Access Geo-Restricted Websites Blocked by Web Application Firewall When Using SSE NATaaS Egress IPs

Contents

Issue

Attempts to access specific website through Cisco Secure Access (SSE) result in a block message stating "sorry you

The site is accessible when using a regular home Wi-Fi connection. The suspected cause is that the remote we

Technical investigation shows that the website's Web Application Firewall (Cloudflare) is blocking the entire Secure

Environment

- Technology: Cisco Secure Access (SSE) with Unified Policy (Internet Policies, Private Policies, DLP Policies
- Access Path: Any Data Center of SSE
- Geo-Restricted Websites
- Security Control: Web Application Firewall (Cloudflare) on the destination website
- Internet access from remote network (SSE egress IPs) versus local network (home Wi-Fi)
- No changes to Secure Access deployment at the time of the issue
- Observed error message: "sorry you have been blocked"

Resolution

To address access issues caused by remote sites blocking Cisco Secure Access NATaaS egress IPs, this workflow is

Step 1: Confirm Error Message and Block Behavior

Observe this message when accessing the site via SSE:

```
sorry you have been blocked
```

Step 2: Validate Website Accessibility from Different Networks

Access the website from:

- Any SSE Data Center (blocked)
- A regular home Wi-Fi connection (accessible)

Step 3: Identify the Security Control Responsible for Blocking

Technical observation: Cloudflare Web Application Firewall (WAF) is blocking the entire Secure Access NATaaS e

Step 4: Confirm Access Path Used by End Users

Determine the method used to send traffic to Secure Access:

- Roaming Security Module
- RAVPN Tunnel
- Site-to-site VPN tunnel
- PAC deployment

Step 5: Explore Bypass or Allowlisting Options

Check if any of these options are possible:

- Business relationship or contact with the destination website administrators to request allowlisting of SSE egre
- SSE egress IPs are listed in the document:
- Alternate access paths that can use different egress IPs not blocked by the WAF.
- Bypass problematic website from SSE proxy (exact steps depend of method used to send traffic to Secure Acc

Step 6: Document Observations and Next Steps

Document these observations:

The error message

The access path and corresponding results

Communications with the remote site administrator if allowlisting.

Cause

The root cause of this issue is that the destination website's Web Application Firewall (Cloudflare) is actively blocki
Israeli IPs or geolocation filtering. Rather, it targets the entire known egress IP range associated with Cisco Secure A

Related Content

- Cisco Technical Support & Downloads