ZTNA Clientless Source IP Address Restrictions

Contents

Issue

When attempting to implement access control for browser-based applications published via ZTNA Clientless, administrators can find that restricting access based on specific allowlisted public IP addresses is not available as a configuration option. The requirement is to allow access only from designated source IP addresses while blocking all other source IPs for applications accessed through ZTNA Clientless with custom domains.

Environment

- Cisco Secure Access - Zero Trust Network Access (ZTNA)
- ZTNA Clientless (browser-based access)
- Applications published with custom domains
- All software versions affected

Resolution

Source IP address-based access restrictions for ZTNA Clientless URLs are not supported in the Cisco Secure Access platform. This limitation applies to all applications published through ZTNA Clientless, regardless of whether they use custom domains or standard ZTNA URLs.

The ZTNA Clientless architecture does not provide the capability to implement IP-based access control lists or allowlisting functionality at the application level. Access control is managed through other authentication and authorization mechanisms within the Zero Trust framework, such as:

- User identity verification
- Device posture assessment

- Multi-factor authentication
- Application-specific policies

Organizations requiring source IP-based access control possibly need to consider alternative approaches or wait for future product enhancements that can include this functionality.
Kindly reach out to Cisco Accounts Team for file a Feature enhancement request.

Cause

The ZTNA Clientless service architecture does not include source IP address filtering capabilities as part of its current feature set. This is a product limitation rather than a configuration issue.

Related Content

- Cisco Technical Support & Downloads