Cisco Secure Access Traffic Steering-Konfiguration und Client-Synchronisierung

Inhalt

Problem

Beim Überprüfen der Cisco Secure Access Traffic Steering-Konfiguration werden in den VPN-Profileinstellungen und XML-Dateien keine Ziel-IP-Adressen oder -Domänen angezeigt, die für die Steuerung des Datenverkehrs konfiguriert sind. Dies führt zu Verwirrung darüber, wie der Secure Access-Client Datenverkehrsziele für Steuerungsentscheidungen bestimmt und wie Konfigurationsänderungen, die im Verwaltungsportal vorgenommen werden, mit dem Client synchronisiert werden.

Insbesondere stellen Administratoren fest, dass die Einstellungen für die Verkehrssteuerung zwar über die VPN-Profilverwaltungsschnittstelle konfiguriert werden, die entsprechenden XML-Dateien für VPN-Profile jedoch keine sichtbaren Einträge für die Zieladressen oder Domänen enthalten, die der Steuerung des Datenverkehrs unterliegen sollten.

Umwelt

- Cisco Secure Access Lösung
- VPN-Profilkonfiguration mit aktivierter Verkehrssteuerung
- Bereitstellung eines sicheren Zugriffs-Clients

Auflösung

Die Verkehrssteuerung in Cisco Secure Access erfolgt über einen dynamischen Mechanismus zur Regelbereitstellung und nicht über statische Einträge in der VPN-Profil-XML. Im Folgenden wird erklärt, wie dieser Prozess funktioniert und wie die Konfiguration validiert wird:

Zustellprozess für Datenverkehrssteuerungsregel

Regeln für die Datenverkehrssteuerung werden nicht in der XML-Datei für das VPN-Profil gespeichert, die Administratoren anzeigen können. Stattdessen werden diese Regeln beim Aufbau der VPN-Verbindung dynamisch vom Head-End für sicheren Zugriff an den Client weitergeleitet. Der Prozess funktioniert wie folgt:

1. Wenn eine VPN-Verbindung hergestellt ist, überträgt das Secure Access-Headend die aktuellen Verkehrslenkungsregeln (Split-Tunnel) an den verbindenden Client
2. Der Client empfängt diese Regeln und schreibt sie direkt in die Routing-Tabelle des lokalen Clients
3. Entscheidungen zur Steuerung des Datenverkehrs basieren auf den Einträgen in der Client-Routing-Tabelle und nicht auf den im VPN-Profil-XML sichtbaren Informationen.

Synchronisierung von Konfigurationsänderungen

Änderungen an den Einstellungen für die Verkehrssteuerung im Managementportal folgen einem bestimmten Synchronisierungsmuster:

- Konfigurationsänderungen, die im Management-Portal vorgenommen werden, werden während einer aktiven VPN-Sitzung nicht wirksam.
- Beim nächsten VPN-Verbindungsaufbau werden neue Regeln für die Datenverkehrssteuerung angewendet.
- Um das Verhalten nach den Konfigurationsänderungen für die Datenverkehrssteuerung zu überprüfen, muss die VPN-Verbindung getrennt und erneut verbunden werden.

Validierungsschritte

So validieren Sie Änderungen an der Datenverkehrssteuerung:

1. Nehmen Sie die gewünschten Änderungen an den Einstellungen für die Datenverkehrssteuerung im Secure Access Management-Portal vor.
2. Trennen Sie die bestehende VPN-Verbindung des Clients.
3. Schließen Sie das VPN wieder an, um die aktualisierten Verkehrslenkungsregeln zu erhalten.
4. Überprüfen Sie die Client-Routing-Tabelle, um sicherzustellen, dass die neuen Regeln

angewendet wurden.

Ursache

Das offensichtliche Fehlen von Traffic-Steering-Zielen in der VPN-Profil-XML-Datei ist vom Design her ausreichend. Cisco Secure Access verwendet ein dynamisches Regelbereitstellungssystem, bei dem Traffic-Steering-Regeln zum Zeitpunkt der Verbindung an den Client übermittelt und durch Einträge in der Routing-Tabelle implementiert werden, anstatt als sichtbare Konfigurationselemente in der Profil-XML gespeichert zu werden. Diese Architektur ermöglicht Richtlinienaktualisierungen in Echtzeit und eine zentrale Kontrolle bei gleichzeitiger Wahrung der Sicherheit und Leistung.

Verwandte Inhalte

- ASA-Konfigurationsleitfaden für Split-Tunneling
- 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.