

Zugriff auf geobeschränkte Websites, die von der Webanwendungs-Firewall blockiert werden, wenn SSE NATaaS-Ausgangs-IPs verwendet werden

Inhalt

Problem

Versuche, über Cisco Secure Access (SSE) auf eine bestimmte Website zuzugreifen, führen zu einer Blockierungsmeldung mit der Meldung, dass eine Sperrung durchgeführt wurde.

Der Zugriff auf die Site ist möglich, wenn eine normale Wi-Fi-Verbindung zu Hause verwendet wird. Der Grund hierfür ist vermutlich, dass die entfernte Website nur Zugriff von bestimmten IP-Adressbereichen aus erlaubt, während die SSE-Ausgangs-IP außerhalb des zulässigen Bereichs zu liegen scheint.

Technische Untersuchungen haben ergeben, dass die Web Application Firewall (Cloudflare) der Website den gesamten Secure Access NATaaS-Ausgangs-IP-Bereich blockiert, unabhängig vom Land. Das Problem ist reproduzierbar und tritt bei Verwendung von SSE-Ausgangs-IPs konsistent auf.

Umwelt

- Technologie: Cisco Secure Access (SSE) mit Unified Policy (Internetrichtlinien, private Richtlinien, DLP-Richtlinien, RBI, Sicherheitsprofile)
- Zugriffspfad: jedes Rechenzentrum von SSE
- Geografisch beschränkte Websites
- Sicherheitskontrolle: Web Application Firewall (Cloudflare) auf der Zielwebsite
- Internetzugriff von Remote-Netzwerk (SSE Egress IPs) im Vergleich zum lokalen Netzwerk (Wi-Fi zu Hause)
- Keine Änderungen an der Bereitstellung von sicherem Zugriff zum Zeitpunkt des Problems
- Fehlermeldung "sorry you have been blocking" (Entschuldigung, dass Sie blockiert wurden)

Auflösung

Um Zugriffsprobleme zu beheben, die durch Remote-Standorte verursacht werden, die Cisco Secure Access NATaaS-Ausgangs-IPs blockieren, wird dieser Workflow empfohlen. Mit diesen Schritten wird ein methodischer Ansatz zur Identifizierung der Art des Blocks und zur Ermittlung

potenzieller Problemumgehungen oder Lösungen sichergestellt.

Schritt 1: Fehlermeldung bestätigen und Verhalten sperren

Beachten Sie beim Zugriff auf die Site über SSE folgende Meldung:

sorry you have been blocked

Schritt 2: Überprüfung der Website-Zugänglichkeit aus verschiedenen Netzwerken

Rufen Sie die Website auf unter:

- Beliebiges SSE-Rechenzentrum (blockiert)
- Eine normale Wi-Fi-Verbindung zu Hause (zugänglich)

Schritt 3: Identifizieren der Sicherheitskontrolle, die für die Sperrung verantwortlich ist

Technische Beobachtung: Die Cloudflare Web Application Firewall (WAF) blockiert den gesamten Secure Access NATaaS-Ausgangs-IP-Bereich.

Schritt 4: Bestätigung des von Endbenutzern verwendeten Zugriffspfads

Bestimmen Sie die Methode zum Senden von Datenverkehr an Secure Access:

- Roaming-Sicherheitsmodul
- RAVPN-Tunnel
- Site-to-Site-VPN-Tunnel
- PAC-Bereitstellung

Schritt 5: Optionen für Umgehung oder Zulassen von Listen erkunden

Überprüfen Sie, ob eine der folgenden Optionen möglich ist:

- Geschäftsbeziehung oder wenden Sie sich an die Administratoren der Ziel-Website, um eine Zulassungsliste für SSE-Ausgangs-IPs anzufordern.
- Die SSE-Ausgangs-IPs werden im Dokument aufgelistet:
- Alternative Zugriffspfade, die verschiedene Ausgangs-IPs verwenden können, die nicht von der WAF blockiert werden.
- Umgehen problematischer Websites vom SSE-Proxy (die genauen Schritte hängen von der Methode ab, die zum Senden von Datenverkehr an den sicheren Zugriff verwendet wird)

Schritt 6: Dokumentieren der Beobachtungen und der nächsten Schritte

Dokumentieren Sie diese Beobachtungen:

Die Fehlermeldung

Der Zugriffspfad und die entsprechenden Ergebnisse

Kommunikation mit dem Administrator des Remote-Standorts, sofern dies zulässig ist

Ursache

Die Ursache dieses Problems liegt darin, dass die Web Application Firewall (Cloudflare) der Zielwebsite den NATaaS-Ausgangs-IP-Bereich von Cisco Secure Access (SSE) aktiv blockiert. Diese Blockierung ist nicht auf nicht israelische IPs oder Geolokationsfilterung beschränkt. Stattdessen zielt sie auf den gesamten bekannten Ausgangs-IP-Bereich ab, der mit Cisco Secure Access verknüpft ist, wahrscheinlich aufgrund einer Richtlinie oder Sicherheitskonfiguration auf der Remotewebsite. Datenverkehr, der von diesen IP-Adressen ausgeht, wird abgelehnt, unabhängig von seinem tatsächlichen Quell- oder Endbenutzerstandort.

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.