

Acceso a sitios web geo-restringidos bloqueados por firewall de aplicaciones web al utilizar IP de salida NATaaS de SSE

Contenido

Problema

Los intentos de acceder a un sitio web específico a través de Cisco Secure Access (SSE) dan como resultado un mensaje de bloqueo que indica "lamento que se haya bloqueado".

Se puede acceder al sitio cuando se usa una conexión Wi-Fi doméstica normal. La causa sospechosa es que el sitio web remoto sólo permite el acceso desde rangos de direcciones IP específicos, mientras que la IP de salida de SSE parece estar fuera del rango permitido.

La investigación técnica muestra que el firewall de aplicaciones web del sitio web (Cloudflare) está bloqueando todo el intervalo de IP de salida de NATaaS de acceso seguro, independientemente del país. El problema es reproducible y se produce de forma coherente al utilizar IP de salida de SSE.

Entorno

- Tecnología: Cisco Secure Access (SSE) con política unificada (políticas de Internet, políticas privadas, políticas DLP, RBI, perfiles de seguridad)
- Ruta de acceso: cualquier Data Center de SSE
- Sitios web georestringidos
- Control de seguridad: Web Application Firewall (Cloudflare) en el sitio web de destino
- Acceso a Internet desde redes remotas (IP de salida SSE) frente a redes locales (Wi-Fi doméstica)
- No hay cambios en la implementación de Secure Access en el momento del problema
- Mensaje de error observado: "lo sentimos, ha sido bloqueado"

Resolución

Para solucionar problemas de acceso causados por sitios remotos que bloquean las IP de salida de NATaaS de Cisco Secure Access, se recomienda este flujo de trabajo. Estos pasos garantizan un enfoque metódico para identificar la naturaleza del bloque y explorar posibles soluciones o soluciones alternativas.

Paso 1: Confirmar mensaje de error y comportamiento de bloqueo

Observe este mensaje al acceder al sitio a través de SSE:

sorry you have been blocked

Paso 2: Validar la accesibilidad del sitio web desde diferentes redes

Acceda al sitio web desde:

- Cualquier Data Center SSE (bloqueado)
- Conexión Wi-Fi doméstica normal (accesible)

Paso 3: identificar el control de seguridad responsable del bloqueo

Observación técnica: Cloudflare Web Application Firewall (WAF) está bloqueando todo el intervalo IP de salida de NATaaS de Secure Access.

Paso 4: Confirmar la ruta de acceso utilizada por los usuarios finales

Determine el método utilizado para enviar tráfico a Secure Access:

- Módulo de seguridad de roaming
- Túnel RAVPN
- Túnel VPN de sitio a sitio
- implementación de PAC

Paso 5: Explorar las opciones de omisión o permitir listados

Compruebe si alguna de estas opciones es posible:

- Relación empresarial o contacto con los administradores del sitio web de destino para solicitar una lista de direcciones IP de salida de SSE permitidas.
- Las IP de salida de SSE se enumeran en el documento:
- Rutas de acceso alternativas que pueden utilizar diferentes IP de salida no bloqueadas por WAF.
- Omitir el sitio web problemático del proxy SSE (los pasos exactos dependen del método utilizado para enviar tráfico a Secure Access)

Paso 6: Documentar las observaciones y los siguientes pasos

Documente estas observaciones:

El mensaje de error

La ruta de acceso y los resultados correspondientes

Comunicaciones con el administrador del sitio remoto si se permite la inclusión en la lista.

Causa

La causa principal de este problema es que el firewall de aplicaciones web (Cloudflare) del sitio web de destino está bloqueando activamente el intervalo IP de salida de NATaaS de Cisco Secure Access (SSE). Este bloqueo no se limita a las IP no israelíes ni al filtrado de geolocalización. Más bien, se dirige a todo el intervalo IP de salida conocido asociado a Cisco Secure Access, probablemente como una cuestión de configuración de seguridad o política en el sitio web remoto. Como resultado, se deniega todo el tráfico que se origine en estas IP, independientemente de su país de origen real o ubicación de usuario final.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).