Bypass Microsoft Updates Traffic in Secure Web Appliance

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Microsoft Updates

Bypass Microsoft Updates

- Bypassing Traffic in SWA

Steps to Passthrough Microsoft Updates

Related Content

Introduction

This document describes the steps to Bypass Microsoft Updates Traffic in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SWA administration.

Cisco recommends that you have these tools installed:

- Physical or Virtual SWA
- Administrative Access to the SWA Graphical User Interface (GUI)

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Microsoft Updates

Microsoft Updates are essential patches, security updates, and feature enhancements released by Microsoft for its operating systems and software applications. These updates are crucial for maintaining the security, stability, and performance of computers and network devices. They ensure that systems are protected against vulnerabilities, bugs are fixed, and new features or improvements are integrated into the software.

The impact of Microsoft Updates on proxy servers, such as Cisco SWA, can be significant. These updates often involve downloading large files or numerous smaller files, which can consume considerable bandwidth and processing resources on the proxy. This can lead to congestion, slower network performance, and increased load on the proxy infrastructure, potentially affecting the overall user experience and other critical network operations.

Bypassing Microsoft Update traffic from the proxy can be a safe and effective way to manage these challenges. Since Microsoft Updates are sourced from trusted Microsoft servers, allowing this traffic to bypass the proxy can help reduce the load on the proxy server without compromising network security. This ensures that essential updates are delivered efficiently while preserving proxy resources for other security and content filtering tasks. It is important, however, to implement such bypass configurations carefully to maintain overall network security and compliance with organizational policies.

Bypass Microsoft Updates

If you are considering avoiding proxying Microsoft Updates traffic, there are two main approaches:

1. **Bypass:** This involves configuring the network to redirect the traffic so that it never reaches the SWA.
2. **Passthrough:** This involves configuring the SWA to neither decrypt nor scan the Microsoft Updates traffic, allowing it to pass through the proxy without inspection.

Bypassing Traffic in SWA

To bypass Microsoft Updates traffic in networks equipped with SWA, the approach varies depending on your proxy deployment setup:

Deployment type	**Bypass traffic**
Transparent deployment	You can redirect Microsoft Updates traffic at the router or Layer 4 switches that are responsible for forwarding traffic to the proxy

	server.
	You can configure bypass settings directly within the SWA graphical user interface (GUI).
Explicit deployment	To prevent the Microsoft Updates traffic from reaching the SWA, you must configure the bypass at the source. This means exempting the relevant URLs on the client machines to ensure that the traffic is not redirected to the SWA.

If bypassing specific traffic requires extensive network redesign and is not feasible, an alternative approach is to configure the SWA to pass through certain types of traffic. This can be achieved by setting the SWA to neither decrypt nor scan the designated traffic, allowing it to pass through the proxy without inspection. This method ensures that essential traffic is delivered efficiently while minimizing the impact on network performance and proxy resources.

Steps to Passthrough Microsoft Updates

There are four main stages to configure passthrough for Microsoft Update traffic:

Stage	Steps
1. Create a Custom URL Category for Microsoft Updates URLs	**Step 1.** From **GUI**, Choose **Web Security Manager** and then click **Custom and External URL Categories**. **Step 2.** Click **Add Category** to add a Custom URL Category. **Step 3.** Assign a unique **Category Name**. **Step 4.** (Optional) Add **Description**. **Step 5.** From **List Order**, choose the first category to position on top. **Step 6.** From **Category Type** drop-down list, choose **Local Custom Category.** **Step 7.** Add Microsoft Updates URLs in the **Sites** Section. **Tip**: You can check the list of Microsoft updates from: Step 2 - Configure WSUS | Microsoft Learn **Caution**: Do not Copy/Paste the URLs as are in the

	Microsoft Documents; format them properly as SWA format. For more information, please visit: Configure Custom URL Categories in Secure Web Appliance - Cisco **Step 8. Submit**.
2. Create an Identification Profile to exempt Microsoft Updates traffic from Authentication	**Step 9.** From **GUI**, Choose **Web Security Manager** and then click **Identification Profiles**. **Step 10.** Click **Add Profile** to add a profile. **Step 11.** Use the **Enable Identification Profile** check box to enable this profile, or to quickly disable it without deleting it. **Step 12.** Assign a unique profile **Name**. **Step 13.** (Optional) Add **Description**. **Step 14.** From the **Insert Above** drop-down list, choose where this profile is to appear in the table. **Step 15.** In the **User Identification Method** section, choose **Exempt from authentication/ identification**. **Step 16.** In the **Define Members by Subnet**, If you would like to Passthrough Microsoft traffic for some specific users, enter the IP addresses or Subnets that applies, or else leave this field blank to include all IP address. **Step 17.** From **Advanced** section, choose **Custom URL Categories**. **Step 18. Add** the **Custom URL Category** that was created for Microsoft updates. **Step 19.** Click **Done.** **Step 20. Submit**.
3. Create a Decryption Policy To Passthrough Microsoft Updates Traffic	**Step 21.** From **GUI**, Choose **Web Security Manager** and then click **Decryption Policy**. **Step 22.** Click **Add Policy** to add a Decryption Policy. **Step 23.** Use the **Enable Policy** check box to enable this policy. **Step 24.** Assign a unique Policy **Name**. **Step 25.** (Optional) Add **Description**. **Step 26.** From the **Insert Above Policy** drop-down list, choose the first Policy. **Step 27.** From the **Identification Profiles and Users**, choose the Identification Profile that you created in the previous steps. **Step 28. Submit**.

	Step 29. In the **Decryption Policies** page, under **URL Filtering**, click on the link associated with this new Decryption Policy. **Step 30.** Select **Passthrough** as the action for Microsoft Updates URL category. **Step 31. Submit**.
4. Create an Access Policy to Allow Microsoft Updates Traffic	**Step 32.** From **GUI**, Choose **Web Security Manager** and then click **Access Policy**. **Step 33.** Click **Add Policy** to add an Access Policy. **Step 34.** Use the **Enable Policy** check box to enable this policy. **Step 35.** Assign a unique Policy **Name**. **Step 36.** (Optional) Add **Description**. **Step 37.** From the **Insert Above Policy** drop-down list, choose the first Policy. **Step 38.** From the **Identification Profiles and Users**, choose the Identification Profile that you created in the previous steps. **Step 39. Submit**. **Step 40.** On the **Access Policies** page, under **URL Filtering**, click on the link associated with this new Access Policy **Step 41.** Select **Allow** as the action for the Custom URL category created for the Microsoft Updates. **Step 42. Submit**. **Step 43. Commit** the changes**.**

Related Content

- User Guide for AsyncOS 15.0 for Cisco Secure Web Appliance - GD(General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- How To Exempt Office 365 Traffic From Authentication and Decryption on Cisco Web Security Appliance (WSA) - Cisco
- Use Secure Web Appliance Best Practices - Cisco
- Bypass Authentication in Secure Web Appliance - Cisco