Zero-Day Protection

Best Practices and Recommendations

Reviewing your Zscaler security settings is a key step to limiting your exposure to dangerous polymorphic and zero-day threats.

Follow the best practices in this document to strengthen your security:

Control What Files Users Access

For better protection, Implement FileType Control which can block dangerous file types from reaching your users.

Add Cloud Sandboxing

For protection from polymorphic threats, Zscaler Cloud Sandbox delivers a needed layer of protection, and easily scales across all users in all locations.

Inspect ALL traffic Including SSL

Adjust your Zscaler policy to inspect SSL. Over 50% of malware is now hiding in SSL traffic

Implement File Quarantine:

A key advantage of Cloud Sandboxing, this features holds onto inbound files until they are approved clean by Zscaler Cloud Sandbox.

Up-level your Policy Strategy:

A review of your security policies helps define what security gaps you still may have left and what changes will make you safer.

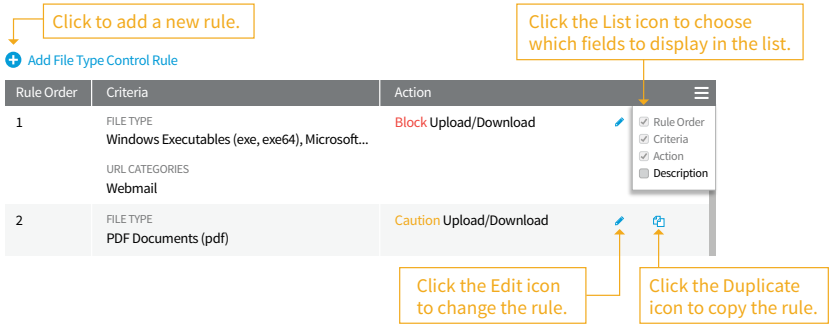
The Zscaler™ Cloud Security Platform provides a completely integrated solution that protects from a broad range of malware. However, with the alarming rise of advanced threats, it is always good for customers to review their Zscaler configuration. By adjusting your file access policy, enabling needed technologies like Cloud Sandboxing, and inspecting SSL, customers can strengthen their user security and minimize the risk of breaches.

Step 1: Control the Files your Users Are Accessing

The first step to strengthening your security is to re-evaluate which files you are allowing to reach your users. Since Zscaler can extend security across all your users regardless of location, using Zscaler File Type Control allows you to protect all your users from dangerous files.

Implementing FileType Control

By default, FileType Control allows the upload and download of all file types. Use the File Type Control policy to restrict the upload and download of various types of files. For example, you can block audio (such as mp3 and wav files) and video files (such as .avi, .mp4, .mpeg and others) so they do not interfere with your bandwidth utilization. You can define rules to restrict the transmission of various files and apply them to individuals, groups, departments and locations. File Type Control



is associated with URL filtering and is not available for cloud apps. For example, to block file attachments in Gmail, select the Webmail URL category. You can also create rules for unknown file types. Zscaler performs MIME type checks for files it cannot initially identify, and any file that falls outside of well-defined MIME types for common apps is tagged as an unknown file type. To recognize the file types inside archive files, the Zscaler service also scans ZIP, 7-Zip, GZIP, TAR, and RAR files.

You can allow, caution or block uploading, downloading or both. When you choose the Caution action, the service displays a warning before it allows the user to perform the action. When the service blocks users, it displays a notification. The content of the block notification is configured in the End User Notification page.

To review how turn on File Type Control and the recommended policy for File Type Control, visit our support article **https://support.zscaler.com/hc/en-us/articles/205038075**

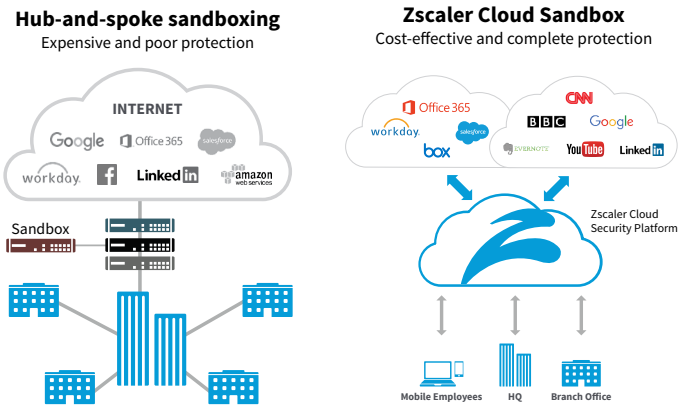
Step 2: Add Cloud Sandboxing to your Security

It's pretty well understood that traditional signature-based security approaches are falling behind in the task of protecting today's organizations. The critical weakness is that in order to stop a threat with a signature, you need to have prior knowledge of the threat. With the increase of zero-day ransomware and polymorphic malware, organizations need to move beyond signature-based detection and add sandboxing as an additional layer of defense. Sandboxing uses dynamic analysis to monitor file behavior in an isolated environment to protect users from zero-day threats.

How Zscaler Cloud Sandbox works

With Zscaler, you can sandbox any suspicious or unknown file without backhauling traffic to the data center. Since Zscaler Cloud Sandbox is implemented from the cloud, it protects all of your users, regardless of their locations. This means that remote office workers and mobile users get the same level of protection as the users at your headquarters, without costly MPLS links or cumbersome VPN connections.

Zscaler Cloud Sandbox is architected to provide inline protection to block threats before they enter your network. Malicious files are instantly blocked, quarantined, or flagged based on your defined policies. Unlike appliances, which work in isolation, Zscaler Cloud Sandbox is fully integrated into the Zscaler Cloud Security Platform to deliver maximum threat visibility and multilevel protection. Because Zscaler is delivered as a service, there is no hardware deploy and manage, and no software to update.



Adding Sandboxing to your Installation

While the default Zscaler platform does provide some cloud sandboxing functions, there are some differences from the complete Cloud Sandbox offering. Only executables (.exe) and library files (.dll) are scanned, and there is a file size limitation to 2mb. Additionally, the default offering is unable to hold files from being delivered until scanned (quarantine).

Zscaler's complete Cloud Sandbox solution allows scanning of multiple file types, scales to much larger file sizes, allows complete policy configuration, can deliver inline holding of files (quarantine) in addition to a host of other sandbox security features. With the ability to easily scale protection across your entire user base, regardless of location, Zscaler Cloud Sandbox is an important security layer for complete threat protection from polymorphic and zero-day threats.

Step 3: Inspect ALL your traffic including SSL

Although SSL is a very effective protocol for securing the communication of legitimate traffic, it is important to note that malware is often delivered over SSL in order to avoid inspection. Zscaler's research team is now seeing over 50% of active malware hiding in SSL traffic. Hackers commonly try to hide in encrypted traffic, as visibility into SSL is often difficult and resource intensive.

Because Zscaler was built to handle encrypted traffic at a global cloud scale, the issue of SSL inspection becomes a non-issue. Zscaler inspects every byte of traffic in real time, including encrypted traffic, so hackers and their malware can be easily identified. In addition to stopping hackers, SSL inspection is also useful when an enterprise wants to know what its employees are intentionally or accidentally sending out of the organization. For example, individuals who are using SSL-encrypted Yahoo mail may be exposing company passwords, personal information, or financial data. SSL inspection is also needed for compliance, to ensure that employees are not putting the organization's confidential data at risk.

The best approach for turning on SSL inspection

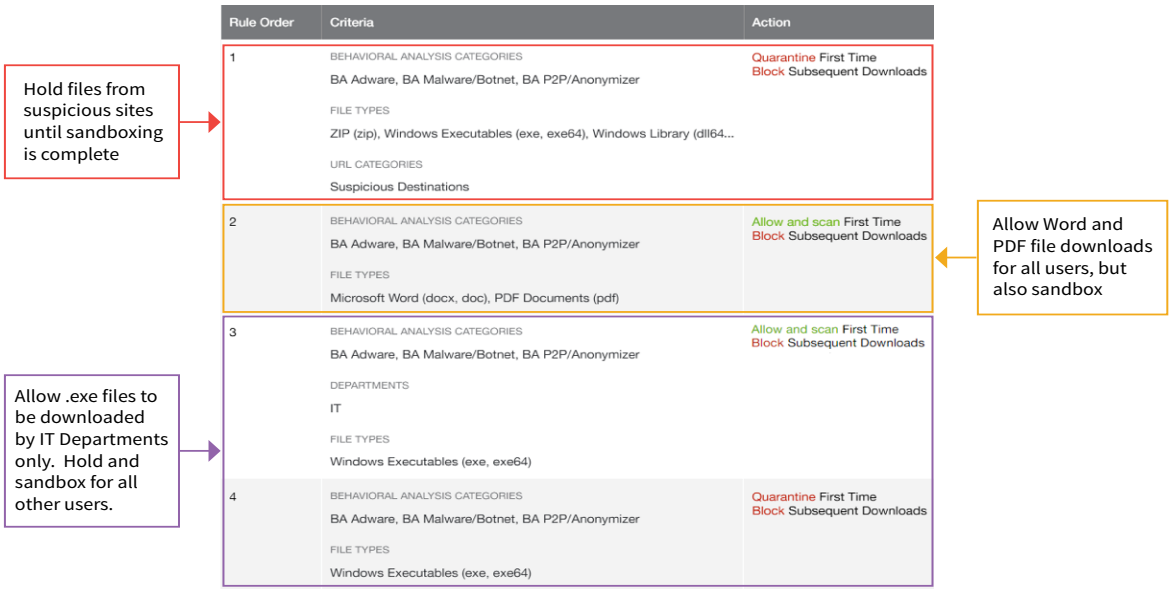
Before deploying SSL inspection for your organization, consider the following best practices:

- Enable SSL inspection on a small location or test lab before enabling it on all locations in your organization to understand how this feature works.
- If you are using the Zscaler intermediate certificate, ensure that the Zscaler root certificate is distributed to all users and that it is installed in their browsers before enabling SSL in a location.
- You may also update your end user notification to inform users of your organization's SSL interception policy.
- When you define SSL inspection policy, you can create a list of URLs/URL categories and cloud apps/cloud app categories for which SSL transactions will not be decrypted. Configure this list carefully because it is applied globally throughout an organization and takes precedence over per-location SSL scanning.
- Start by enabling SSL inspection for "risky" URL categories only, such as Security Risk and Legal Liability categories such as Adult Content, Gambling, and Unknown/Miscellaneous. Include all other categories in the list of URL categories for which SSL transactions will not be decrypted. Then, when your organization is ready, enable SSL inspection for all URL categories except Banking and Healthcare, to allay privacy concerns within the organization.
- The list of URL categories and cloud apps for which SSL transactions will not be decrypted does not apply to road warriors who configure their browsers or PAC files to send traffic to port 9443. To use this feature, your organization must subscribe to a dedicated proxy port.
- Firefox browsers do not accept SSL certificates installed in Internet Explorer browsers. You must install SSL certificates on Firefox browsers separately if your organization allows Firefox browsers. Google Chrome, however, uses the same certificate store as Internet Explorer.
- Certain client applications, like Dropbox, use a technique called Certificate Pinning, where the client application is hard coded to accept only one specific client certificate. Apps that use certificate pinning might not work with SSL inspection. They should be included in the list of URL categories for which SSL transactions will not be decrypted.
- Enable user authentication as well, to allow the service to apply user policies.

To enable your installation to start inspecting SSL, Zscaler recommends you review the **implementation guide to deploying SSL inspection**

Step 4: Implement File Quarantine

A key feature of Zscaler Cloud Sandbox, File Quarantine allows you to prevent a file from delivery to a user until it has been sandboxed. Many traditional sandboxes often end up installed out-of-line, so malicious files are delivered and only after the fact are you notified that the file was malicious. Since Zscaler Cloud Sandbox is delivered from the cloud and architected into the Zscaler Platform, File Quarantine becomes a tremendous security advantage. With complete control over how quarantining is implemented, Zscaler Cloud Sandbox allows organizations to define a policy that best fits their needs. You can define quarantining by user groups, url destinations and file types.



Implementing File Quarantine

File Quarantine is implemented via the Cloud Sandbox Policy. Before you enable File Quarantine you must evaluate the best policy approach based upon your tolerance for malicious files.

Low Tolerance for Malicious Files: If your organization has low tolerance for downloading malware, you can choose "Quarantine" for First Time Action on a majority of URL Categories. Organizations that may choose this option include:

- Customers looking to strengthen their zero-day security posture
- Financial institutions or organizations with high-value transactions and or access to sensitive data.

Low Tolerance for Download Delays: If your organization has lower tolerance for download delays and end-user interruptions from quarantining files, you can choose "Allow & Scan" for First Time Action based on specific URL Categories or defined User Groups. Organizations that may choose this option include:

- Organizations with engineering or research labs that regularly download Windows executables or other files "suspicious" in nature, despite not having malicious intent.

To read more about File Quarantine feature and how to configure Zscaler's Cloud Sandbox policy, see the support article: **https://support.zscaler.com/hc/en-us/articles/209673846-How-do-I-add-rules-to-the-Sandbox-policy-**

Step 5: Review and Up-level your Policy Strategy

A thorough review of your policy configuration is the last step in closing your security gaps. Since the Zscaler Platform is a completely integrated security solution, there are several key security policies that protect your users and traffic. Evaluating your current policy settings against Zscaler's recommendations and your internal security requirements can help strengthen your security posture against advanced threats.

The following support articles can help you walk through the key policies to review within your Zscaler Installation:

Malware Protection Policy

Dedicated detection engine for Antivirus, Anti-Spyware that leverages signature based detection and malware threat feeds. Review recommended settings for this policy here:
https://support.zscaler.com/hc/en-us/articles/205031885

Advanced Malware Threats Policy

Protect from Botnets, Command and Control, Malicious Sites, Browser Exploits, Phishing and Fraud, and Cross Site Scripting. Integrated into the Zscaler Platform, the solution calculates a risk score based upon user browsing content and patterns. Review the recommended setting for this policy here:
https://support.zscaler.com/hc/en-us/articles/204971595#Configuring-Advanced-Threats-Protection

Cloud Application Control Policy

Provides granular control over popular web sites and applications. They are organized by function into categories for easy reference. Review recommended settings for this policy here:
https://support.zscaler.com/hc/en-us/articles/205036485-About-the-Cloud-App-Control-Policy

Browser Control Policy

Enforces user browser version control to minimize older browser vulnerabilities. Review recommended setting for this policy here:
https://support.zscaler.com/hc/en-us/articles/204345869-What-is-the-recommended-Browser-Control-policy-

Firewall Policy

The Zscaler provides an integrated cloud-based next-generation firewall capability that allows granular control over your organization's outbound TCP, UDP and ICMP traffic. This includes Firewall and DNS dashboards, giving your organization visibility into applications running in your networks. Review recommended settings for this policy here:
https://support.zscaler.com/hc/en-us/articles/204364389-About-Firewall-Policies

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com