routing konfigurieren, um zu ermöglichen, dass der Datenverkehr der Spoke-Site direkt über den lokalen Spoke-Internet-Circuit mit CSA verbunden wird, anstatt über den Hub zu laufen. Bei dieser Konfiguration müssen alle Cisco Zieladressen bekannt sein, die bei der Einrichtung des CSA-Tunnels verwendet werden, damit Routingausnahmen (Breakout/Split-Routing) auf Netzwerkgeräten wie Fortigate-Firewalls definiert werden können.

Die spezifische Anforderung besteht darin, alle Zielinformationen (IP-Adressen oder URLs) für CSA-Endpunkte zu identifizieren, die vom CSC bei der Einrichtung von TLS/DTLS-Tunneln verwendet werden. Dadurch wird die ordnungsgemäße Konfiguration von Routing-Richtlinien ermöglicht, die den Hub-Spoke-VPN-Tunnel für den CSA-Verkehr umgehen.

Umwelt

- Cisco Secure Access (CSA)-Bereitstellung
- Cisco Secure Client (CSC) auf Windows-Endgeräten
- Hub-Spoke-Netzwerktopologie mit Fortigate-Firewalls
- TLS-/DTLS-Tunnelverbindung zu CSA

Auflösung

Um Split-Routing für Cisco Secure Access-Verbindungen zu konfigurieren, müssen die in den nächsten Abschnitten beschriebenen Zielinformationen auf dem Fortigate-Gerät konfiguriert werden, damit eine direkte Verbindung zu CSA-Endpunkten möglich ist.

CSA-Zieldomäne und -Ports

Primäre Domäne

`*.vpn.sse.cisco.com`

Erforderliche Ports und Protokolle

- TCP/UDP 443: Verwendung für TLS-/DTLS-Tunnelaufbau
- UDP 500/4500: Verwendet für IPsec-Tunnelaufbau
- TCP 80: Wird für die Sperrungsprüfung von VPN-Zertifikaten verwendet

Fortigate-Konfigurationsansatz

Konfigurieren Sie Routing-Richtlinien auf dem Fortigate-Gerät, um den Datenverkehr für die CSA-Domäne (`*.vpn.sse.cisco.com`) und die angegebenen Ports über den lokalen Spoke-Internetkreis und nicht über den Hub-Spoke-VPN-Tunnel zu leiten. Dadurch wird der in den nächsten Codeausschnitten skizzierte Datenverkehrsfluss aktiviert.

Gewünschter Datenverkehrsfluss

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Anstelle des Datenverkehrs am Hub-Standort

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Wichtige Überlegungen

Die CSA-Verbindungsziele werden während der Laufzeit dynamisch bestimmt, d. h., dass bestimmte IP-Adressen für statische Routing-Konfigurationen nicht vorgegeben werden können. Der domänenbasierte Ansatz mit *.vpn.sse.cisco.com stellt die zuverlässigste Methode zum Konfigurieren von Split-Routing-Richtlinien dar.

Informationen zu den aktuellen Ziel- und Port-Anforderungen finden Sie in der offiziellen Cisco Secure Access-Dokumentation, da diese höchstwahrscheinlich mit neuen Softwareversionen aktualisiert werden.

Ursache

In Hub-Spoke-Netzwerktopologien wird der gesamte Internetdatenverkehr von Spoke-Standorten in der Regel standardmäßig über die Hub-Website geroutet. Bei der Implementierung von CSA mit CSC führt dieses Standard-Routing-Verhalten dazu, dass der CSA-Tunnel-Datenverkehr durch den Hub-Standort geleitet wird, bevor er die CSA-Endpunkte erreicht, was zu Latenz und ineffizienter Bandbreite führen kann. Die dynamische CSA-Endpunktauswahl erfordert domänenbasierte Routing-Richtlinien anstelle statischer IP-basierter Regeln, um eine ordnungsgemäße Split-Routing-Funktionalität sicherzustellen.

Verwandte Inhalte

- [Cisco Secure Access-Dokumentation - Verbindungsanforderungen](#)
- [Cisco Secure Access-Dokumentation - Netzwerkkonfiguration](#)

- [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.