Azure-hosted FQDN Connectivity Issues Through Secure Access with Meraki Integration

Contents

Issue

Specific Azure-hosted FQDNs become unreachable when user traffic is routed through Meraki to Cisco Secure Access, despite Secure Access logs showing the traffic as "allowed." The issue primarily affects RDP connectivity using non-standard ports to these FQDNs.

When searching logs by FQDN in the Secure Access portal, only DNS Security logs are displayed showing "allowed" status. However, RDP connectivity to the same destinations on non-standard ports fails. When the FQDN is resolved to an IP address and Activity Search uses the destination IP, Cloud Firewall logs that had been blocking traffic are revealed.

Environment

- Cisco Secure Access (SSE) with Meraki integration
- Meraki Dashboard with local breakout capability
- Azure-hosted development resources requiring RDP access on non-standard ports
- Traffic routing through Meraki tunnel to Secure Access

Resolution

Immediate Workaround

Add the affected FQDNs to Meraki local breakout rules to bypass Secure Access for the specific destinations detailed in the next sections.

Step 1: Access Meraki Dashboard

Navigate to the Meraki Dashboard and locate the local breakout configuration section.

Step 2: Configure Local Breakout Rules

Add the problematic FQDNs to the local breakout rules to bypass Secure Access routing. This configuration change immediately restores access for affected users by routing traffic directly from Meraki to the internet, bypassing the Secure Access tunnel.

Troubleshooting and Analysis

Step 1: Log Analysis by FQDN

Search Secure Access Activity logs using the FQDN. This primarily shows DNS Security logs and can display the "allowed" status for web traffic on port 443.

Step 2: Log Analysis by Destination IP

Resolve the FQDN to its IP address and search Activity logs using the destination IP instead of the FQDN. This reveals Cloud Firewall logs that show blocked traffic, providing the actual traffic disposition.

Step 3: Verify Traffic Flow

Confirm that the issue occurs only when traffic follows the path: **User → Meraki → Tunnel → Secure Access → Internet**. Test that bypass via local breakout resolves the connectivity problem.

Long-term Resolution

The observed behavior has been identified as expected functionality within the current Secure Access implementation. A feature request (FR CSE-I-5543) has been opened to address the visibility and functional concerns related to:

- Discrepancy between FQDN-based and IP-based log searches
- Inconsistent traffic disposition reporting between DNS Security and Cloud Firewall logs
- Improved visibility for RDP traffic on non-standard ports

Cause

The issue stems from a discrepancy in how Secure Access processes and reports traffic for Azure-hosted FQDNs when accessed via RDP on non-standard ports. When searching logs by FQDN, the system primarily displays DNS Security logs showing "allowed" status for web traffic (typically port 443). However, the actual RDP traffic on non-standard ports is being processed by Cloud Firewall rules, which are only visible when searching by the resolved destination IP address rather than the FQDN.

This creates a visibility gap where administrators see "allowed" traffic in FQDN-based searches while the actual RDP connections are being blocked by firewall policies that are only apparent in IP-based log searches. The behavior is currently considered expected functionality, but a feature request has been submitted to improve the visibility and consistency of traffic reporting across different search methods.

Related Content

- Cisco Technical Support & Downloads