Verify Bypass Behavior Feature for Secure Access Microsoft 365 Compatibility

Contents

Issue

When configuring Cisco Secure Access with Microsoft 365 Compatibility feature enabled, there is uncertainty about whether specific Microsoft-related Fully Qualified Domain Names (FQDNs) are automatically bypassed from Secure Web Gateway (SWG) processing and TLS decryption. Specifically, clarification is needed regarding the bypass behavior for these domains:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

The primary concern centers around whether these domains require manual addition to the Do Not Decrypt List or if they are automatically excluded when Microsoft 365 Compatibility is enabled. Additionally, there is confusion about the interaction between SWG-level bypasses and IPS-level decryption settings, particularly for manage.microsoft.com which appears in documentation suggesting manual Do Not Decrypt List configuration can still be required.

Environment

- Cisco Secure Access
- Microsoft 365 Compatibility feature enabled
- Secure Web Gateway (SWG) inspection and TLS decryption configured
- IPS decryption policies in use
- Microsoft management and update services requiring connectivity

Resolution

The Microsoft 365 Compatibility feature behavior was verified through laboratory testing with these

findings:

Microsoft 365 Compatibility Feature Scope

The Microsoft 365 Compatibility feature exempts Microsoft 365-related domains marked as "Optimize" and "Allow" in Microsoft's endpoint categories from SWG inspection and policy enforcement. This allows traffic to those domains to pass through unaltered at the SWG layer.

Laboratory Testing Results

Testing was conducted in a controlled lab environment with Microsoft 365 Compatibility enabled. This behavior was observed for the specified FQDNs:

Step 1: Enable Microsoft 365 Compatibility Feature

The Microsoft 365 Compatibility feature was activated in the Secure Access configuration.

Step 2: Test Traffic to Target FQDNs

Web traffic was generated to each of the three FQDNs using a standard internet browser:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Step 3: Verify Bypass Behavior in Dashboard

Analysis of the Secure Access dashboard confirmed that web traffic inspection and decryption were not occurring for traffic to these specific destinations when the Microsoft 365 Compatibility feature was enabled.

Step 4: Confirm DNS Steering Behavior

DNS traffic to these destinations continued to be steered through Secure Access, which aligns with documented behavior unless a specific DNS exemption is configured.

Key Behavioral Findings

Based on the testing results and documentation analysis:

- **SWG Bypass:** The three specified FQDNs are bypassed from web traffic inspection when Microsoft 365 Compatibility is enabled.
- **TLS Decryption:** Decryption is bypassed at the SWG layer for these domains.
- **DNS Steering:** DNS queries continue to be processed through Secure Access unless explicitly exempted.
- **Domain Coverage:** While "*.microsoft.com" as a whole domain is not entirely bypassed by specification, the specific URLs tested are bypassed in practice.

IPS Layer Considerations

The Microsoft 365 Compatibility feature operates at the SWG layer. For IPS-level decryption bypass, manual configuration can still be required:

- If IPS decryption bypass is also desired for these domains, manual addition to the Do Not Decrypt List can be necessary.
- The Do Not Decrypt List primarily affects IPS-side decryption rather than SWG processing.
- This explains why documentation can reference adding manage.microsoft.com to the Do Not Decrypt List even when Microsoft 365 Compatibility is enabled.

Cause

The confusion arises from the layered architecture of Cisco Secure Access, where Microsoft 365 Compatibility affects SWG-level processing, while IPS decryption operates as a separate layer with its own configuration requirements. The Microsoft 365 Compatibility feature automatically handles SWG bypass for qualifying Microsoft domains, but IPS decryption policies can require separate configuration through the Do Not Decrypt List.

Related Content

- Cisco Secure Access Microsoft 365 Compatibility Documentation
- Create Effective Do Not Decrypt List for Cisco Secure Access
- Cisco Technical Support & Downloads