Deployment Guide for Securing Microsoft Office 365

RELEASE 5 | AUGUST 2019

Table of Contents

Preface

GUIDE TYPES

Overview guides provide high-level introductions to technologies or concepts.

Reference architecture guides provide an architectural overview for using Palo Alto Networks® technologies to provide visibility, control, and protection to applications built in a specific environment. These guides are required reading prior to using their companion deployment guides.

Deployment guides provide decision criteria for deployment scenarios, as well as procedures for combining Palo Alto Networks technologies with third-party technologies in an integrated design.

DOCUMENT CONVENTIONS

Notes provide additional information.

Cautions warn about possible data loss, hardware damage, or compromise of security.

Blue text indicates a configuration variable for which you need to substitute the correct value for your environment.

In the **IP** box, enter **10.5.0.4/24**, and then click **OK**.

Bold text denotes:

- Command-line commands;

```
# show device-group branch-offices
```

- User-interface elements.

  In the **Interface Type** list, choose **Layer 3**.

- Navigational paths.

  Navigate to **Network > Virtual Routers**.

- A value to be entered.

  Enter the password **admin**.

Italic text denotes the introduction of important terminology.

An *external dynamic list* is a file hosted on an external web server so that the firewall can import objects.

Highlighted text denotes emphasis.

Total valid entries: 755

ABOUT PROCEDURES

These guides sometimes describe other companies' products. Although steps and screen-shots were up-to-date at the time of publication, those companies might have since changed their user interface, processes, or requirements.

GETTING THE LATEST VERSION OF GUIDES

We continually update reference architecture and deployment guides. You can access the latest version of this and all guides at this location:

https://www.paloaltonetworks.com/referencearchitectures

WHAT'S NEW IN THIS RELEASE

Palo Alto Networks® made the following changes since the last version of this guide:

- Added best practice configuration for security profiles
- Updated App-IDs to content release 8177-5588
- Changed *GlobalProtect™ cloud service* to *Prisma™ Access*
- Changed *Aperture™* to *Prisma SaaS*

Comprehensive revision history for this guide

Purpose of This Guide

This guide provides reference architectures for securing Microsoft Office 365 with the Palo Alto Networks Security Operating Platform.

This deployment guide:

- Provides architectural guidance and deployment details for using Prisma Access (formerly *GlobalProtect cloud service*), Palo Alto Networks next-generation firewalls and Prisma SaaS (formerly *Aperture*) in order to provide visibility, control, and protection to your Office 365 environment.
- Requires that you first read the Reference Architecture Guide for SaaS. The reference architecture guide provides architectural insight and guidance necessary for your organization to plan linkage of pertinent features with the next-generation firewall in a high availability design.

OBJECTIVES

Completing the procedures in this guide, you are able to successfully deploy security policy on Prisma Access and the Palo Alto Networks next-generation firewall in order to provide visibility and control over Office 365. You also enable the following functionality:

- Integration of MineMeld™ to capture IP address and URL information from Microsoft to enhance security policy and provide selective decryption.

AUDIENCE

This deployment guide is written for technical readers, including solution architects and design engineers, who want to deploy the Palo Alto Networks Security Operating Platform in order to secure Microsoft Office 365. It assumes the reader is familiar with the basic concepts of SaaS applications, networking, security, and high availability, as well as a basic understanding of network and internet perimeter architectures.

RELATED DOCUMENTATION

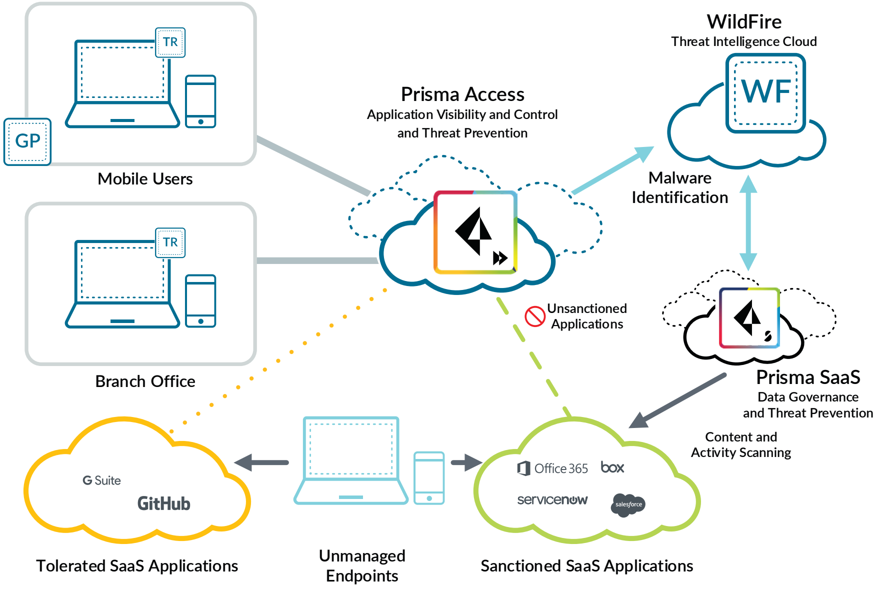
The following documents support this deployment guide:

- Palo Alto Networks Security Operating Platform Overview—Introduces the various components of the Security Operating Platform and describes the roles they can serve in various designs
- Reference Architecture Guide for SaaS—Presents a detailed discussion of the available design considerations and options for securing SaaS applications.

Deployment Overview

This reference architecture describes how the Palo Alto Networks Security Operating Platform allows organizations to gain visibility and control of SaaS application usage, ensure the appropriateness of stored data, and mitigate the risk of data leaks and threat propagation.

Figure 1 Key components of the SaaS reference architecture



The security technologies used throughout this reference architecture include:

- **Prisma Access and Next-Generation Firewall**—Prisma Access (formerly *GlobalProtect cloud service*) and on-premises next-generation firewalls natively inspect all traffic in order to identify applications, threats, and content. Prisma Access protects mobile users and branch offices. The next-generation firewall protects users at campus sites. Prisma Access and the next-generation firewall provide visibility into the use of SaaS applications and the ability to control which SaaS applications are available to your users. They link application traffic to users, regardless of where the users reside or what device type they use. To ensure consistent security posture for all users and all devices regardless of location, the firewall directs mobile device traffic through a next-generation firewall.

- **Prisma SaaS**—Prisma SaaS (formerly *Aperture*) secures sanctioned SaaS applications. Without any configuration on endpoints, it provides complete visibility across all users, folders, and activity within a SaaS application, and it enables detailed analysis and analytics of application use to prevent data risk and compliance violations. More importantly, Prisma SaaS allows granular context-aware policy control within these SaaS applications in order to drive enforcement and quarantine users and data as soon as a violation occurs.

- **Threat Intelligence Cloud**—The integration of the Prisma Access, the next-generation firewall and Prisma SaaS with the Palo Alto Networks WildFire® cloud-based threat-analysis service prevents known and unknown threats from spreading through the sanctioned SaaS applications, effectively cutting off a new insertion point for malware.

Combined, these technologies function as a multi-mode cloud access security broker (CASB), offering in-line and API-based protections working together to minimize the range of cloud risks that can lead to breaches.

In-Line Application Visibility and Control

Prisma Access and the next-generation firewall provide both visibility into the use of SaaS applications on the network and the ability to control users' access to those applications. Key to both visibility and control is App-ID™ functionality. By inspecting the session and payload information of the traffic traversing the firewall, App-ID identifies applications and granular application functionality. App-ID is always enabled in Prisma Access and the next-generation firewall, ensuring advanced visibility to all applications.

App-ID uses traffic-payload information in order to identify applications. Because the vast majority of SaaS applications encrypt the traffic between client and server, to have granular visibility and control to the application, Prisma Access and the next-generation firewall must decrypt the traffic. To provide decryption, the Prisma Access and the firewall insert themselves into the SSL negotiation between the client and the application server. Prisma Access and the firewall send the client their certificate information instead of the application's and the application their certificate information instead of the client's. This allows Prisma Access and the firewall to build separate SSL sessions. One session for the client and one session for the application. This allows the Prisma Access and the firewall to have full visibility and control of the traffic. However, some standalone or "thick" client applications don't operate if the certificate information they receive does not match pinned certificates stored in the client application. To maintain full visibility and control, you should avoid client applications that operate in this manner.

To provide consistent visibility and control for remote users and mobile endpoints, Prisma Access for users ensures that all traffic to the internet and SaaS applications traverses the security service. The GlobalProtect app runs on common PC and mobile endpoint operating systems. Rather than letting traffic go directly between the SaaS client and the SaaS application, the GlobalProtect app sends all mobile user traffic through an always-on connection to Prisma Access. To ensure a quality experience for users, Prisma Access is a distributed global service. Each client will connect to the Prisma Access location that has the best response time relative to their location, preferring in-country locations when available.

SaaS application use is not always consistent organization-wide. To gain visibility and control of who uses SaaS applications, Prisma Access for users maps the username it knows from the mobile user login to an IP address through User-ID™. Prisma Access can also pull the group information for each user from a directory service to enable better reporting and policy definition. When the user is on-premises, the GlobalProtect app can initiate a login-only connection to an internal GlobalProtect gateway to provide a high-fidelity User-ID that is redistributed to on-premises next-generation firewalls. When an internal gateway is not used, the next-generation firewall can also integrate with multiple user information repositories to dynamically map usernames to IP addresses.

Reporting on SaaS application use helps to identify which applications are on the network as well who is using them and how. You can use these reports to define policy and monitor usage compliance. When defining policy, you must decide which applications to allow without restrictions and which applications to block without exception. You can conditionally allow applications that are important but lack data-governance capabilities and those applications controlled by business partners. The list of granular application functions you can limit varies by application. However, common functions include file upload or download. You can also limit who has access to an application or application function based on user and group information.

API-Based Data Visibility and Protection

Prisma SaaS ensures the appropriateness of data stored in sanctioned and managed SaaS applications, and it secures data that is critical to the organization, sensitive, or subject to compliance issues.

Prisma SaaS also provides governance for SaaS application data and usage regardless of whether the owner is an internal or an external user or whether they use an organization's managed endpoints, a personal device, or an endpoint managed by another organization. Because it connects directly to your sanctioned SaaS applications through the application's API, Prisma SaaS even provides governance to data stored in the application before the deployment of the service. As such, Prisma SaaS isn't deployed in-line with application traffic, supporting users who access data from outside of your network and managed endpoints.

Because Prisma SaaS provides visibility into stored data and historical activities, you can explore and investigate them on-demand. Because visibility also extends into the access logs, you can see who accessed your data and when, even if the users were external.

Beyond on-demand visibility, Prisma SaaS automatically assesses risk through content, activity, and security control policies. Content policies scan the content of data for information that is critical, sensitive, or subject to compliance and assign a risk value based on how the data is shared. You can mitigate the risk automatically or manually by quarantining, changing share access, or alerting the owner or an administrator. To highlight the abnormal movement of data out of the SaaS application, you can use activity policies to identify abnormal activity, such as large amounts of downloading or exporting data. Finally, security control policies allow you to monitor the configuration of SaaS applications for misconfigurations that would reduce your security.

Prisma SaaS reports summarize policy violations, capture how sensitive content is exposed, list the top domains to which users are sharing files, identify users who present the greatest risk, and list the most popular file types and risks per file type across managed cloud applications.

Preventing Threats

Within the Security Operating Platform, Prisma Access, the next-generation firewall, Prisma SaaS, Traps™, and the threat intelligence cloud work together to prevent malware threats introduced through SaaS applications.

Prisma Access and the next-generation firewall prevent threats that are transported between your organization and external applications including SaaS. It doesn't matter whether it is a sanctioned or tolerated SaaS application; they provide consistent protection for known threats for mobile and on-premises users. However, access directly to the SaaS application from personal devices or from business partners does not traverse Prisma Access or on-premises next generation firewalls and is not visible at the network perimeter.

To address this exception, Prisma SaaS provides the ability to connect directly to sanctioned SaaS applications through the application's APIs to provide threat prevention and data governance. Because it connects to the SaaS application, Prisma SaaS can prevent threats from reaching unmanaged endpoints, such as personal devices and business partners. It also detects threats as users upload data into the application and scans data stored in the application before deploying Prisma SaaS. This prevention allows you to stop threats before your users or business partners may even attempt to access compromised assets.

All of the components of the Palo Alto Security Operating Platform use WildFire to identify previously unknown malware. When WildFire identifies new malware, regardless of where it was found, going forward all the components of the platform can prevent it.

Microsoft Office 365 Design

Palo Alto Networks Security Operating Platform provides visibility and control, data governance, and threat prevention for Office 365. With the Security Operating Platform, you can secure your Office 365 environment and other SaaS applications using:

- An inline approach with Prisma Access for mobile users and branch offices and on-premises Palo Alto Networks next-generation firewalls to secure inline traffic with deep visibility, segmentation, secure access, and threat prevention. This approach combines user, content, and application inspection features within the next-generation firewall to enable CASB functions. The inspection technology maps users to applications to deliver granular control over cloud application usage regardless of location or device. Other features include application-specific function control, URL, and content filtering, policies based on application risk, DLP, user-based policies, and prevention of known and unknown malware.
- An API approach with Prisma SaaS to connect directly to SaaS applications for data classification, DLP, and threat detection. Prisma SaaS delivers complete visibility and granular enforcement across all user, folder and file activity within sanctioned SaaS applications, providing detailed analysis and analytics on usage without requiring any hardware, software or network changes. It allows granular, context-aware policy control within SaaS applications to drive enforcement and quarantine users and data should a violation occur.

VISIBILITY AND CONTROL OF OFFICE 365

Prisma Access and the next-generation firewall provides visibility and granular control of all applications that traverse the firewall. SaaS applications are just a subset of the applications that App-IDs provide visibility and fine-grained policy control. Prisma Access and the next-generation firewall supports the following App-IDs for Office 365.

Access Control

The following App-IDs provide visibility and control to a user accessing the application. They are used only during the authorization process. Subsequent traffic to the application (such as uploads or downloads) does not match this App-ID.

office365-consumer-access—This App-ID controls the access to the consumer version of Office 365. Its presence in the SaaS reports and logs indicates only that there is access to the application; do not use it as an indicator of traffic quantity.

office365-enterprise-access—This App-ID controls the access to the enterprise version of Office 365. Its presence in the SaaS reports and logs indicates only that there is access to the application; do not use it as an indicator of traffic quantity.

Note

File transfers in some Office 365 applications may match the office365-enterprise-access App-ID.

Office 365 Base Application Support

ms-office365-base—The base App-ID matches the core functionality of the application.

ms-product-activation—This App-ID matches the activation of Microsoft Office 365 software after installation.

ocsp—Online Certificate Status Protocol App-ID.

soap—This App-ID is used to obtain service configuration details.

OneDrive, SharePoint, and Office Online Applications

ms-office-ondemand—This service is no longer offered by Microsoft. Online versions of Office applications do not match this App-ID.

ms-onedrive—This is a container App-ID, and the policy applied to it applies to all of the App-IDs it contains. However, because all of the functional App-IDs do not match Office 365 traffic, use the base App-ID instead of this container.

ms-onedrive-base—The base App-ID matches the core functionality of the application.

ms-onedrive-downloading—Does not match Office 365 application traffic.

ms-onedrive-share—Does not match Office 365 application traffic.

ms-onedrive-uploading—Does not match Office 365 application traffic.

sharepoint-online—The App-ID matches the online versions of Word, Excel, PowerPoint, and OneDrive applications.

sharepoint-online-downloading—Identifies downloading files from the online versions of Word, Excel, PowerPoint, and OneDrive applications.

sharepoint-online-editing—Identifies editing files in the online versions of Word, Excel, PowerPoint, and OneDrive applications.

sharepoint-online-sharing—Identifies sharing files from the online versions of Word, Excel, PowerPoint, and OneDrive applications.

sharepoint-online-uploading—Identifies uploading files to the online versions of Word, Excel, PowerPoint, and OneDrive applications.

Outlook

outlook-web-online—The core Office 365 Outlook application support.

mapi-over-http—Used by standalone Outlook clients to communicate to the server.

ms-exchange—Used by standalone Outlook clients to communicate to the server.

rpc-over-http—Used by standalone Outlook clients to communicate to the server.

activesync—Used by iOS Mail and Calendar to communicate to the server.

Skype for Business

ms-lync—This is a container App-ID, and the policy applied to it applies to all of the App-IDs it contains. However, because all of the functional App-IDs do not match Office 365 traffic, use the base App-ID instead of this container.

ms-lync-apps-sharing—Does not match Office 365 application traffic.

ms-lync-audio—Does not match Office 365 application traffic.

ms-lync-base—The base App-ID matches the core functionality of the application.

ms-lync-content-sharing—Does not match Office 365 application traffic.

ms-lync-file-transfer—Does not match Office 365 application traffic.

ms-lync-video—Does not match Office 365 application traffic.

ms-lync-online—This App-ID matches the additional core functionality of the application.

ms-lync-online-apps-sharing—Does not match Office 365 application traffic.

ms-lync-online-filetransfer—Does not match Office 365 application traffic.

rtcp—Required by the ms-lync-base App-ID and used for media negotiation.

rtp-base—Required by the ms-lync-base App-ID and used for media streaming.

stun—Required by the ms-lync-online App-ID and used for media negotiation.

Teams

ms-teams—The core Office 365 Teams application support

ms-teams-downloading—Identifies downloading files from Teams.

ms-teams-editing—Identifies editing content in Teams.

ms-teams-posting—Identifies posting content to Teams.

ms-teams-sharing—Identifies sharing content from Teams.

ms-teams-uploading—Identifies uploading files to Teams.

DATA GOVERNANCE FOR OFFICE 365

Prisma SaaS scans data stored in Office 365's OneDrive, SharePoint Online, and Exchange to provide data governance and risk mitigation. Prisma SaaS content policies scan content in Office 365. User-activity policies rely upon the actions defined by the SaaS application. The supported actions for this application include the following:

- **Create**—A file or folder was created. (SharePoint and OneDrive)
- **Download**—A file or folder was downloaded. (OneDrive)
- **Edit**—A link on a file, or collaborator on a folder was modified. (SharePoint and OneDrive)
- **Preview**—A file was previewed. (SharePoint and OneDrive)
- **Share**—A file or folder was shared. (OneDrive)
- **Sync**—A folder was marked for sync. (SharePoint)
- **Upload**—A file or folder was uploaded. (SharePoint and OneDrive)

Assumptions and Prerequisites

- The Prisma Access and cloud services plugin version tested in this deployment guide is 1.3.1.
- The PAN-OS® version tested in this deployment guide is 8.1.6.
- The MineMeld version tested in this deployment guide is 0.9.62.
- Prisma Access, next-generation firewalls and Panorama™ must be operational. This guide covers only the policy specific to Office 365 and not the deployment of the firewalls or MineMeld.
- Panorama is required for Prisma Access. For the next-generation firewall, it is optional but recommended that you centralize the security policy configuration across multiple firewalls.

The following SaaS application clients were tested as part of creating the example policies and recommendations:

- Web client on Windows and macOS
- "Thick" standalone clients on Windows and macOS, including:
  - Outlook for Office 365 on Windows 10 and macOS
  - OneDrive on Windows 10 and macOS
  - Skype for Business 2016
- Mobile applications for iOS and Android
  - Mail and Calendar on iOS
  - Outlook on Android
  - OneDrive on iOS and Android
  - Skype for Business on iOS

Caution

The policies shown in this guide are examples. Each client and operating system has unique behavior, and the examples shown in this guide might not support all client implementations. It is highly recommended that you test these policies with the clients you plan to support before implementing the policies in a production environment.

Deployment

Procedures

Configuring Security Profiles

One of the key elements to securing traffic is to inspect the traffic that is allowed by the security rules for threats. Security profiles define the content inspection rules. This section defines best-practice security profiles you should use on traffic to the internet and SaaS applications. To use security profiles, enable decryption, because the firewall cannot inspect encrypted traffic.

1.1 Configure Antivirus Profile

Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. This profile blocks traffic that contains malware.

Note

Email response codes with SMTP (not IMAP or POP3) are used for SMTP, IMAP, and POP3. SMTP 541 response messages are returned to notify that the session was blocked. IMAP and POP3 do not have the same response model. In live deployments, instead of DoS concerns with retries, the endpoints typically stop resending after a small number of sends with timeouts.

Table 1   Antivirus profile settings

Decoder	Action	WildFire action
smtp	reset-both	reset-both
smb	reset-both	reset-both
pop3	reset-both	reset-both
imap	reset-both	reset-both
http	reset-both	reset-both
ftp	reset-both	reset-both

First, create a profile for traffic to the internet.

Step 1: Log in to the Panorama web console.

Step 2: Navigate to **Objects > Security Profiles > Antivirus**.

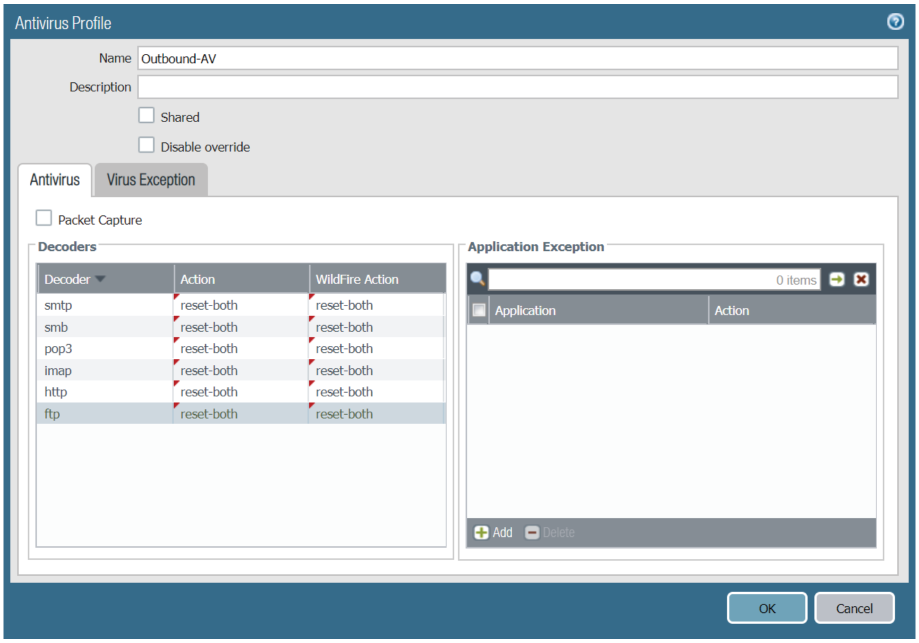
Step 3: In the **Device Group** list, choose **Mobile_User_Device_Group**, and then click **Add**.

Step 4: In the **Name** box, enter **Outbound-AV**.

Step 5: On the Antivirus tab, in the smtp row, in the **Action** list, choose **reset-both**.

Step 6: In the smtp row, in the **Wildfire Action** list, choose **reset-both**.

Step 7: Repeat Step 5-Step 6 for all the rows in Table 1, and then click **OK**.



Antivirus Profile

Name: Outbound-AV

Description:

□ Shared

□ Disable override

□ Packet Capture

Decoders

Decoder	Action	WildFire Action
smtp	reset-both	reset-both
smb	reset-both	reset-both
pop3	reset-both	reset-both
imap	reset-both	reset-both
http	reset-both	reset-both
ftp	reset-both	reset-both

Application Exception

0 items

□ Application	Action

1.2 Create Anti-Spyware Profile

Anti-Spyware profiles block spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.

First, create a profile for traffic to the internet.

Step 1: In **Objects > Security Profiles > Anti-Spyware**, click **Add**.

Step 2: In the **Name** box, enter **Outbound-AS**.

Next, add rule for spyware threats categorized as low or informational that uses the signature's default action.

Step 3: On the Rules tab, click **Add**.

Step 4: In the **Rule Name** box, enter **Default-Low-Info**.

Step 5: In the Severity pane, select **low**, select **informational**, and then click **OK**.

Next, add a rule that blocks spyware threats categorized as critical, high, or medium.

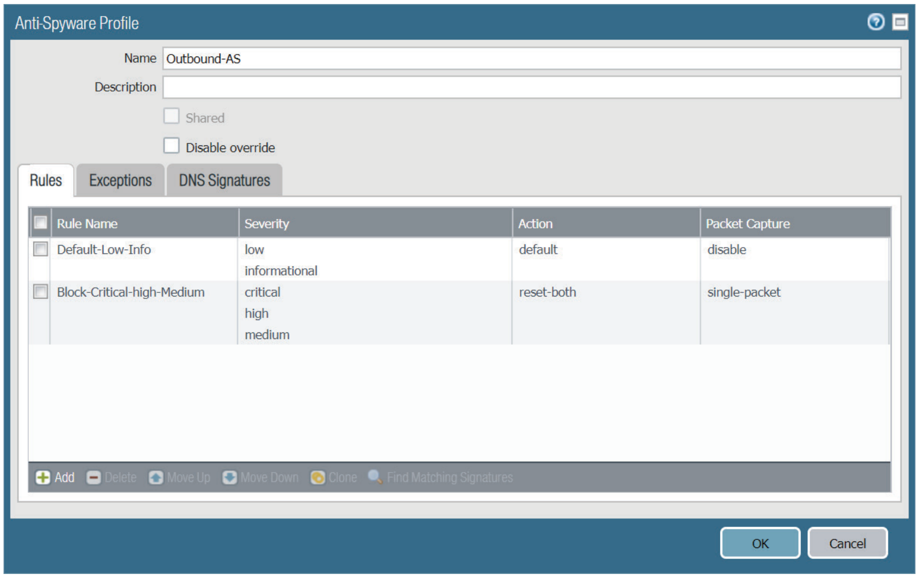
Step 6: On the Rules tab, click **Add**.

Step 7: In the **Rule Name** box, enter **Block-Critical-High-Medium**.

Step 8: In the **Action** list, choose **Rest Both**.

Step 9: In the **Packet Capture** List, choose **single-packet**.

Step 10: In the Severity pane, select **critical**, select **high**, select **medium**, and then click **OK**.



Name: Outbound-AS

Description:

□ Shared

□ Disable override

Rule Name	Severity	Action	Packet Capture
□ Default-Low-Info	low informational	default	disable
□ Block-Critical-high-Medium	critical high medium	reset-both	single-packet

Step 11: On the DNS Signatures tab, in the **Packet Capture** list, choose **single-packet**, and then click **OK**.

1.3 Configure Vulnerability Protection

Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. Although Anti-Spyware profiles help identify infected hosts as traffic leaves the network. Vulnerability Protection profiles protect against threats entering the network.

First, create a profile for traffic to the internet.

Step 1: In **Objects > Security Profiles > Vulnerability Protection**, click **Add**.

Step 2: In the **Name** box, enter **Outbound-VP**.

Next, add rule for vulnerabilities categorized as low or informational that uses the signature's default action.

Step 3: On the Rules tab, click **Add**.

Step 4: In the **Rule Name** box, enter **Default-Low-Info**.

Step 5: In the Severity pane, select **low**, select **informational**, and then click **OK**.

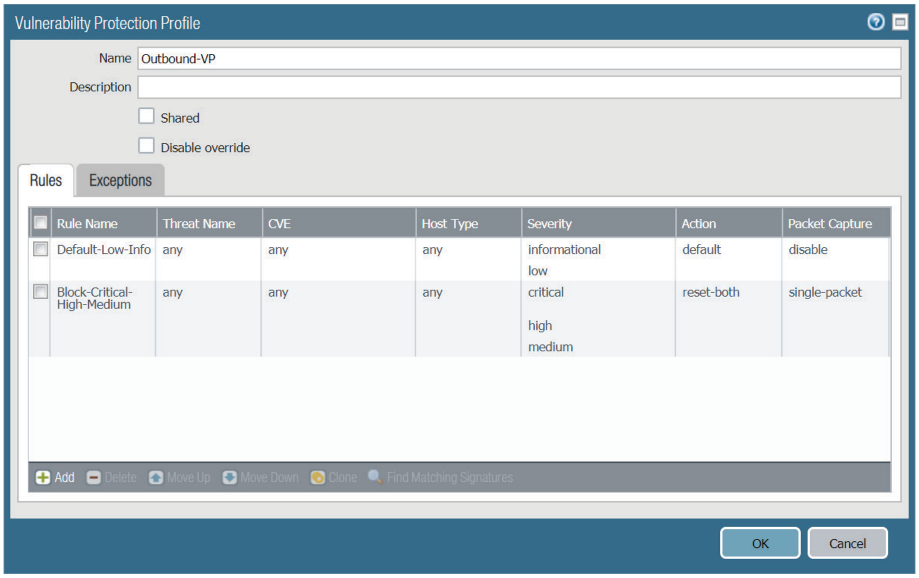
Next, add a rule that blocks vulnerabilities categorized as critical, high, or medium.

Step 6: In the **Rule Name** box, enter **Block-Critical-High-Medium**.

Step 7: In the **Action** list, choose **Reset Both**.

Step 8: In the **Packet Capture** list, choose **single-packet**.

Step 9: In the Severity pane, select **critical**, select **high**, and select **medium**, and then click **OK**.



Name: Outbound-VP

Description:

☐ Shared

☐ Disable override

☐	Rule Name	Threat Name	CVE	Host Type	Severity	Action	Packet Capture
☐	Default-Low-Info	any	any	any	informational low	default	disable
☐	Block-Critical-High-Medium	any	any	any	critical high medium	reset-both	single-packet

Step 10: Click **OK**.

1.4 Create Custom URL Categories

Next, you create placeholders for custom url categories used in security rules and url filtering profiles. Using these placeholder categories prevents the need to modify the default template:

- **Black-List**—Placeholder you use in block rules and objects in order to override default template behavior
- **White-List**—Placeholder you use in permit rules and objects in order to override default template behavior

Step 1: In **Objects > Custom Objects > URL Category**, click **Add**.

Step 2: In the **Name** box, enter **Black-List**, and then click **OK**.

Step 3: In the **Name** box, enter **White-List**, and then click **OK**.

1.5 Create URL Filtering Profile

URL Filtering profiles enable you to monitor and control how users access the internet over HTTP and HTTPS. In this procedure, you block access to URLs that are part of malicious categories.

Table 2 URL categories to block

Category	Site access
command-and-control	block
hacking	block
malware	block
phishing	block
Black-List	block

Step 1: In **Objects > Security Profiles > URL Filtering**, click **Add**.

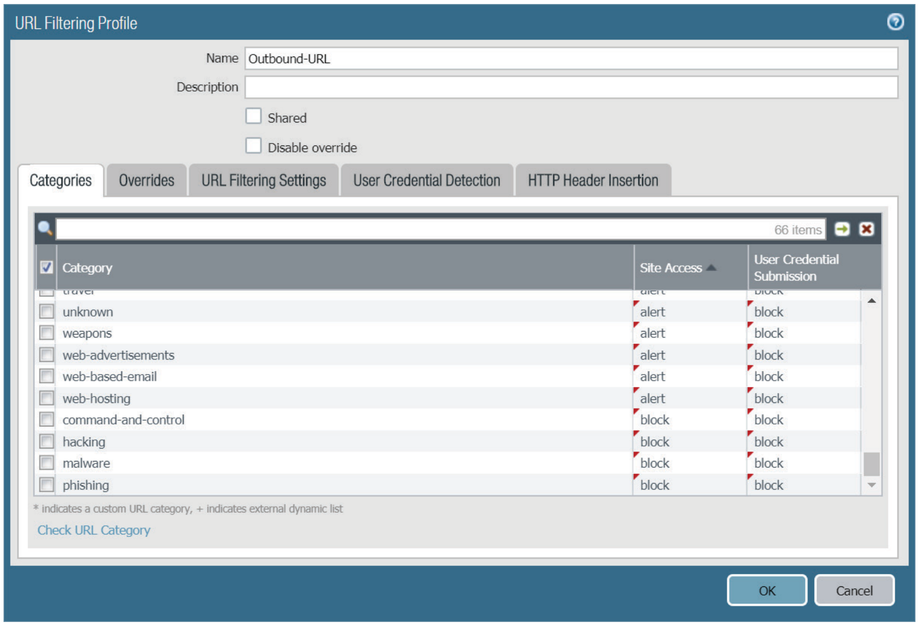
Step 2: In the **Name** box, enter **Outbound-URL**.

Step 3: On the Categories tab, for the category **command-and-control**, in the **Site Access** list, choose **block**.

Step 4: Repeat Step 3 for all the categories in Table 2.

Step 5: For all other categories, in the **Site Access** list, choose **alert**.

Step 6: For all categories, in the **User Credential Submission** list, choose **block**.



URL Filtering Profile

Name Outbound-URL

Description

□ Shared

□ Disable override

☑ Category	Site Access	User Credential Submission
□ travel	alert	block
□ unknown	alert	block
□ weapons	alert	block
□ web-advertisements	alert	block
□ web-based-email	alert	block
□ web-hosting	alert	block
□ command-and-control	block	block
□ hacking	block	block
□ malware	block	block
□ phishing	block	block

* indicates a custom URL category, + indicates external dynamic list

Check URL Category

Step 7: On the URL Filtering Settings tab, select **User-Agent**, select **Referrer**, and then select **X-Forwarded-For**.

Step 8: On the User Credential Detection tab, in the **User Credential Detection** list, choose **Use IP User Mapping**.

Step 9: In the **Valid Username Detected Log Severity** list, choose **high**, and then click **OK**.

1.6 Create File Blocking Profile

Now you create a file-blocking profile that blocks file types known to carry malicious payloads. The following table shows the files types the file-blocking profile blocks in both inbound and outbound traffic.

Table 3 File types to block

File type	Description
7z	7z archive file
bat	Windows BAT
chm	Microsoft Compiled HTML Help
class	Java Class File
cpl	Windows Control Panel File
dll	Windows Dynamic Link Library
hlp	Windows Help File
hta	HTML Application
jar	Java Archive File
ocx	Activex File
pif	Windows Program Information File
scr	Windows Screen Saver File
torrent	Torrent File
vbe	VBScript Encoded File
wsf	Windows Script

Step 1: In **Objects > Security Profiles > File Blocking**, click **Add**.

Step 2: In the **Name** box, enter **Outbound-FB**.

Step 3: Click **Add**.

Step 4: In the **Name** box, enter **Alert-All**.

Step 5: Click **Add**.

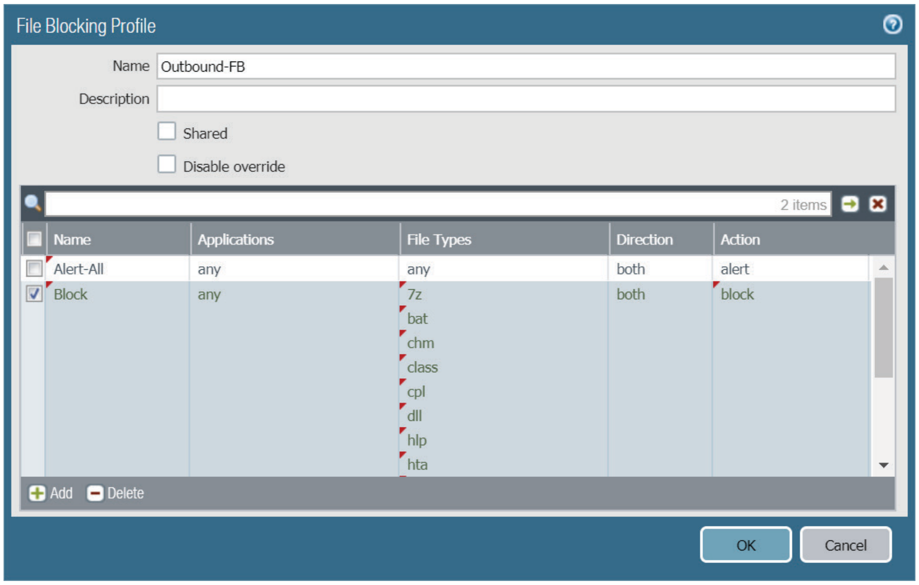
Step 6: In the **Name** box, enter **Block**.

Step 7: In the **File Types** box, click **Add**.

Step 8: In the **File Types** list, choose **7z**.

Step 9: Repeat Step 7-Step 8 for the remaining file types in Table 3.

Step 10: In the **Action** list, choose **block**, and then click **OK**.



File Blocking Profile

Name: Outbound-FB

Description:

□ Shared

□ Disable override

2 items

□	Name	Applications	File Types	Direction	Action
□	Alert-All	any	any	both	alert
☑	Block	any	7z bat chm class cpl dll hlp hta	both	block

1.7 Create WildFire Analysis Profile

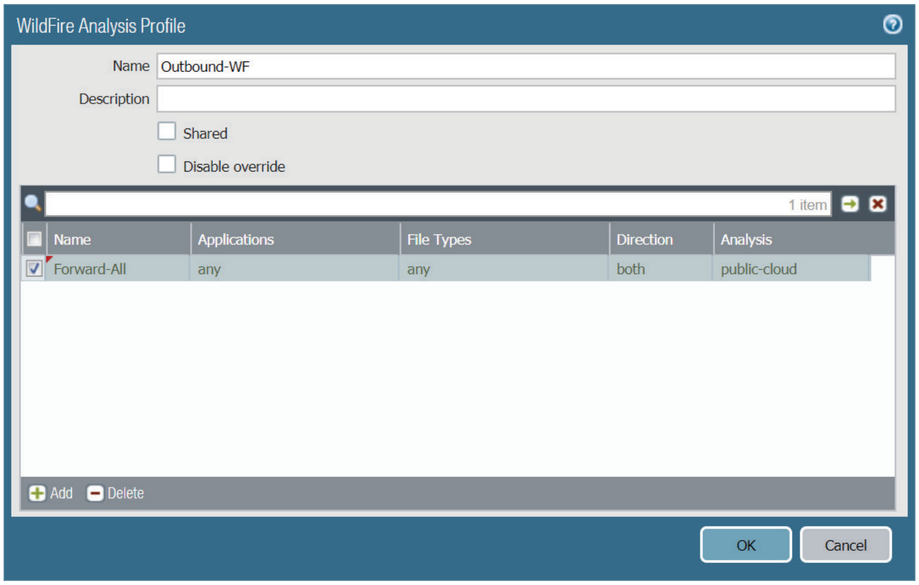
Create a WildFire analysis profile that forwards all unknown files or email links to WildFire for analysis.

Step 1: In **Objects > Security Profiles > WildFire Analysis**, click **Add**.

Step 2: In the **Name** box, enter **Outbound-WF**.

Step 3: Click **Add**.

Step 4: In the **Name** box, enter **Forward-All**, and then click **OK**.



WildFire Analysis Profile

Name: Outbound-WF

Description:

□ Shared

□ Disable override

1 item

☐	Name	Applications	File Types	Direction	Analysis
☑	Forward-All	any	any	both	public-cloud

1.8 Create Security Profile Group

In this procedure, you create a security profile group that combines all of the security profiles you created in this section. The security profile group allows you to add all the security profiles to a security rule by referencing a single object.

Step 1: In **Objects > Security Profile Groups**, click **Add**.

Step 2: In the **Name** box, enter **Outbound**.

Step 3: In the **Antivirus Profile** list, choose **Outbound-AV**.

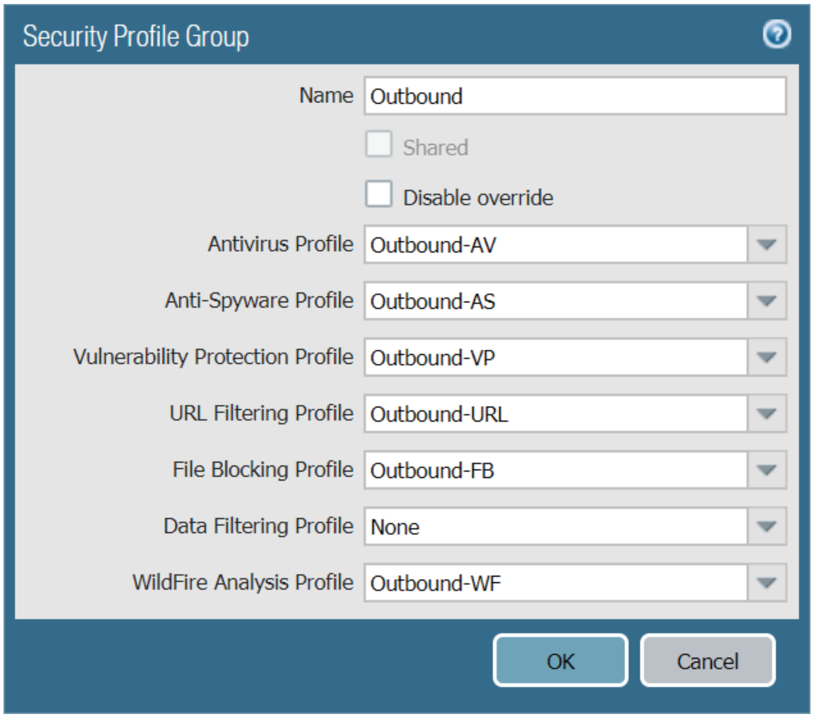
Step 4: In the **Anti-Spyware Profile** list, choose **Outbound-AS**.

Step 5: In the **Vulnerability Protection Profile** list, choose **Outbound-VP**.

Step 6: In the **URL Filtering Profile** list, choose **Outbound-URL**.

Step 7: In the **File Blocking Profile** list, choose **Outbound-FB**.

Step 8: In the **WildFire Analysis Profile** list, choose **Outbound-WF**, and then click **OK**.



Security Profile Group

Name: Outbound

□ Shared

□ Disable override

Antivirus Profile: Outbound-AV

Anti-Spyware Profile: Outbound-AS

Vulnerability Protection Profile: Outbound-VP

URL Filtering Profile: Outbound-URL

File Blocking Profile: Outbound-FB

Data Filtering Profile: None

WildFire Analysis Profile: Outbound-WF

Procedures

Sanctioning or Tolerating Microsoft Office 365

2.1 Sanction Microsoft Office 365

2.2 Limit access to a specific Microsoft Office 365 enterprise instance

2.3 Block Uploads to OneDrive

2.1 Sanction Microsoft Office 365

In this procedure, you allow Office 365 in the security policy and exclude Skype from decryption because the stand-alone clients use certificate pinning.

You should add an **ssl** and **web-browsing** rule in order to allow those App-IDs, because all of the App-IDs for this application explicitly depend on that rule. Because the App-ID shifts after decryption, you cannot use the application-default service. Set the services to **service-http** and **service-https**.

Step 1: In **Policies** > **Security**, add the rules in the following table.

Table 4 Sanctioning Office 365: example security policy rules

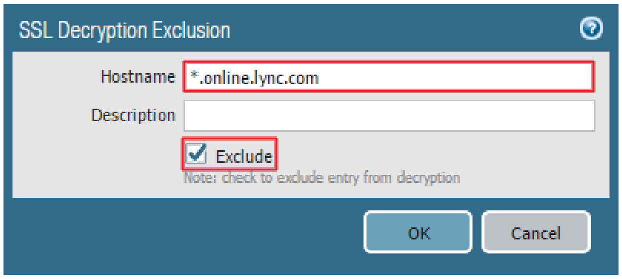
Name	Src Zone	Dst Zone	Application (App-ID)	Service	Action	Policy
Product Activation	Private	Internet	ms-product-activation	application-default	Allow	Outbound
Office 365 Enterprise	Private	Internet	office365-enterprise-access	application-default	Allow	Outbound
Office 365 Base	Private	Internet	ms-office365-base ocsp soap	application-default	Allow	Outbound
OneDrive and Office Online	Private	Internet	ms-onedrive-base sharepoint-online sharepoint-online-downloading sharepoint-online-editing sharepoint-online-sharing sharepoint-online-uploading	application-default	Allow	Outbound
Outlook	Private	Internet	outlook-web-online mapi-over-http ms-exchange rpc-over-http activesync	application-default	Allow	Outbound
Skype for Business	Private	Internet	ms-lync-base ms-lync-online rtcp rtp-base stun	application-default	Allow	Outbound
Teams	Private	Internet	ms-teams ms-teams-downloading ms-teams-editing ms-teams-posting ms-teams-sharing ms-teams-uploading	application-default	Allow	Outbound
SSL and Web	Private	Internet	ssl web-browsing	service-http service-https	Allow	Outbound

Next, exclude Skype for Business from decryption, because the standalone clients have pinned certificates.

Step 2: In **Device** > **Certificate Management** > **SSL Decryption Exclusion**, click **Add**.

Step 3: In the **Hostname** box, enter ***.online.lync.com**.

Step 4: Select **Exclude**, and then click **OK**.



SSL Decryption Exclusion

Hostname: *.online.lync.com

Description:

☑ Exclude

Note: check to exclude entry from decryption

2.2 Limit access to a specific Microsoft Office 365 enterprise instance

To limit login access to specific Office 365 enterprise instances and block access to all other Office 365 enterprise and consumer accounts, configure HTTP header insertion. You configure header insertion through the URL filtering security profile in PAN-OS 8.1. Header insertion also requires that the firewall decrypt the Office 365 traffic.

Step 1: In **Objects > Security Profiles > URL Filtering**, click **Outbound-URL**.

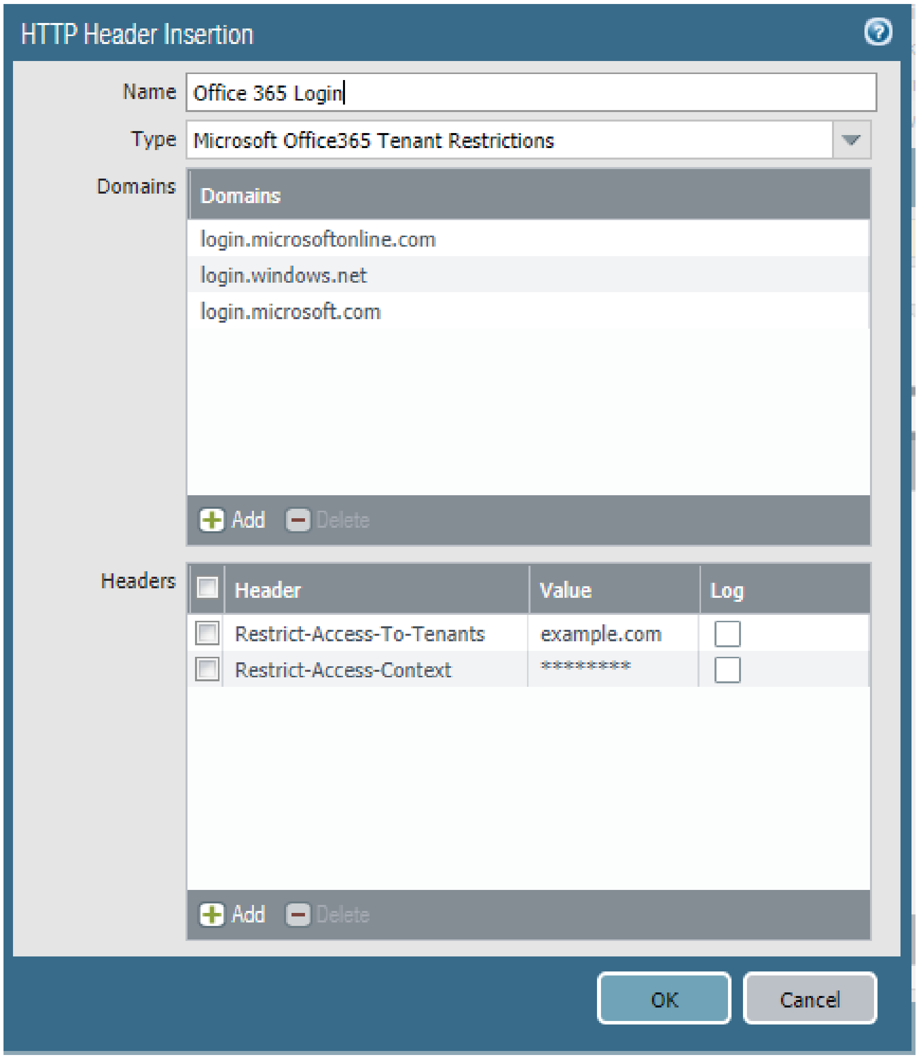
Step 2: Click the **HTTP Header Insertion** tab, and then click **Add**.

Step 3: In the **Name** box, enter **Example Domain**.

Step 4: In the **Type** list, choose **Microsoft Office365 Tenant Restrictions**.

Step 5: To the right of **Headers**, click **Restrict-Access-To-Tenants**.

Step 6: In the **Value** box, enter **example.com**, and then click **OK**.



HTTP Header Insertion

Name: Office 365 Login

Type: Microsoft Office365 Tenant Restrictions

Domains

Domains
login.microsoftonline.com
login.windows.net
login.microsoft.com

Headers

□	Header	Value	Log
□	Restrict-Access-To-Tenants	example.com	□
□	Restrict-Access-Context	*********	□

Step 7: To the right of **Headers**, click **Restrict-Access-To-Tenants**.

Step 8: In the **Value** box, enter your directory ID, and then click **OK**.

Note

You can find your directory ID in the Azure portal. Sign in as an administrator, select Azure Active Directory, then select Properties.

Next, modify the security policy to include the URL filter for HTTP header insertion per the following table.

Table 5 Office 365 security policy with HTTP header insertion

Name	Application (App-ID)	Service	Action	Policy
Product Activation	ms-product-activation	application-default	Allow	Outbound
Office 365 Enterprise	office365-enterprise-access	application-default	Allow	Outbound
Office 365 Base	ms-office365-base ocsp soap	application-default	Allow	Outbound
OneDrive and Office Online	ms-onedrive-base sharepoint-online sharepoint-online-downloading sharepoint-online-editing sharepoint-online-sharing sharepoint-online-uploading	application-default	Allow	Outbound
Outlook	outlook-web-online mapi-over-http ms-exchange rpc-over-http activesync	application-default	Allow	Outbound
Skype for Business	ms-lync-base ms-lync-online rtcp rtp-base stun	application-default	Allow	Outbound
Teams	ms-teams ms-teams-downloading ms-teams-editing ms-teams-posting ms-teams-sharing ms-teams-uploading	application-default	Allow	Outbound
SSL and Web	ssl web-browsing	service-http service-https	Allow	Outbound

2.3 Block Uploads to OneDrive

Optional

Use a file blocking security profile on the next-generation firewall to block uploads into OneDrive.

Step 1: In **Objects > Security Profiles > File Blocking**, click **Add**.

Step 2: In the **Name** box, enter **Block Uploads**, and then click **Add**. A new row is highlighted.

Step 3: In the **Name** column, enter **Uploads**.

Step 4: In the **Direction** list, choose **upload**.

Step 5: In the **Action** list, choose **block**, and then click **OK**.

Step 6: Modify the security policy rules for the **office365-enterprise-access** and **sharepoint-online** App-IDs to include the file-blocking security profile.

Table 6 Office 365 security policy with file blocking

Procedures

Refining Security and Decryption Policies with External Dynamic Lists

MineMeld allows you to further control security rules when using positive security control policies with applications that have explicit dependencies on SSL and web-browsing App-IDs. MineMeld monitors and aggregates IP address and URL information published by application vendors. The aggregate output is available to the next-generation firewall (to download and integrate into security and decryption policies) as an External Dynamic List.

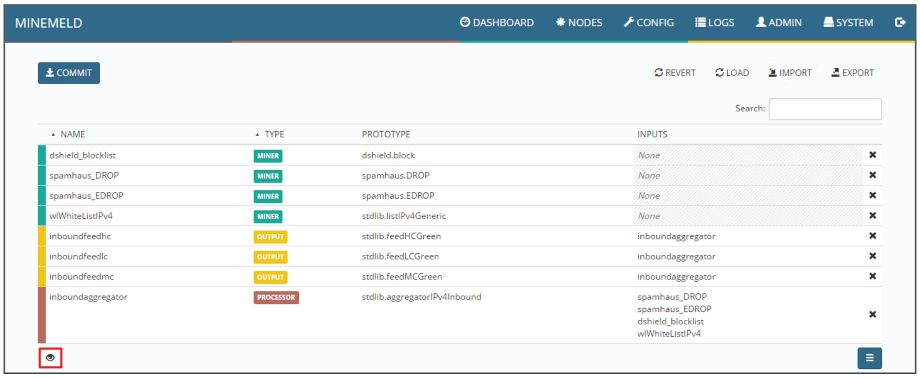
These procedures describe configuring MineMeld and the next-generation firewall for the integration of Microsoft Office 365 URL and IP address ranges.

3.1 Configure MineMeld

This procedure assumes you already have deployed an instance of MineMeld. MineMeld is configured to download and aggregate Microsoft Office 365 URLs and IP address ranges for use by the next-generation firewall.

Step 1: Log in to MineMeld.

Step 2: In Config, enable expert mode.

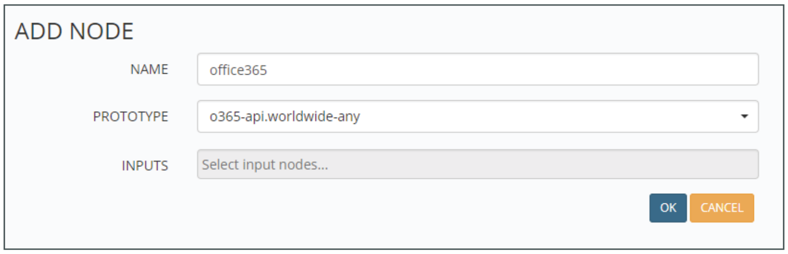


NAME	TYPE	PROTOTYPE	INPUTS	
dshield_blocklist	MINER	dshield.block	*None*	✖
spamhaus_DROP	MINER	spamhaus.DROP	*None*	✖
spamhaus_EDROP	MINER	spamhaus.EDROP	*None*	✖
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	*None*	✖
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	✖
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	✖
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	✖
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4	✖

Step 3: Click **+**.

Step 4: In the **Name** box, enter **office365**.

Step 5: In the **Prototype** list, choose **O365-api.worldwide-any**, and then click **OK**.



ADD NODE

NAME	office365
PROTOTYPE	o365-api.worldwide-any
INPUTS	Select input nodes...

Next add the IPv4 aggregator.

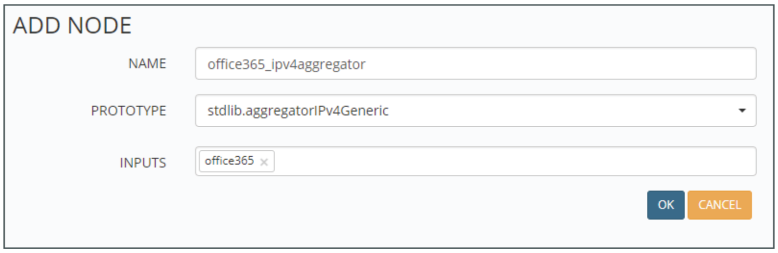
Step 6: In **Config**, click the eye icon on the bottom left of the page.

Step 7: Click **+.**

Step 8: In the **Name** box, enter **office365_ipv4aggregator**.

Step 9: In the **Prototype** list, choose **stdlib.aggregatorIPv4Generic**.

Step 10: In the **Input** list choose **office365**, and then click **OK**.



ADD NODE

NAME	office365_ipv4aggregator
PROTOTYPE	stdlib.aggregatorIPv4Generic
INPUTS	office365 ×

Next, add the IPv6 aggregator.

Step 11: In **Config**, click the eye icon on the bottom left of the page.

Step 12: Click **+**.

Step 13: In the **Name** box, enter **office365_ipv6aggregator**.

Step 14: In the **Prototype** list, choose **stdlib.aggregatorIPv6Simple**.

Step 15: In the **Input** list choose **office365**, and then click **OK**.

Next, add the URL aggregator.

Step 16: In **Config**, click the eye icon on the bottom left of the page.

Step 17: Click **+**.

Step 18: In the **Name** box, enter **office365_URLaggregator**.

Step 19: In the **Prototype** list, choose **stdlib.aggregatorURL**.

Step 20: In the **Input** list choose **office365**, and then click **OK**.

Next, configure the IPv4 feed output.

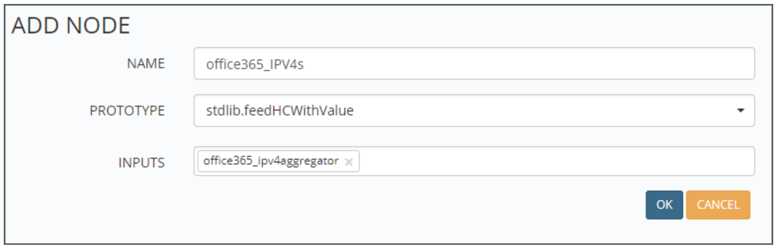
Step 21: In **Config**, click the eye icon on the bottom left of the page.

Step 22: Click **+**.

Step 23: In the **Name** box, enter **office365_IPv4s**.

Step 24: In the **Prototype** list, choose **stdlib.feedHCWithValue**.

Step 25: In the **Input** list choose **office365_ipv4aggregator**, and then click **OK**.



ADD NODE

NAME office365_IPV4s

PROTOTYPE stdlib.feedHCWithValue

INPUTS office365_ipv4aggregator ×

Next, configure the IPv6 feed output.

Step 26: In **Config**, click the eye icon on the bottom left of the page.

Step 27: Click **+.**

Step 28: In the **Name** box, enter **office365_IPv6s**.

Step 29: In the **Prototype** list, choose **stdlib.feedHCWithValue**.

Step 30: In the **Input** list choose **office365_ipv6aggregator**, and then click **OK**.

Next, configure the URL feed output.

Step 31: In **Config**, click the eye icon on the bottom left of the page.

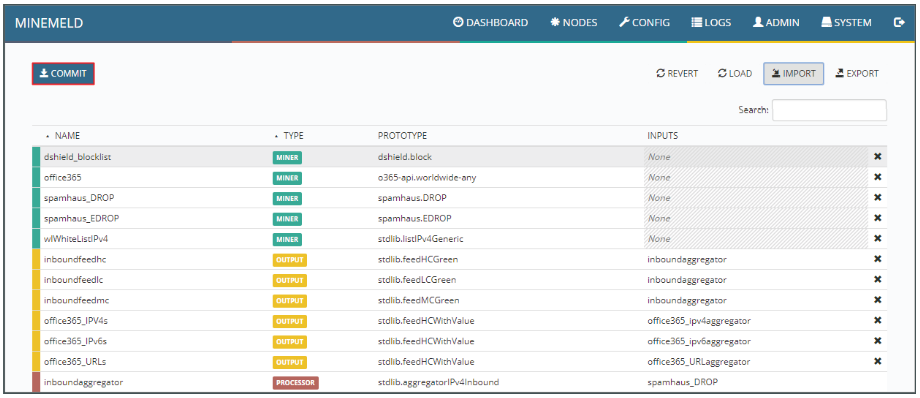
Step 32: Click **+.**

Step 33: In the **Name** box, enter **office365_URLs**.

Step 34: In the **Prototype** list, choose **stdlib.feedHCWithValue**.

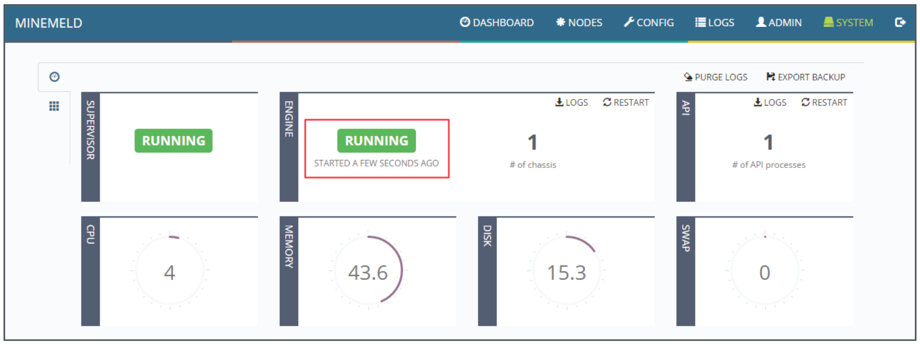
Step 35: In the **Input** list choose **office365_URLaggregator**, and then click **OK**.

Step 36: Click **Commit** and wait for the system to restart.

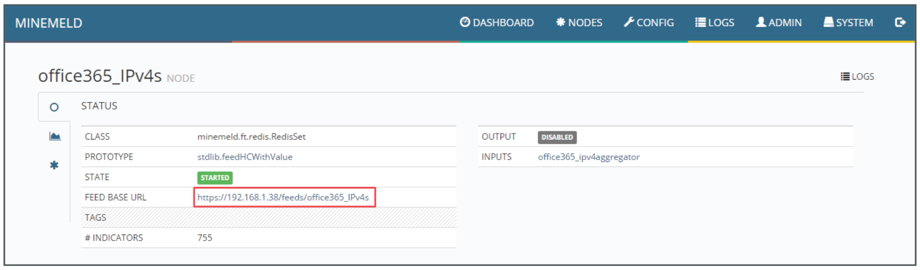


NAME	TYPE	PROTOTYPE	INPUTS	
dshield_blocklist	MINER	dshield.block	*None*	✖
office365	MINER	o365-api.worldwide-any	*None*	✖
spamhaus_DROP	MINER	spamhaus.DROP	*None*	✖
spamhaus_EDROP	MINER	spamhaus.EDROP	*None*	✖
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	*None*	✖
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	✖
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	✖
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	✖
office365_IPV4s	OUTPUT	stdlib.feedHCWithValue	office365_ipv4aggregator	✖
office365_IPv6s	OUTPUT	stdlib.feedHCWithValue	office365_ipv6aggregator	✖
office365_URLs	OUTPUT	stdlib.feedHCWithValue	office365_URLaggregator	✖
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP	

Step 37: Verify the system has restarted. In System, Engine shows as running.



Step 38: In **Nodes > office365_IPv4s**, note the FEED BASE URL, which you will need in the next procedure.



office365_IPv4s NODE

STATUS

CLASS	minemeld.ft.redis.RedisSet
PROTOTYPE	stdlib.feedHCWithValue
STATE	STARTED
FEED BASE URL	https://192.168.1.38/feeds/office365_IPv4s
TAGS	
# INDICATORS	755

OUTPUT	DISABLED
INPUTS	office365_ipv4aggregator

Step 39: Repeat the previous step for the **office365_IPv6s** and **office365_URLs** nodes.

3.2 Define IP Feeds in the Firewall

Step 1: In **Objects > External Dynamic Lists**, click **Add**.

Step 2: In the Name box, enter **Office365 - IPv4 Feed**.

Step 3: In the **Type** list, choose **IP List**.

Step 4: In the **Source** box, enter the value you noted in Procedure 3.1, Step 38.

Step 5: In the **Repeat** list, choose **Five Minute**, and then click **OK**.

Step 6: Repeat this procedure with the IPv6 feed.

3.3 Define the URL Feeds

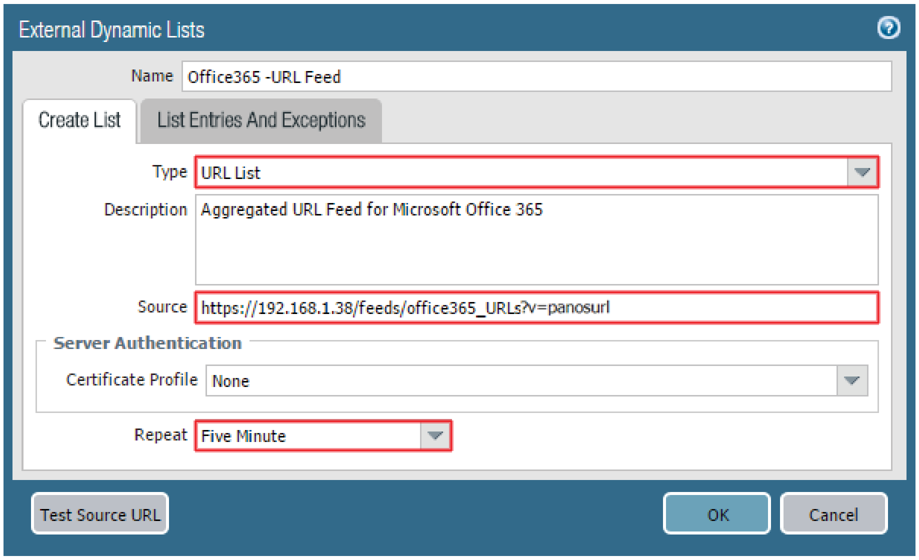
Step 1: In **Objects > External Dynamic Lists**, click **Add**.

Step 2: In the **Name** box, enter **Office365 - URL Feed**.

Step 3: In the **Type** list, choose **URL List**.

Step 4: In the **Source** box, enter the value you noted in Procedure 3.1, Step 38 and append **?v=panosurl** to the end of the URL.

Step 5: In the **Repeat** list, choose **Five Minute**, and then click **OK.**



External Dynamic Lists

Name: Office365 -URL Feed

Type: URL List

Description: Aggregated URL Feed for Microsoft Office 365

Source: https://192.168.1.38/feeds/office365_URLs?v=panosurl

Server Authentication

Certificate Profile: None

Repeat: Five Minute

3.4 Add EDLs to the Security Policy Rules

Modify the security policy to include destination IP addresses and URL domains contained in the external dynamic lists. A catch-all rule is required because Office 365 uses content delivery networks (CDNs) for some of its services, and CDN IP address information is not included in the IPv4 or IPv6 EDLs. Also, Skype for Business communicates dynamically with many devices outside the Office 365 servers and should not be limited to the IPv4 or IPv6 EDLs.

Figure 2 Sanctioning Office 365: example security policy rules

Name	Dst Address	Application (App-ID)	Service	URL Category	Action	Policy
Product Activation	any	ms-product-activation	application-default	any	Allow	Outbound
Office 365 Enterprise	Office365 -IPv4 Feed Office365 -IPv6 Feed	office365-enterprise-access	application-default	Office365 - URL Feed	Allow	Outbound
Office 365 Base	Office365 -IPv4 Feed Office365 -IPv6 Feed	ms-office365-base	application-default	Office365 - URL Feed	Allow	Outbound
OneDrive and Office Online	Office365 -IPv4 Feed Office365 -IPv6 Feed	ms-onedrive-base sharepoint-online	application-default	Office365 - URL Feed	Allow	Outbound
Outlook	Office365 -IPv4 Feed Office365 -IPv6 Feed	outlook-web-online mapi-over-http ms-exchange rpc-over-http activesync	application-default	Office365 - URL Feed	Allow	Outbound
Outlook Online URLs	any	outlook-web-online	application-default	Office365 - URL Feed	Allow	Outbound
Skype for Business	any	ms-lync-base ms-lync-online rtcp rtp-base stun	application-default	Office365 - URL Feed	Allow	Outbound
Office 365 Catch All	any	ms-office365-base ms-onedrive-base ocsp sharepoint-online soap ssl web-browsing	service-http service-https	Office365 - URL Feed	Allow	Outbound

3.5 Add EDLs to the Decryption Policy Rules

Optional

You can optionally add a decryption policy rule that uses Office 365 external dynamic lists to selectively decrypt Office 365 traffic. This example procedure assumes you already have generated and deployed the certificates required to do SSL decryption to the firewall and endpoints.

Step 1: In **Policies > Decryption**, click **Add**. The decryption policy rule window appears.

Step 2: On the **General** tab, in the **Name** box, enter **O365**.

Step 3: On the **Source** tab, in the **Source Zone** pane, click **Add**.

Step 4: In the **Source Zone** list, choose **Private**.

Step 5: On the **Destination** tab, in the **Destination Zone** pane, click **Add**.

Step 6: In the **Destination Zone** list, choose **Internet**.

Step 7: On the **Service/URL Category** tab, in the **URL Category** pane, click **Add**.

Step 8: In the **URL Category** list, choose **Office365-URL Feed**.

Step 9: On the **Options** tab, for **Action** select **Decrypt**.

Step 10: In the **Type** list, choose **SSL Forward Proxy**.

Step 11: In the **Decryption Profile** list, select **default**, and then click **OK**.

Step 12: Click **Commit**.

3.6 Verify EDLs

Step 1: If you are using an on-premises next-generation firewall, log in to the firewall's CLI.

Step 2: Show the feed.

```
request system external-list show type ip name "Office 365 -IPv4 Feed"
```

Note

EDLs must be used in a security policy rule before they are retained by the firewall. If the EDL is not used in a security policy rule, the firewall returns "Server error: external dynamic list file either empty or not found."

Step 3: Validate the output.

```
vsys1/Office365 -IPv4 Feed:
        Next update at         : Fri July 28 10:51:51 2018
        Source                 : https://192.168.1.38/feeds/office365_IPv4s
        Referenced             : Yes
        Valid                  : Yes
        Auth-Valid             : Yes

        Total valid entries    : 755
        Total invalid entries  : 0
        Valid ips:
                104.209.35.177-104.209.35.177
                104.211.160.244-104.211.160.244
                104.214.144.252-104.214.144.252
```

You can use the feedback form to send comments about this guide.

HEADQUARTERS

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA
http://www.paloaltonetworks.com

Phone: +1 (408) 753-4000
Sales: +1 (866) 320-4788
Fax: +1 (408) 753-4001
info@paloaltonetworks.com

B-000208P-1 08/19