(https://help.zscaler.com)

How does the Zscaler service enforce policies?

Search

The Zscaler service uses full-featured inline proxies called Zscaler Enforcement Nodes (ZENs) to inspect and enforce policies on traffic leaving your organization and coming into your organization. Each ZEN has two main modules for inspecting traffic and applying policies: a web module and a firewall module.

Below is a high-level view of how traffic flows through the ZEN and its modules.

- When the ZEN receives outbound web traffic from your organization to the Internet:
  - It sends the traffic to its web module for policy evaluation. If the traffic violates a web policy, it blocks the transaction.
  - If the traffic does not violate any web policies, it sends the traffic to the firewall module for policy evaluation.
  - If the traffic violates a firewall policy, it blocks the transaction. If the traffic does not violate any firewall policies, it allows the traffic to the Internet.
- When the ZEN receives outbound non-web traffic going to ports other than 80/443:
  - It sends the traffic directly to the firewall module for policy evaluation.
  - If the traffic violates a firewall policy, it blocks the transaction. If the traffic does not violate any firewall policies, it allows the traffic to the Internet.
- When the ZEN receives inbound web traffic (HTTP/HTTPS traffic for ports 80/443) from the Internet in response to HTTP GET/POST requests.

- It sends the traffic to its web module for policy evaluation.
- If the traffic violates a web policy, the traffic is blocked. If the traffic does not violate any web policies, it allows the traffic into your organization.

See more about how within the Web Module, the policies that are enforced change depending on the type of web traffic received, and whether SSL inspection is enabled

When the ZEN receives web traffic (HTTP/HTTPS traffic on port 80/443), the web module first inspects the traffic and applies your organization's web policies. The policies that are applied depend upon the type of web traffic received, and if the traffic is encrypted, whether you have SSL inspection enabled.

HTTP Traffic

The policies enforced depend on whether the transaction is an HTTP GET request, HTTP POST request, or an HTTP GET/POST response. To learn more about the order of policy enforcement for each traffic type, see the sections and image below. In each case, when the Web Module determines that a transaction violates a specific policy, the ZEN immediately blocks that transaction and does not continue enforcing the policies that follow. The ZEN also does not send the traffic to the firewall module for policy evaluation. However, your firewall logs will show that the user's web transaction has been blocked.

HTTP GET Request

This is a user request to retrieve a resource from the web (for example, a web page). The ZEN scans the GET request and applies policies in the following order:

1. **Security Exceptions (if configured)**: The ZEN first checks if the requested URL is included in your organization's list of whitelisted URLs (https://help.zscaler.com/zia/how-do-i-whitelist-urls), configured in the Security Exceptions tab of the Malware Protection (https://help.zscaler.com/zia/about-malware-protection)
 or
Advanced Threat Protection (https://help.zscaler.com/zia/about-advanced-threat-protection)
 policies. If the URL is included under Security Exceptions, the Z kips

over the security-related policies below (Known Malicious URLs, Country-Based Blocking, and Signature-Based Detection).

2. **Known Malicious URLs (Advanced Threat Protection)**: The ZEN checks if the requested URL is known to have malicious content using an extensive URL database that is updated daily with feeds from various partners. This check falls under the Advanced Threat Protection policies.

   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.

3. **Cloud App Control**: The ZEN checks if the requested application violates the
   Cloud App Control (https://help.zscaler.com/zia/about-cloud-app-control)
   policy configured by your organization.

   By default, if a user requests a cloud app that you explicitly allow with Cloud App Control policy, the service only applies the Cloud App Control policy and does not apply the URL Filtering policy. The service proceeds straight to evaluating Browser Control. For example, if you have a Cloud App Control rule that allows viewing Facebook, but a URL Filtering policy that blocks www.facebook.com, a user will still be allowed to view Facebook because by default, the service does not apply the URL Filtering policy if a Cloud App Control rule allows the transaction.

   This behavior changes, however, if you allow cascading to URL filtering in
   Advanced Settings (https://help.zscaler.com/zia/about-advanced-settings)
   . If you do, the service applies the URL Filtering policy even if it applies a Cloud App Control policy allowing the transaction. Therefore in the example above, with cascading enabled, the service will apply the URL Filtering policy and block the user from Facebook.

   If a user requests a cloud app for which you have not configure[illegible]loud App Control policy rule - for example, the user requests eBay.com, and

you don't have a Cloud App Control rule for eBay.com - the service still evaluates and applies the URL filtering policy.

4. **URL Filtering**: The ZEN checks if the requested URL belongs to URL categories or custom URL categories blocked by your organization's URL Filtering (https://help.zscaler.com/zia/about-url-filtering) policy.

   If the user's requested URL is for a cloud app that is explicitly allowed by a Cloud App Control rule, the service skips this policy and moves to the next one. The only exception is if your organization has enabled **Cascading to URL Filtering** in Advanced Settings (https://help.zscaler.com/zia/about-advanced-settings). If so, the service still applies URL Filtering policy even if a Cloud App Control policy rule has already explicitly allowed the app.
5. **Browser Control**: The ZEN checks if the user's browser, or the plug-ins or applications within your user's browser, violates your organization's Browser Control (https://help.zscaler.com/zia/about-browser-control) policy.
6. **Country-Based Blocking (Advanced Threat Protection)**: The ZEN checks if the request is being sent to a server in a country you've blocked as a suspicious destination under your Advanced Threat Protection policy.

   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.
7. **Signature-Based Detection for URLs (Advanced Threat Protection)**: The ZEN checks the request using signature-based detection and provides protection against botnets, XSS, phishing, malicious active content, and other advanced threats. It also calculates the Suspicious Content Protection (https://help.zscaler.com/zia/about-advanced-threats-protection) (Page Risk™) value and blocks the page if the value exceeds the value you set in the Advanced Threat Protection policy. This entire check falls under the Advanced Threat Protection policy.

If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.

8. **P2P Control (Advanced Threat Protection)**: The ZEN checks if the requested application is a prohibited P2P file sharing, anonymizer, or VoIP application. This check falls under the Advanced Threat Protection policy.
9. **Bandwidth Control**: The ZEN checks how the request must be treated (allowed full or reduced bandwidth) in accordance with your organization's Bandwidth Control (https://help.zscaler.com/zia/about-bandwidth-control) policy and the current bandwidth usage at the user's location.

Close

HTTP POST Request

This is a user request to submit or post data to the web (for example, emails sent through webmail or posts on social networking sites). The ZEN scans the POST request and applies policies in the following order:

1. **Security Exceptions (if configured)**: The ZEN first checks if the requested URL is included in your organization's list of whitelisted URLs, (https://help.zscaler.com/zia/how-do-i-whitelist-urls) configured in the Security Exceptions tab of the Malware Protection (https://help.zscaler.com/zia/about-malware-protection) or Advanced Threat Protection (https://help.zscaler.com/zia/about-advanced-threat-protection) policies. If the URL is included under Security Exceptions, the ZEN skips over the security-related policies below (Known Malicious URLs, Country-Based Blocking, Signature-Based Detection, and Anti-virus and Anti-Spyware Control).
2. **Known Malicious URLs (Advanced Threat Protection)**: The ZEN checks if the requested URL is known to have malicious content, using an extensive URL database that is updated daily with feeds from various partners. This check falls under the Advanced Threat Protection policies.

If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.

3. **Cloud App Control**: The ZEN checks if the requested application violates the
   Cloud App Control (https://help.zscaler.com/zia/about-cloud-app-control)
   policy configured by your organization.
4. **URL Filtering**: The ZEN checks if the URL belongs to URL categories or custom URL categories blocked by your organization's
   URL Filtering (https://help.zscaler.com/zia/about-url-filtering) policy.
5. **Browser Control**: The ZEN checks if the user's browser, or the plug-ins or applications within your user's browser, violates your organization's
   Browser Control (https://help.zscaler.com/zia/about-browser-control)
   policy.
6. **Country-Based Blocking (Advanced Threat Protection)**: The ZEN checks if the request is being sent to a server in a country you've blocked as a suspicious destination under your Advanced
   Threat Protection policy.

   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.
7. **File Type Control**: The ZEN checks if the post request violates your
   File Type Control (https://help.zscaler.com/zia/about-file-type-control)
   policy.
8. **Signature-Based Detection for URLs (Advanced Threat Protection)**: The ZEN checks the request using signature-based detection and provides protection against botnets, XSS, phishing, malicious active content, and other advanced threats. It also calculates the
   Suspicious Content Protection (https://help.zscaler.com/zia/about-advanced-threats-protection)
   (Page Risk™) value and blocks the page if the value exceeds the value you set in the Advanced Threat Protection policy. This entire check falls under the Advanced Threat Protection policy.

   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.

9. **AV/AS Controls**: The ZEN checks files in the request against anti-virus and anti-spyware signatures. The service has dedicated threads for processing files that are larger than 10 MB to ensure that the evaluation of large files does not cause a bottle-neck and delay the evaluation of smaller files. This check falls under the Malware Protection policy.

   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.
10. **Data Loss Prevention**: The ZEN checks if the post request includes content that violates your organization's DLP policy.
11. **P2P Controls**: The ZEN checks if the requested application is a prohibited P2P file sharing, anonymizer, or VoIP application. This check falls under the Advanced Threat Protection policy.
12. **Bandwidth Control**: The ZEN checks how the request must be treated (allowed full or reduced bandwidth) in accordance with your organization's
    Bandwidth Control (https://help.zscaler.com/zia/about-bandwidth-control)
    policy and the current bandwidth usage at the user's location.

Close

HTTP GET/POST Response

This is data sent from the destination host back to the user in response to an HTTP GET or POST request. The ZEN scans the response and applies policies in the following order:

1. **Security Exceptions (if configured)**: The ZEN first checks if the responding URL is included in your organization's list of whitelisted URLs (https://help.zscaler.com/zia/how-do-i-whitelist-urls), configured in the Security Exceptions tab of the
   Malware Protection (https://help.zscaler.com/zia/about-malware-protection)
   or
   Advanced Threat Protection (https://help.zscaler.com/zia/about-advanced-threat-protection)
   policies. If the URL is included under Security Exceptions, the ZEN skips over the security-related policies below (Signature-Based Detection, Sandbox, and Anti-virus and Anti-Spyware Control).

2. **File Type Control**: The ZEN checks if any files in the response violate your
   File Type Control (https://help.zscaler.com/zia/about-file-type-control) policy.
3. **Signature-Based Detection for URLs (Advanced Threat Protection)**: The ZEN checks the response using signature-based detection and provides protection against botnets, XSS, phishing, malicious active content, and other advanced threats. It also calculates the
   Suspicious Content Protection (https://help.zscaler.com/zia/about-advanced-threats-protection)
   (Page Risk™) value and blocks the page if the value exceeds the value you set in the Advanced Threat Protection policy. This entire check falls under the Advanced Threats Protection policy.

   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.
4. **Sandbox (check for known malicious files)**: The ZEN checks if the response contains any malicious files that have been previously identified the by the Sandbox engine.

   If the responding URL falls under Security Exceptions, the service skips this policy and moves to the next one.
5. **AV/AS Controls**: The ZEN checks the files in the response against anti-virus and anti-spyware signatures. The service has dedicated threads for processing files that are larger than 10 MB to ensure that the evaluation of large files does not cause a bottle-neck and delay the evaluation of smaller files. This check falls under the Malware Protection policy.

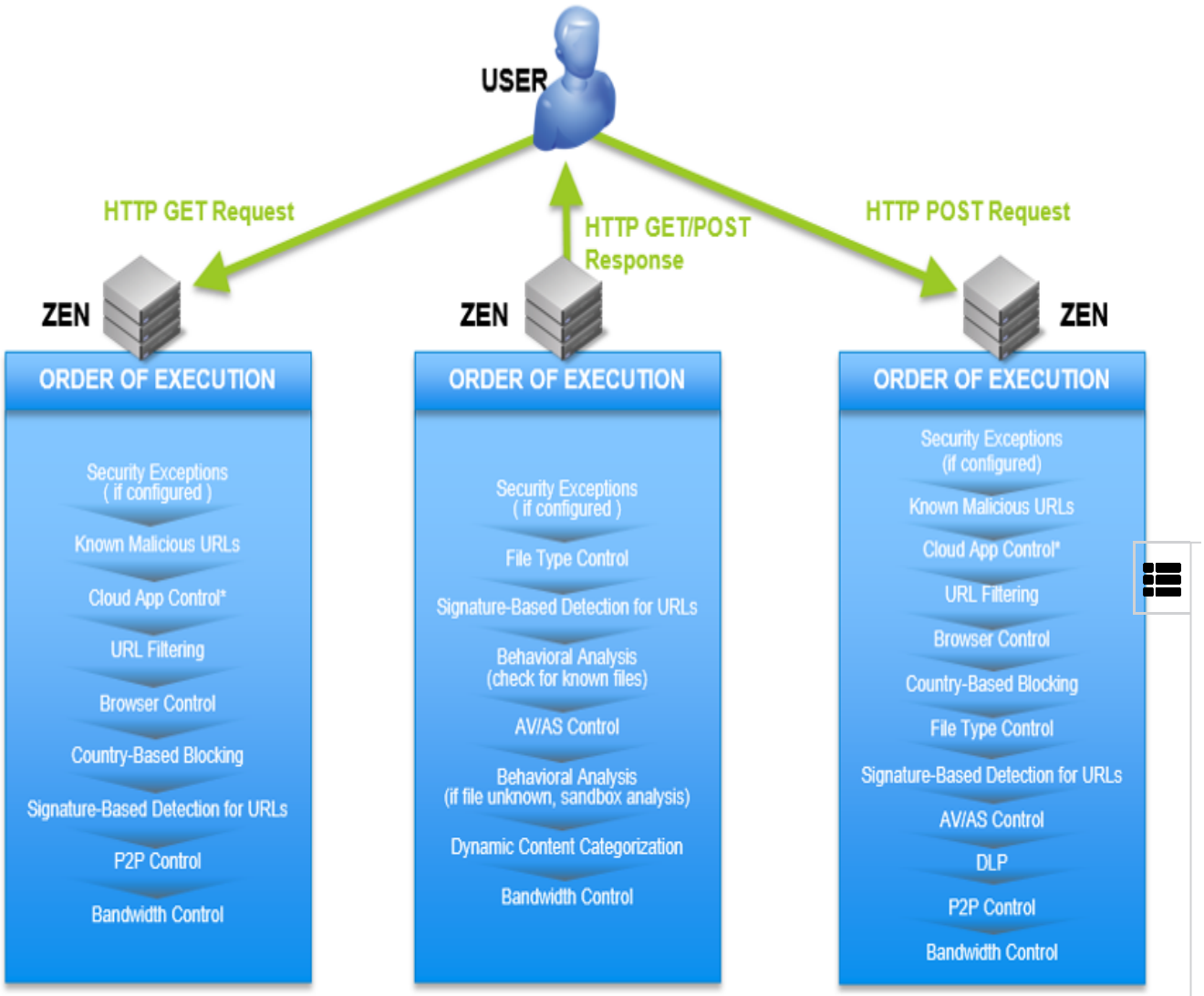
   If the user's requested URL falls under Security Exceptions, the service skips this policy and moves to the next one.
6. **Sandbox (sandboxing vs behavioral analysis)**: If a file in the response has not been previously identified as a malicious file by the Sandbox engine, the service conducts analysis of the file to detect any malicious behavior.

If the responding URL falls under Security Exceptions, the service skips this policy and moves to the next one.

7. **Dynamic Content Categorization**: The ZEN checks the responding URL for any content that could place the website into the Adult Material, Drugs, Gambling, or Violence super-categories. If the ZEN determines that the website belongs in one of those categories, it checks your URL filtering policy to see if the response must be allowed or blocked. If the responding URL does not belong to any of those four super-categories, the ZEN categorizes the page as belonging to the Miscellaneous super-category and allows or blocks based on your policy.
   Dynamic Content Categorization (https://help.zscaler.com/zia/how-do-i-configure-advanced-url-policy-settings)
   must be enabled in Advanced URL Policy Settings.
8. **Bandwidth Control**: The ZEN checks how the request must be treated (allowed full or reduced bandwidth) based on your organization's Bandwidth Control (https://help.zscaler.com/zia/about-bandwidth-control)
   policy and the current bandwidth usage at the user's location.

Close

Below is an illustration that summarizes the order of policy enforcement for different traffic types.



*By default, if a user requests a cloud app that you explicitly allow with Cloud App Control policy, the service only applies the Cloud App Control policy and does not apply the URL Filtering policy. The service proceeds straight to evaluating Browser Control.

HTTPS Traffic

When the ZEN receives HTTPS traffic, the policies that are enforced depend on whether SSL inspection is enabled.

- If SSL inspection is enabled, and the requested or responding URL does not fall under the
  Do Not Inspect list (https://help.zscaler.com/zia/how-do-i-skip-inspection-traffic-specific-urls-or-cloud-apps)
  , the ZEN performs SSL inspection, then sends the traffic to the web module, where it enforces policies in exactly the same way as HTTP traffic.
- If SSL inspection is disabled, or if the requested or responding URL falls under the Do Not Inspect list, the ZEN applies a limited set of policie

HTTPS GET/POST requests, as long as your organization meets certain deployment criteria. See deployment details.
If the traffic is an HTTPS GET/POST response, the ZEN neither inspects nor enforces policy on the traffic.

Firewall Module

If the user's HTTP or HTTPS transaction is not blocked by the web module, the ZEN then sends the traffic to the firewall module for policy enforcement. However, the following must also be true:

- The traffic is outbound, going from the user to the web.
- The organization has enabled firewall policy for the location.

As long as the above conditions are met, the firewall module enforce policies on the web traffic. If your organization's web policy allows a transaction but has a conflicting firewall policy that blocks it, the service will apply the firewall policy. For example, if the web Cloud App Control policy allows the application Box.com, but the firewall policy blocks it, the service will block the transaction.

Close

See more about how the ZEN treats non-web traffic going to ports other than 80/443
If the ZEN receives outbound, non-web traffic going to ports other than 80/443, and the organization has firewall policy enabled on the user's location, the ZEN inspects the traffic and applies policy using only the firewall module. If the organization has not enabled firewall policy for the location, the ZEN will neither scan nor apply any policy to the traffic.

Close

See examples that highlight the value of considering the order of policy enforcement when configuring your policies
Knowing how the service applies your policies in different scenarios helps ensure that your organization's traffic is secured as expected, and that you understand why certain policies do or do not trigger on your users' traffic. Consider the examples below.

Example 1

Consider an organization that:

- Under the web policy, allows the cloud application Box.net
- Under the firewall policy, blocks the same application

When a user from the organization opens a browser and requests the application Box.net, the user will be blocked because even if the web module, which first performs inspection, allows the traffic, the firewall module still inspects and enforces firewall policy on the traffic.

Example 2

Consider another example that applies to policy enforcement within just the web module. The web module has a specific order in which it applies policies for different types of web traffic. As it inspects the traffic, once the service finds a policy violation, it immediately blocks the transaction and does not apply any of the following web policies. For instance, with HTTP POST requests, the service applies the File Type Control policy before the DLP policy. Now, consider an organization that:

- Under the File Type Control policy, blocks PDFs from being sent out of its corporate network
- Under the DLP policy, blocks documents containing social security numbers, and specifies that the Zscaler service send notifications to auditors when it detects users attempting to do so

In this case, if a user in the organization attempts to send a PDF that contains credit card numbers, the service will block the transaction, but it will do so because of the File Type Control policy, rather than the DLP policy. The DLP policy itself will never trigger, and the service will not send a notification alerting the auditor that a user has attempted to send social security numbers out of the organization.

Close