

Toegang tot Geo-Restricted Websites geblokkeerd door Web Application Firewall bij het gebruik van SSE NATaaS Egress IPs

Inhoud

uitgeven

Pogingen om toegang te krijgen tot een specifieke website via Cisco Secure Access (SSE) resulteren in een blokkeringsbericht met de tekst "sorry dat u bent geblokkeerd".

De site is toegankelijk wanneer u een gewone Wi-Fi-verbinding voor thuisgebruik gebruikt. De vermoedelijke oorzaak is dat de externe website alleen toegang biedt vanaf specifieke IP-adresbereiken, terwijl de SSE-uitgang IP buiten het toegestane bereik lijkt te vallen.

Technisch onderzoek toont aan dat de Web Application Firewall (Cloudflare) van de website het volledige Secure Access NATaaS egress IP-bereik blokkeert, ongeacht het land. Het probleem is reproduceerbaar en treedt consequent op bij het gebruik van SSE-uitgang-IP's.

milieu

- Technologie: Cisco Secure Access (SSE) met Unified Policy (internetbeleid, privébeleid, DLP-beleid, RBI, beveiligingsprofielen)
- Toegangspad: elk datacenter van SSE
- Geo-beperkte websites
- Beveiligingscontrole: webtoepassingsfirewall (Cloudflare) op de bestemmingswebsite
- Internettoegang vanaf extern netwerk (SSE-uitgang IP's) versus lokaal netwerk (Wi-Fi thuis)
- Geen wijzigingen in de implementatie van Secure Access op het moment van het probleem
- Foutmelding: "Sorry dat u bent geblokkeerd"

resolutie

Om toegangsproblemen aan te pakken die worden veroorzaakt door externe sites die Cisco Secure Access NATaaS-IP's blokkeren, wordt deze workflow aanbevolen. Deze stappen zorgen voor een methodische aanpak om de aard van het blok te identificeren en potentiële oplossingen of oplossingen te verkennen.

Stap 1: Bevestig foutmelding en blokgedrag

Let op dit bericht bij het openen van de site via SSE:

sorry you have been blocked

Stap 2: Toegankelijkheid van websites valideren vanuit verschillende netwerken

Toegang tot de website van:

- Elk SSE-datacenter (geblokkeerd)
- Een gewone Wi-Fi-verbinding voor thuis (toegankelijk)

Stap 3: Identificeer de beveiligingscontrole die verantwoordelijk is voor het blokkeren

Technische observatie: Cloudflare Web Application Firewall (WAF) blokkeert het volledige Secure Access NATaaS IP-bereik.

Stap 4: Bevestig het toegangspad dat door eindgebruikers wordt gebruikt

Bepaal de methode voor het verzenden van verkeer naar Secure Access:

- beveiligingsmodule voor roaming
- RAVPN-tunnel
- Site-to-site VPN-tunnel
- PAC-implementatie

Stap 5: Opties voor het omzeilen of toestaan van aanbiedingen verkennen

Controleer of een van deze opties mogelijk is:

- Zakelijke relatie of contact met de beheerders van de bestemmingswebsite om een vermelding van SSE-uitgang-IP's aan te vragen.
- De IP's voor SSE-uitgang worden weergegeven in het document:
- Alternatieve toegangspaden die verschillende IP-adressen kunnen gebruiken die niet zijn geblokkeerd door de WAF.
- Problematische website omzeilen van SSE-proxy (exacte stappen zijn afhankelijk van de gebruikte methode om verkeer naar Secure Access te verzenden)

Stap 6: Documentwaarnemingen en volgende stappen

Documenteer deze waarnemingen:

De foutmelding

Het toegangspad en de bijbehorende resultaten

Communicatie met de beheerder van de externe site indien vermelding is toegestaan.

Oorzaak

De hoofdoorzaak van dit probleem is dat de Web Application Firewall (Cloudflare) van de bestemmingswebsite actief het IP-bereik van Cisco Secure Access (SSE) NATaaS-uitgang blokkeert. Deze blokkering is niet beperkt tot niet-Israëliische IP's of geolocatiefiltering. In plaats daarvan richt het zich op het gehele bekende IP-bereik voor uitgang dat is gekoppeld aan Cisco Secure Access, waarschijnlijk als een kwestie van beleid of beveiligingsconfiguratie op de externe website. Als gevolg hiervan wordt elk verkeer dat afkomstig is van deze IP's geweigerd, ongeacht het land van herkomst of de locatie van de eindgebruiker.

Verwante inhoud

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.