

Secure Access Traffic Steering Behavior and Exception List Configuration

Inhalt

Problem

Benutzer benötigen eine Klarstellung zum Cisco Secure Access Traffic Steering-Verhalten, wenn sie die Einstellung ZTA verwenden, um alle Internetziele mit Standard-Ausnahmekonfigurationen zu sichern. Spezifische Fragen ergeben sich zu:

- Legt fest, ob die Entscheidungen zur Steuerung des Datenverkehrs auf den Ziel-IP-Adressen nach der DNS-Auflösung basieren.
- Wie der DNS-Datenverkehr selbst im Steuerungsprozess behandelt wird.
- Legt fest, ob zusätzliche lokale Domäneneinträge konfiguriert werden müssen, die über den lokalen Standarddomäneneintrag in der Ausnahmeliste hinausgehen.

Die betreffende Konfiguration finden Sie unter: Verbinden > Endbenutzerverbindungen > Zugriff ohne Vertrauen > (Zugriffsprofile ohne Vertrauen) > Sicherer Internetzugriff > Verkehrssteuerung > ZTA zum Sichern aller Internetziele verwenden

Die Standard-Ausnahmeliste umfasst private IP-Adressbereiche (Klasse A, B und C) und die lokale Domäne ".local". Benutzer müssen das Betriebsverhalten dieser Einstellungen verstehen.

Umwelt

- Sicherer Zugriff von Cisco
- ZTA-Konfiguration (Zero Trust Access)
- Verkehrslenkung aktiviert
- Standard-Ausnahmeliste mit privaten IP-Bereichen und .local-Domäne

Auflösung

Die Cisco Secure Access-Verkehrssteuerung funktioniert wie folgt:

Entscheidungsfindungsprozess für die Datenverkehrssteuerung

Entscheidungen zur Steuerung des Datenverkehrs werden auf Basis der Ziel-IP-Adresse nach der DNS-Auflösung getroffen. Das System wertet die tatsächliche Ziel-IP aus, die sich aus der DNS-Namensauflösung ergibt, um zu bestimmen, ob der Datenverkehr durch den Security Stack mit nicht vertrauenswürdigen Zugriff geleitet werden muss.

Verarbeitung von DNS-Datenverkehr

DNS-Abfragen selbst unterliegen nicht der Steuerung des Datenverkehrs. Wenn Endpunkte DNS-Serverzuweisungen über DHCP erhalten, die auf interne DNS-Server verweisen (in der Regel mit privaten IP-Adressen), wird diese DNS-Kommunikation an der Steuerung des Datenverkehrs vorbeigeleitet und lokal verarbeitet.

Konfiguration der Ausnahmeliste

Die Standard-Ausnahmeliste umfasst:

- Private IP-Adressbereiche (Klasse A: 10.0.0.0/8, Class B: 172.16.0.0/12, Class C: 192.168.0.0/16)
- Die .local-Domäne

Bei Organisationen, die benutzerdefinierte lokale Domänen (interne Domänennamen) verwenden, müssen der Ausnahmeliste weitere Domäneneinträge hinzugefügt werden, um sicherzustellen, dass der interne Datenverkehr nicht unnötig durch den Sicherheitsstapel geleitet wird. Der lokale Standardeintrag (.local) deckt die standardmäßigen lokalen Netzwerkkennungsprotokolle ab, umfasst jedoch möglicherweise nicht alle internen Unternehmensdomänen.

Konfigurationsverifizierung

So überprüfen Sie die ordnungsgemäße Konfiguration:

Navigieren Sie zu Verbinden > Endbenutzerverbindung > Zugriff ohne Vertrauenswürdigkeit > Sicherer Internetzugriff > Datenverkehrssteuerung.

Überprüfen Sie die Ausnahmeliste, um sicherzustellen, dass sie alle erforderlichen privaten IP-Bereiche und lokalen Domännennamen enthält, die für die interne Infrastruktur Ihres Unternehmens spezifisch sind.

Ursache

Dies ist eine Informationsanfrage zum Betriebsverhalten der Cisco Secure Access Traffic Steering-Funktionen. Klärungsbedarf ergibt sich aus der Komplexität der Verkehrssteuerungslogik und der Interaktion zwischen DNS-Auflösung, IP-basierten Routing-Entscheidungen und Mechanismen zur Ausnahmebehandlung.

Verwandte Inhalte

- [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.