Geographic Access Restriction for Zero Trust Access and VPN Connections

Contents

Issue

Organizations requiring geographic access restrictions for Zero Trust Access (ZTA) and VPN connections can find that existing ZTA and VPN policies need to be disabled when attempting to implement country-based access controls. Users experience complete loss of access to required resources when policies are disabled due to the inability to locate native geographic restriction options within the Secure SSE product interface. The specific requirement to restrict access to connections originating only from within a particular country cannot be configured using built-in product capabilities, resulting in widespread user impact when existing policies are deactivated in an attempt to implement such restrictions.

Environment

- Cisco Secure Access Service Edge (SASE) / Secure SSE product
- Zero Trust Access (ZTNA) implementation
- VPN services requiring geographic access control
- Private resource access policies
- Organization requiring country-specific access restrictions

Resolution

The Cisco Secure SSE product does not currently provide native functionality to restrict private resource access based on user geographic location or country. The approaches described in the next sections can be considered to address this limitation.

Feature Request Submission

A feature request must be submitted to Cisco to add geographic restriction capabilities for ZTA and VPN access. This enhancement request is evaluated by the product team for potential inclusion in future releases. Organizations can work with their Cisco Account Manager to help prioritize such feature requests based on business requirements.

Manual Workaround Consideration

A potential manual workaround involves adding country-specific public IP address ranges as network object groups in access policies.

Step 1: Obtain the country public IP address ranges from the appropriate Regional Internet Registry (RIR).

Step 2: Create network object groups containing the identified IP ranges. Configure network object groups within the access policy configuration to include the specific IP address ranges allocated to the target country.

Step 3: Apply the network object groups to access policies. Modify existing access policies to reference the created network object groups, effectively limiting access to connections originating from the specified IP ranges.

Important Limitations

This manual approach has significant limitations as it relies on static IP range definitions and cannot account for dynamic IP allocations, mobile users, or VPN services that could bypass geographic restrictions. Additionally, this method requires ongoing maintenance to ensure IP range accuracy.

Temporary Policy Management

Until a permanent solution is available, organizations must avoid disabling all ZTA and VPN policies simultaneously. Instead, consider implementing a phased approach where critical access policies remain active while geographic restriction requirements are being addressed through alternative means or awaiting product enhancements.

Cause

The Cisco Secure SSE product architecture does not include native geographic access control capabilities for private resource access. The product access policy framework is designed around user identity, device posture, and network-based controls, but does not incorporate geographic location as a policy enforcement parameter. This represents a product capability gap rather than a configuration issue or software defect.

Related Content

- Cisco Technical Support & Downloads