

Acesse sites restritos geograficamente bloqueados pelo firewall do aplicativo Web ao usar IPs de saída SSE NATaaS

Contents

Problema

As tentativas de acessar um site específico através do Cisco Secure Access (SSE) resultam em uma mensagem de bloqueio dizendo "desculpe o bloqueio".

O site pode ser acessado ao usar uma conexão Wi-Fi doméstica comum. A causa suspeita é que o site remoto permite acesso apenas de intervalos de endereços IP específicos, enquanto o IP de saída do SSE parece estar fora do intervalo permitido.

A investigação técnica mostra que o Firewall de Aplicativo Web (Cloudflare) do site está bloqueando todo o intervalo de IP de saída de NATaaS de Acesso Seguro, independentemente do país. O problema é reproduzível e ocorre de forma consistente ao usar IPs de saída de SSE.

Ambiente

- Tecnologia: Cisco Secure Access (SSE) com política unificada (políticas da Internet, políticas privadas, políticas DLP, RBI, perfis de segurança)
- Caminho de acesso: qualquer data center do SSE
- Sites Restritos Geograficamente
- Controle de segurança: Firewall de aplicativos da Web (Cloudflare) no site de destino
- Acesso à Internet de rede remota (IPs de saída SSE) versus rede local (Wi-Fi residencial)
- Nenhuma alteração na implantação do Secure Access no momento do problema
- Mensagem de erro observada: "Sorry you have been locked"

Resolução

Para resolver problemas de acesso causados por sites remotos que bloqueiam IPs de saída de NATaaS do Cisco Secure Access, este fluxo de trabalho é recomendado. Essas etapas garantem uma abordagem metódica para identificar a natureza do bloco e explorar possíveis soluções alternativas ou resoluções.

Etapa 1: Confirmar mensagem de erro e bloquear comportamento

Observe esta mensagem ao acessar o site via SSE:

sorry you have been blocked

Etapa 2: Validar a acessibilidade do site de diferentes redes

Acesse o site a partir de:

- Qualquer data center SSE (bloqueado)
- Uma conexão Wi-Fi doméstica comum (acessível)

Etapa 3: Identificar o Controle de Segurança Responsável pelo Bloqueio

Observação técnica: o Firewall de Aplicativo Web (WAF) do Cloudflare está bloqueando todo o intervalo de IP de saída de NATaaS de acesso seguro.

Etapa 4: Confirmar o caminho de acesso usado pelos usuários finais

Determine o método usado para enviar o tráfego para o Secure Access:

- Módulo de segurança de roaming
- Túnel RAVPN
- Túnel VPN site a site
- distribuição de PAC

Etapa 5: Explorar Opções de Ignorar ou Permitir Listagem

Verifique se alguma destas opções é possível:

- Relacionamento comercial ou contato com os administradores do site de destino para solicitar a lista de permissão de IPs de saída SSE.
- Os IPs de saída SSE estão listados no documento:
- Caminhos de acesso alternativos que podem usar diferentes IPs de saída não bloqueados pelo WAF.
- Ignorar site problemático do proxy SSE (as etapas exatas dependem do método usado para enviar tráfego para o Secure Access)

Etapa 6: Documentar observações e próximas etapas

Documente estas observações:

A mensagem de erro

O caminho de acesso e os resultados correspondentes

Comunicações com o administrador do local remoto, se permitido.

Causa

A causa raiz desse problema é que o Firewall de Aplicativo Web (Cloudflare) do site de destino está bloqueando ativamente o intervalo de IP de saída NATaaS do Cisco Secure Access (SSE). Esse bloqueio não está limitado a IPs não israelenses ou filtragem de geolocalização. Em vez disso, ele é direcionado a todo o intervalo de IP de saída conhecido associado ao Cisco Secure Access, provavelmente por uma questão de configuração de política ou segurança no site remoto. Como resultado, qualquer tráfego originário desses IPs é negado, independentemente do país de origem real ou local do usuário final.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.