Secure Access Traffic Steering Behavior and Exception List Configuration

Contents

Issue

Users require clarification on Cisco Secure Access Traffic Steering behavior when using the **Use ZTA to secure all internet destinations** setting with default Exception configurations. Specific questions arise regarding:

- Whether traffic steering decisions are based on post-DNS resolution destination IP addresses.
- How DNS traffic itself is handled in the steering process.
- Whether additional local domain entries need to be configured beyond the default .local domain entry in the Exception list.

The configuration in question is located at: **Connect > End User Connectivity > Zero Trust Access > (Zero Trust Access Profiles) > Secure Internet Access > Traffic Steering > Use ZTA to secure all internet destinations**

The default Exception list includes private IP address ranges (Class A, B, and C) and the .local domain, and users need to understand the operational behavior of these settings.

Environment

- Cisco Secure Access
- Zero Trust Access (ZTA) configuration
- Traffic Steering feature enabled
- Default Exception list containing private IP ranges and .local domain

Resolution

The Cisco Secure Access Traffic Steering behavior operates as follows:

Traffic Steering Decision Process

Traffic steering decisions are made based on the destination IP address after DNS resolution. The system evaluates the actual destination IP that results from DNS name resolution to determine whether traffic must be steered through the Zero Trust Access security stack.

DNS Traffic Handling

DNS queries themselves are not subject to traffic steering. When endpoints receive DNS server assignments via DHCP that point to internal DNS servers (typically using private IP addresses), these DNS communications bypass the traffic steering mechanism and are handled locally.

Exception List Configuration

The default Exception list includes:

- Private IP address ranges (Class A: 10.0.0.0/8, Class B: 172.16.0.0/12, Class C: 192.168.0.0/16)
- The .local domain

For organizations using custom local domains (internal domain names), additional domain entries must be added to the Exception list to ensure internal traffic is not unnecessarily steered through the security stack. The default .local entry covers standard local network discovery protocols but possibly do not encompass all organizational internal domains.

Configuration Verification

To verify proper configuration:

Navigate to **Connect > End User Connectivity > Zero Trust Access > Secure Internet Access > Traffic Steering**.

Review the Exception list to ensure it includes all necessary private IP ranges and local domain names

specific to the internal infrastructure of your organization.

Cause

This is an informational request regarding the operational behavior of Cisco Secure Access Traffic Steering features. The need for clarification arises from the complexity of traffic steering logic and the interaction between DNS resolution, IP-based routing decisions, and exception handling mechanisms.

Related Content

- Cisco Technical Support & Downloads