Best Practices for Integrating Zscaler™ Security Analytics & Logging Capabilities into the Security Operations Workflow

zscaler™

Table of contents

Table of contents

Overview

As security threats continue to advance, security operations have become a necessary function for protecting our digital way of life. Security teams require continuous improvement in operations to identify and respond to fast-evolving threats, including high-fidelity intelligence, contextual data, and automation prevention workflows. They must leverage automation to reduce strain on their analysts and execute the mission of the Security Operation Center (SOC) to identify, investigate, and mitigate threats.

In this guide, we'll help you establish the key processes and best practices to enable your security operations to detect emerging threats and respond effectively and quickly. At every step along the way, we'll show you how you can integrate Zscaler's security analytics and logging capabilities to optimize your policies to power your SOC, including processes for preventing, logging, detecting, investigating, and mitigating threats.

This first installment of a three-part series focuses on leveraging Zscaler logs for analytics and incident investigation using the Zscaler dashboard, and dissecting security logs exported via the Nanolog Streaming Service (NSS) to a Security Information and Event Management (SIEM) system. Subsequent documents will detail the Zscaler technology partnership and API integrations with SOC tools such as SIEM, SOAR, CASB, TIP, etc., for automated response, remediation, and threat hunting.

SOC Goals and Key Processes

Security operations can be defined more broadly as a function that identifies, investigates, and mitigates threats. The four main functions of security operations are:

- Real-time event monitoring, classification, and triage
- Threat assessment, prioritization, and analysis
- Incident response, remediation, and recovery
- Vulnerability assessment, audit, and compliance management

In this section, we'll outline the key Zscaler capabilities for each of these processes. Later, we'll go into much further depth with detailed tips on settings, policies, and approaches for using Zscaler throughout the incident response lifecycle.

Real-Time Event Monitoring, Classification, and Triage

The initial triage is an important step to collect, correlate, and analyze log data to find a "signal in the noise." Key indicators of compromise (IoCs) can be found within user activity, security events, and firewall allow/block, among others. In addition, specific sequences and combinations of these events in specific patterns can signal an event that requires your attention.

As threats and anomalous activities are detected in your environment, Zscaler Internet Access™ (ZIA™) security engines generate logs which are sent to Nanolog clusters in real time. These logs can be viewed/analyzed within the Zscaler dashboards, insights, and logs, and can also be exported to your SIEM through Nanolog Streaming Service (NSS).

Zscaler Nanolog is a verbose record in a compressed format that includes rich threat context and other useful information for event classification and threat hunting.

Threat Assessment, Prioritization, and Analysis

Prioritization is the key to success in any endeavor, and it's even more critical in cybersecurity. Prioritizing events help the security operations team to focus on those that could be the most impactful to business operations and maintaining business continuity. At this stage, it is the responsibility of your security operations team to review and respond to any activity that indicates an adversary has infiltrated your environment.

Powered by threat intelligence from the Zscaler ThreatLabZ research team and numerous threat intelligence feeds from partners, including the Microsoft Active Protections Program (MAPP), Zscaler can detect the specific indicators that signal activity of specific adversary tools, methods, and infrastructure in use and proactively protect against new vulnerabilities.

The log includes fields to identify the engine that generated the event, threat name, type of threat, risk score, matching rule, action taken, and other information to help you quickly analyze, identify, categorize and prioritize the events.

Incident Response, Remediation, and Recovery

The faster you can detect and respond to an incident, the more likely you are to be able to contain the damage and prevent a similar attack from happening in the future. At this stage, the security operations team is responsible for identifying and segmenting the user and network that are impacted and taking remediation steps to recover. The more data points and evidence you have will help in making that determination and acting quickly. In some cases, the security operations team may only be responsible for incident response, with other teams handling remediation and recovery.

Zscaler simplifies remediation and recovery by helping you detect events quickly, so you can respond in time to help prevent further damage. Tools, such as the asset discovery and device posture assessment capabilities with Zscaler Client Connector, deliver updated and detailed information about your assets. User/location profiles allow you to quickly deploy policy as well as identify and isolate impacted users.

Additionally, Zscaler's API capabilities and integrations allow threat correlation and automated response via partner security solutions, such as SIEM, SOAR, and EDR, that are typically used in a security operations workflow.

Vulnerability Assessment, Audit, and Compliance Management

The best security outcome is preventing an attacker from ever infiltrating your system. It's optimal to find and fix vulnerabilities and misconfigurations before an attacker exploits them to gain access to your environments. Running vulnerability scans, configuration audits, and generating compliance reports are some of the most common audit activities for SOC teams looking to find these vulnerabilities and misconfigurations. Keep in mind that these assessments will only identify technical vulnerabilities rather than procedural ones.

From the dashboard, Zscaler allows you to generate on-demand and scheduled reports that provide information tailored for audiences like auditors, executive management, security operators, and others to show compliance, user-level risk exposure, policy misconfigurations, and recommended security policy settings.

Adversary Behavior and the MITRE ATT&CK Framework

MITRE ATT&CK is an adversary model and framework for describing the actions an adversary may take to compromise and operate within an enterprise network. The framework defines adversarial tactics, techniques, and procedures (TTPs), and categorizes them based on the sequence of steps involved in an attack. Associating logs/activities to MITRE ATT&CK tactics can be helpful when identifying the stage of an attack and preventing the attacker's progress. To learn more about MITRE ATT&CK and how Zscaler integrates ATT&CK into ZIA, refer to this white paper **here**.

Zscaler Cloud: Defense-in-Depth Threat Protection Capabilities

ZIA is a cloud-delivered secure internet and web gateway as a service. ZIA is built on a highly scalable, truly distributed, multitenant, purpose-built TCP forward proxy architecture, designed for full content inspection, including SSL decryption. For more information about ZIA, refer to the **ZIA datasheet**.

The Zscaler cloud platform is expertly positioned to disrupt the kill chain. For inbound threats, a layered approach helps stop threats from reputation-based blocking while providing advanced behavioral analysis.

For outbound protection, Zscaler can deliver complete protection from botnet callbacks and malicious outbound activity, disrupting data exfiltration and malware attempting to persist within the network.

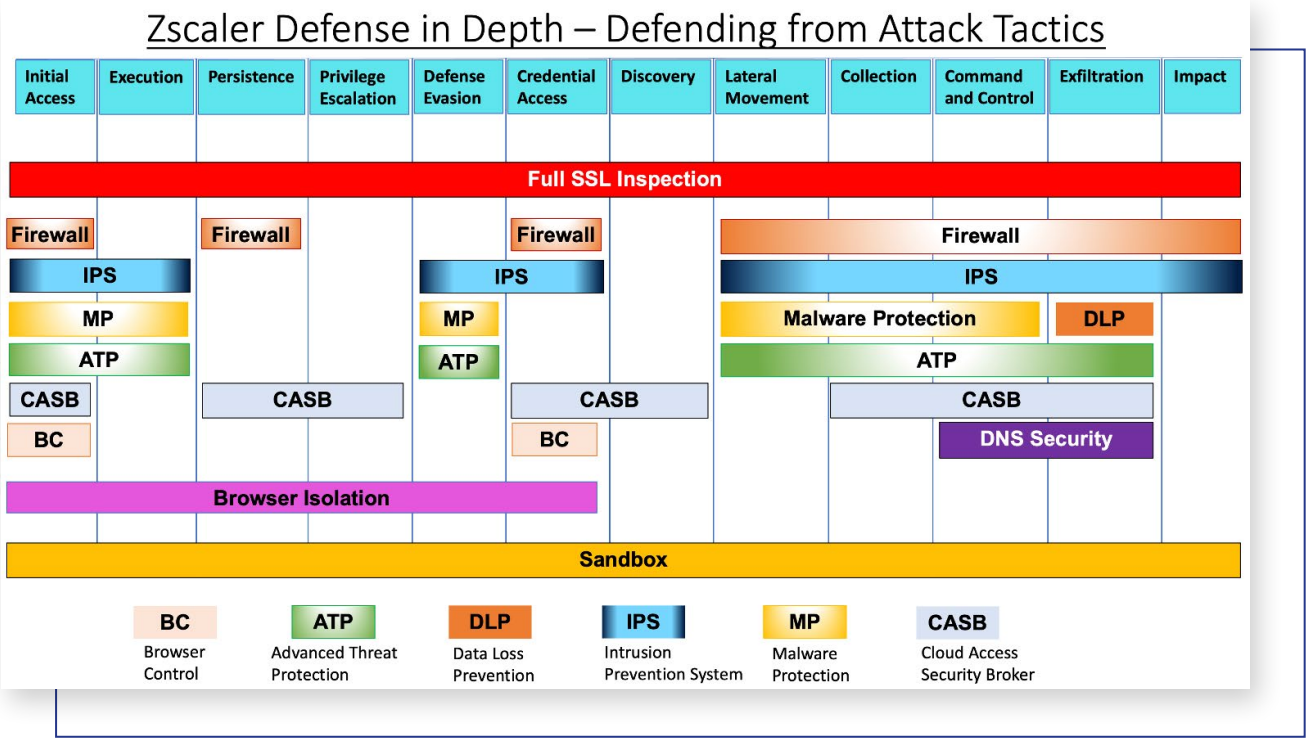


Figure 1. ZIA security engine alignment with the MITRE ATT&CK framework tactics.

Zscaler security services include Advanced Threat Protection (ATP), Browser Control, Browser Isolation, Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), DNS Security, File Type Control, Next-Gen Firewall Control, Intrusion Prevention System (IPS) Control, Malware Protection, Sandbox, SSL Inspection, URL Filtering and Cloud App Control.

Zscaler Internet Access (ZIA) Logging Architecture

Nanolog and Nanolog Streaming Service (NSS)

For all user traffic, the Zscaler Nanolog service creates a verbose log line at the close of the connection. Unlike a typical proxy log, Nanolog includes rich threat context and other useful information for threat hunting.

Zscaler Nanolog consolidates logs from all users, locations, and devices globally into a central repository determined by customers. Administrators can view and mine transaction data by user, device, application, and location in real time. Logs are stored for 180 days in the Zscaler Nanolog servers in North American or European locations specified by customers.

Zscaler Nanolog powers our analytics capabilities—dashboards, insights, and reporting—to provide real-time visibility into user and threat activity.

Zscaler also supports forwarding this log to your on-premises or cloud SIEM in near-real time using NSS, enabling real-time alerting, correlation with the logs of your firewall and other devices, and long-term local log archival.

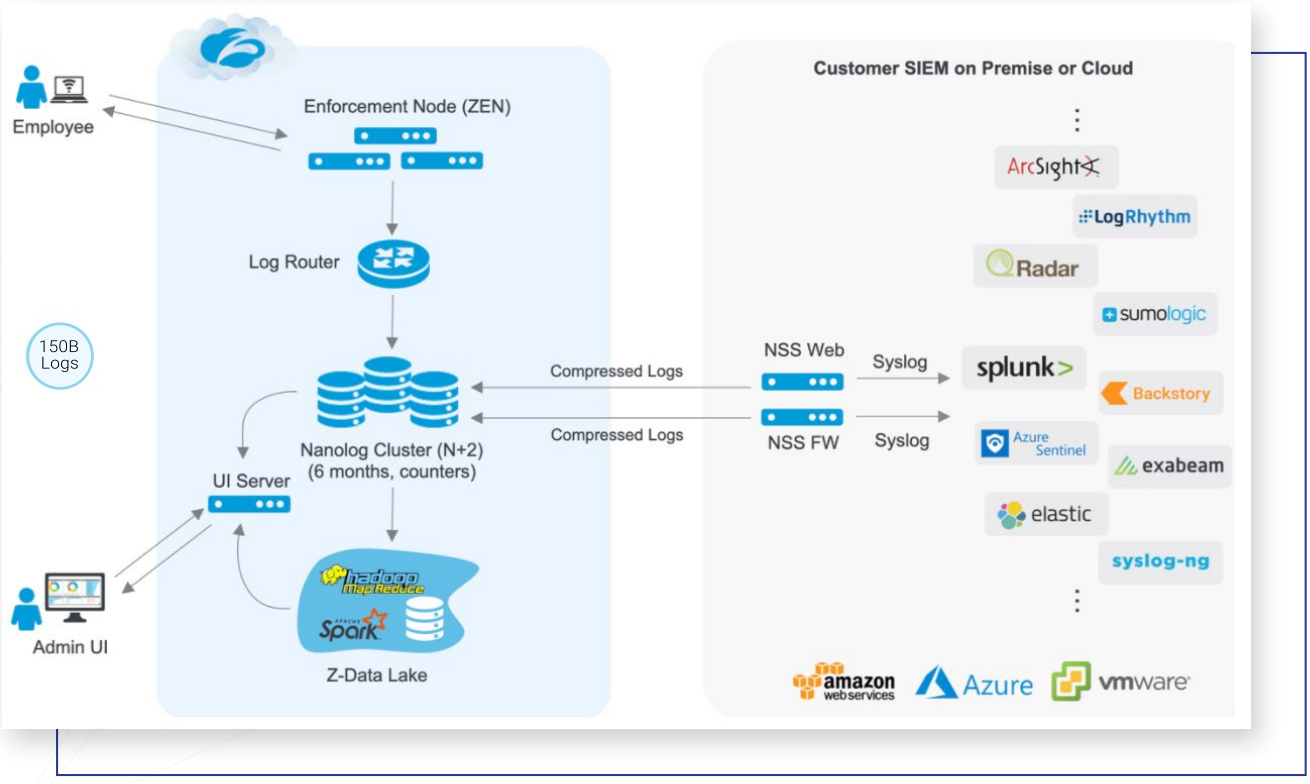


Figure 2. Zscaler Nanolog and Nanolog Streaming Service (NSS) Architecture

ZIA Analytics

Visibility is key to security operations and investigations. Context-rich threat logs provide useful information for analysis, remediation, and threat hunting. ZIA provides multiple tools for log analysis. These include:

- **Dashboards** for near-real-time visibility into your organization's internet traffic and threats
- **Insights and logs** for analyzing traffic from Nanolog clusters through charts
- **Reports** for analyzing data through a wide range of standard reports, based on your organization's subscription, with the ability to create up to 500 custom reports as well.

Role-based administration enables you to granularly control what different admins can do and their access level in the ZIA Admin Portal. These include dashboard **View Only** or **Full Access**, Policy Settings, Traffic Forwarding settings, etc., and hierarchy to ensure that admins do not create conflicting policies and settings. Learn more at: **https://help.zscaler.com/zia/about-administrators**

Dashboards

Multiple dashboards provide different views to track internet usage and quickly take action when you see anomalous trends or security threats. The Zscaler service provides the following predefined dashboards that are relevant to security operations:

- **Web Overview** dashboard provides a high-level view of your organization's web traffic including top advanced threats.
- **Security** dashboard provides data about the various threats that were blocked, such as viruses, spyware, and advanced threats. Additionally, The Sandbox Patient-Zero Events widget lists patient-zero events that occurred in your organization.
- **Web Browsing** dashboard provides visibility into the browsing activity of your users, including top blocked URL categories and top blocked users.
- **DNS Overview** provides data about your organization's DNS traffic.
- **Firewall** dashboard provides data about firewall traffic.
- **IPS Overview** dashboard provides real-time visibility into your organization's IPS traffic.

To learn more about default dashboards: **https://help.zscaler.com/zia/about-dashboards**

Insights and Logs

The Insights and Logs pages are where you can view and define traffic information when analyzing traffic through charts and accessing corresponding Nanolog data. Insights allow you to interactively drill down to specific transactions and are available for the following:

- **Web Insights and Logs** provide access to log data related to web transactions and security events, such as the URLs that were requested, Page Risk Index scores for each, the number of bytes sent and received, and more.
- **Mobile Insights and Logs** provide access to log data related to web transactions and security events, such as the URLs that were requested, Page Risk Index scores for each, the number of bytes sent and received, and more for mobile traffic.

- **Firewall Insights and Logs** provide access to log data related to firewall policy applied, network transactions, client and server details, and network services and applications.
- **DNS Insights and Logs** provides access to data such as the DNS request and response details. You can use data types and filters to define the DNS traffic information you want to view.
- **Threat Insights** page allows you to view organization-specific threats in the form of visual paths from origins to targets. You can choose to view threat statistics in a 2D map or a 3D globe.
- **Tunnel Insights and Logs** provide access to data about GRE and IPSec tunnels, such as their health, status, and authentication and encryption algorithms.
- **SaaS Security Insights and Logs** provide access to log data related to web transactions and security events specific to SaaS applications/tenants configured.

To learn more about how to use Insights to analyze traffic: **https://help.zscaler.com/zia/analyzing-traffic-using-insights**

The Zscaler Nanolog service provides real-time log consolidation across the globe, so you can view every transaction performed by your users regardless of their location. From the Insights page, you can view the logs by clicking on the Logs tab or by clicking on a specific item in the chart and choosing "View Logs." Logs are stored for 180 days in Zscaler Nanolog servers. You can also apply filters to narrow down the list or to find transactions, such as those associated with a specific user or URL. The logs can be exported as a CSV file.

Reports

The Reporting page is where you can view and generate pre-defined reports targeted at specific executive/department/use case. Pre-defined reports are available for the following:

- **Executive Insights Report** provides an organization's key contacts with a monthly overview of the traffic volume and security posture of your organization.
- **CIPA Compliance Report** is an interactive report that provides information on the top URL categories that are blocked from the Legal Liability class, and the top users and domains blocked from accessing obscene or harmful material.
- **Company Risk Score Report** allows organizations to monitor and assess their organizational, location, and user-level risk exposure.
- **Company Summary Report** is an interactive report that provides information tailored for audiences such as the CIO and CSO of your organization.
- **Security Policy Audit Report** allows you to view your security policy settings and improve them by following best practice guidelines.
- **Quarterly Business Review Report** provides customers with extensive insight into how Zscaler is helping protect their network, quarter to quarter. It helps customers observe emerging traffic trends and the types of threats that Zscaler is blocking.
- **SaaS Asset Summary Report** allows you to view a summary of SaaS Security API-based discovery and remediation activities. This serves as the starting point when investigating what data is affected and identifying risky users.
- **SaaS Assets Report** shows you the current state of your files and email messages. It also allows you to see the activity for any particular file or email message all in one place.

- **Anomaly Detection Report** (new in Release 6.1) helps you identify potential data exfiltration events and malicious insiders with a high-confidence detection of anomalous user behavior and organization-level anomalies.

Additionally, Interactive Report supports real-time interactive analysis and presents a wide range of standard reports such as The Company Summary Report (CSO). Furthermore, you can view details such as the specific URLs that users requested, risk score of each URL, and more. Scheduling reports delivers standard and custom reports for regular distribution to specified recipients.

Zscaler Nanolog Streaming Service (NSS)

Zscaler NSS offers two streams of highly compressed logs that can be streamed to your SIEM:

- NSS for Web: Streams web and mobile traffic logs.
- NSS for Firewall: Streams logs from the Zscaler next-generation firewall.

The web and mobile traffic logs and the firewall logs are stored in the Nanolog in the Zscaler service cloud. The logs are encrypted and streamed in a highly compressed format to reduce the bandwidth footprint. An organization must deploy an NSS Virtual Machine (VM) that unscrambles the logs, applies the configured filters to exclude unwanted logs, converts the filtered logs to the configured output format so they can be parsed by your SIEM, and then streams the logs to your SIEM over a raw TCP connection.

We recommend deploying at least one NSS for web and mobile logs and another NSS for firewall logs. Each NSS opens a secure tunnel to the Nanolog in the Zscaler cloud.

NSS for Weblogs

NSS for Weblog stream is a verbose record in a compressed format that includes rich threat context and other useful information for remediation and threat hunting. It includes more than 100 fields. You can configure NSS feeds to selectively filter and send logs for web proxy, tunnel, SaaS security logs, and alerts to your SIEM as separate feeds.

Streams of events are generated for the below log types:

- Proxy Logs: All access logs processed by Zscaler proxy including IPS (web) logs
- Tunnel Logs: Up/Down tunnel events and summary usage statistics
- SaaS Security Logs: Cloud access security broker (CASB) events generated for SaaS applications
- Alerts Logs: System alerts for events such as connectivity loss

NSS for Firewall Logs

NSS for Firewall Log stream includes firewall and DNS logs in a compressed format. You can configure NSS feeds to selectively filter and send logs for firewall, DNS, and alerts to your SIEM as separate feeds.

Streams of events are generated for the below log types:

- Cloud Firewall logs: All access logs processed by Zscaler Cloud Firewall including IPS (non-web) logs
- DNS logs: Logs for DNS traffic where DNS traffic is sent via Zscaler
- Alerts: System alerts for events such as connectivity loss

IPS Web vs. IPS Non-Web

IPS for Web included in Advanced Threat Protection is a signature-based engine that detects threats coming from web traffic (HTTP, HTTPS, and FTP), such as cross-site scripting, botnet, command-and-control traffic, embedded/malicious web pages, etc.

IPS for non-Web included in Firewall is a signature-based engine that detects network-level intrusions over all ports and protocols. This includes protection for HTTP, HTTPS, FTP, DNS, TCP, UDP, and IP-based ports and protocols. IPS Control also enables you to create granular rules for specific users, groups, departments, and so on. You can enable **IPS Control** on a per-location basis.

Detected threats for web traffic will show in **Weblog** and non-web traffic will show in **Firewall log**. Detected threats for both web and non-web traffic will show in **Firewall Insights > Logs**. Threats detected from web-only traffic also appear in the **Security Dashboard**. Threats detected from non-web traffic also appear in the **IPS Dashboard**.

Note: Web IPS policy is applied first followed by non-Web IPS.

NSS Deployment

An organization can deploy the NSS instance on-premises, on an ESX Virtual Machine, on an EC2 Instance, on AWS, or on Microsoft Azure. NSS deployment guides for these platforms are below:

https://help.zscaler.com/zia/nss-deployment-guide-amazon-web-services
https://help.zscaler.com/zia/nss-deployment-guide-microsoft-azure
https://help.zscaler.com/zia/nss-deployment-guide-vmware-vsphere

Syslog Formats

Zscaler supports many syslog formats. This includes industry-standard formats and the ability to create custom log strings. The Common Event Format (CEF) and Log Event Extended Format (LEEF) are two primary standards used by SIEMs. To learn more: **https://help.zscaler.com/zia/syslog-overview**

NSS Feeds

An NSS feed specifies the data from the logs that the NSS will send to the SIEM. Each feed can have a different list of fields, a different format, and different filters. You can add one or more feeds for the logs and one feed for alerts. You can add up to eight NSS feeds for each NSS.

Refer to the following help articles for configuring NSS feeds:

https://help.zscaler.com/zia/adding-nss-feeds-alerts
https://help.zscaler.com/zia/adding-nss-feeds-dns-logs
https://help.zscaler.com/zia/adding-nss-feeds-firewall-logs
https://help.zscaler.com/zia/adding-nss-feeds-saas-security-logs
https://help.zscaler.com/zia/adding-nss-feeds-tunnel-logs
https://help.zscaler.com/zia/adding-nss-feeds-web-logs

NSS Feed Output Format

Feed Output Format defines the fields that will be displayed in the output. For each NSS feed/log type, there is a default feed output format populated when you add a new feed and select the log type. You can edit the default list; if you choose **Custom** as the **Field Output Type**, change the delimiter as well.

For all possible fields and formats, refer to the below links:

https://help.zscaler.com/zia/nss-feed-output-format-dns-logs
https://help.zscaler.com/zia/nss-feed-output-format-firewall-logs
https://help.zscaler.com/zia/nss-feed-output-format-tunnel-logs
https://help.zscaler.com/zia/nss-feed-output-format-saas-security-logs
https://help.zscaler.com/zia/nss-feed-output-format-web-logs

We recommend following the general guidelines for NSS feeds and feed formats provided in the following help article: **https://help.zscaler.com/zia/general-guidelines-nss-feeds-and-feed-formats**

Dissecting a Weblog

The weblog provides access to log data related to web transactions and security events. Weblog provides threat context that is spread over 100 fields. Broadly, there are five different categories of security logs that can be dissected from the weblog for investigation:

- **Content Filtering** (URL Filtering & File Type Control)
- **Malware Protection** (Reputation, AV, Yara)
- **Advanced Threat Protection** (Reputation, IPS [web])
- **Sandbox** – Known Malicious (Cloud Effect)
- **Sandbox** – Unknown (potential zero-day)

While there are many fields included in the weblog for each category, in general, the following key fields can be used to search/identify the five different categories of security logs mentioned above for your investigation:

Weblog Field	Web Insights Field	Description & Example
Ruletype	Policy Type	Policy type (applies only to Block rules, not Allow) e.g., File Type Control, Data Loss Prevention, Sandbox
Rulelabel	Rule Name	Name of the rule applied (applies only to Block rules, not Allow) e.g., URL_Filtering_1
malwareclass	Threat Class	The class of malware that was detected in the transaction e.g., Win32.Ransom.WannaCry
malwarecat	Threat Category	The category of malware that was detected in the transaction e.g., Adware, Trojan, Sandbox Malware
urlclass	URL Class	Class of the destination URL e.g., General Surfing, Privacy Risk
urlcat	URL Category	Category of the destination URL e.g., Entertainment, Adult Themes, Games
filetype	File Type	Type of file associated with the transaction e.g., RAR Files, ZIP, Windows Executables
fileclass	File Class	Type of file associated with the transaction e.g., Active Web Content, Archive Files, Audio
threatname	Threat Name	The name of the threat that was detected in the transaction e.g., win32.banker.trickbot
reason	Policy Action	Action that the service took and the policy that was applied, if the transaction was blocked e.g., Virus/Spyware/Malware Blocked; Not allowed to browse this category

You can also use the "reason" field to distinguish between reputation block vs. content-based block (e.g., "IPS block outbound request: botnet command-and-control traffic" vs. "reputation block outbound request malicious URL").

The following fields may also be useful for your investigation:

Weblog Field	Insights Field	Description & Example
ssldecrypted	SSL Inspected	Tells you whether the transaction was SSL inspected or not e.g., Yes or No
referrer	Referrer URL	HTTP referer URL e.g., www.google.com
location	Location	Gateway location or sublocation of the source e.g., Headquarters
bamd5	MD5	The MD5 hash of the malware file that was detected in the transaction or the MD5 of the file that was sent for analysis to the Sandbox engine
riskscore	URL Class	The Page Risk Index score of the destination URL. The service computes risk for each page by weighing several factors; the range is 0 to 100, from the lowest to the highest risk e.g., 10

Additionally, you can use "**protocol**" as a key field to identify/search for stealthy threats that use HTTP, HTTPS, or SSL.

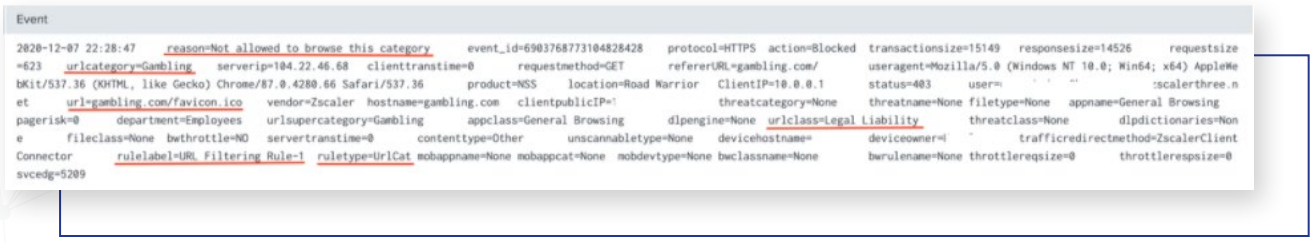
Content Filtering (URL Filtering and File Type Control) Logs

Analyzing Content Filtering Logs can identify traffic blocks due to policy violations, such as URL category not allowed, or File type, such as EXE files, are not allowed to be downloaded.

The following key fields and search parameters are useful when dissecting the weblog to identify traffic blocks due to URL category filtering policy violation:

ruletype="UrlCat"
rulelabel="<rulename>"
urlcat=<predefined>, <custom> or <TLD>

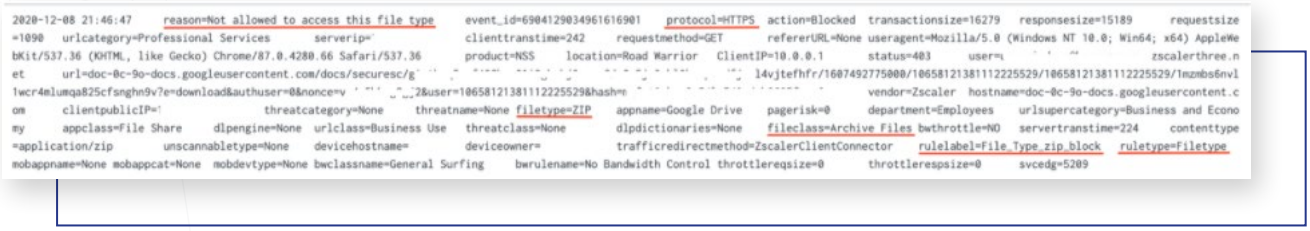
Sample URL Filtering Log



The following key fields and search parameters are useful to dissect the weblog to identify traffic blocks due to File Type Control policy violation:

ruletype="Filetype"
rulelabel="<rulename>"
fileclass="Executable, Archive, Office,..."
filetype="exe, exe64, py,..."

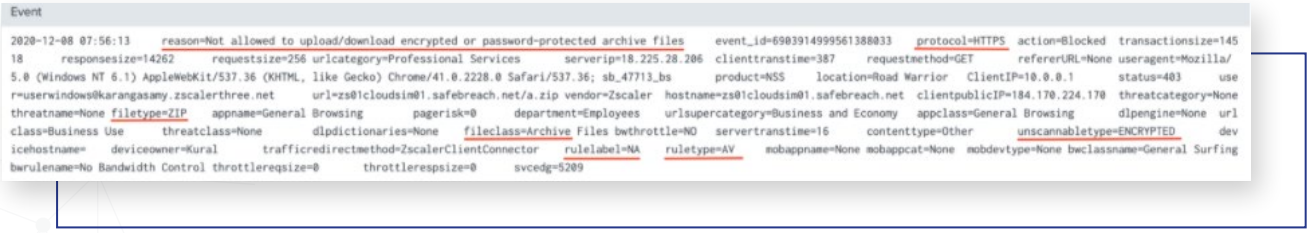
Sample File Type Control Log



Additionally, if for any reason, we cannot parse or scan the file content, e.g., corrupt archive, password protected, unable to determine the file type, etc., a special field "unscannabletype" shows the reason for the scan failure. You can use this field to search/identify the files that were not scanned.

unscannabletype="Unscannable", "Undetectable", "Encrypted/Password Protected"

Sample Unscannable File Log



Malware Protection (Reputation, AV, Yara) Logs

Analyzing the Malware Protection Log helps the security team identify potential threats, such as policy violators, malicious file downloads, or compromised users/endpoints/devices, and take corrective action before the threat becomes widespread. This type of log includes malware detection verdicts, namely file reputation, antivirus and Yara file scanning for files transferred over HTTP(S).

The following key fields and search parameters are useful to dissect the weblog to identify traffic blocks due to malware: **ruletype**="AV"

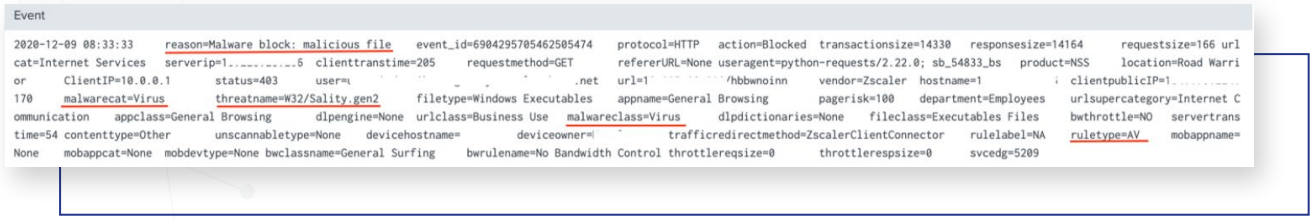
Additionally, you can use the "**malwarecat**" or "**malwareclass**" field to search / identify threats blocked in a specific malware category or malware class:

malwarecat="Adware," "Archive Bomb," "Backdoor," "Dialer," "Downloader," "Exploit," "Macro Virus," "MalwareTool," "Other Malware," "Other Spyware," "Other Virus," "Password Stealer," "Ransomware," "Trojan," "Unrecognized Virus," "Unwanted Application," "Worm," "None"

malwareclass=<custom>
e.g. **malwareclass**="Virus", "Spyware"

You can also use the "**reason**" field to search/identify malware blocks.

Sample Malware Protection Log



Advanced Threat Protection (Reputation, IPS [web]) Logs

Analyzing the Advanced Threat Protection log helps security teams identify potential threats, such as malicious destinations/contents/traffic patterns, phishing, command-and-control traffic, compromised users/endpoints/devices, and vulnerable and potentially unwanted applications, and take corrective action before threats become widespread. This type of log includes cloud IPS and reputation-based engine detection of advanced threats. Reputation-based detection looks for suspicious destination IPs, domains, or URLs, and leverages Page Risk Index which calculates the risk of a page in real-time by identifying malicious content within the page. The IPS engine uses signature-based detection and has a high fidelity rate. IPS botnet callback is high confidence as it is written based upon communication patterns. Some threats, such as browser exploit, SSH tunneling, and cookie stealing can only be detected by IPS.

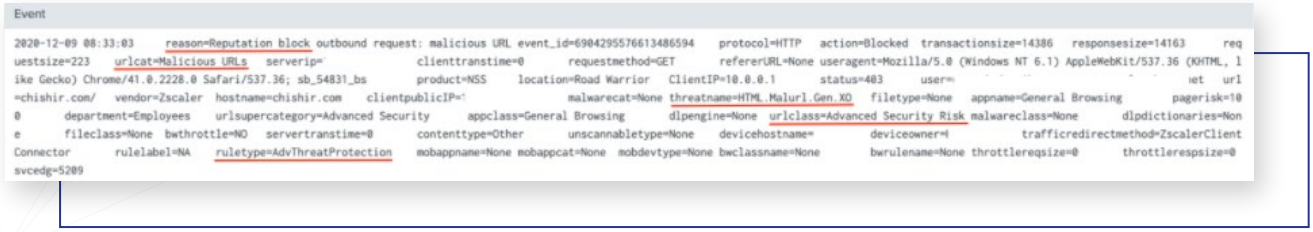
You can use the "**reason**" field to search/identify advanced threat blocks and differentiate between "reputation" vs. "IPS" blocks.

The following key fields and search parameters are useful for dissecting the weblog to identify traffic blocks due to advanced threats: **ruletype**="AdvThreatProtection"

Additionally, you can use the "**urlcat**" or "**urlclass**" field to search/identify threats blocked in a specific URL category or URLs that are classified as advanced security risk: **urlclass**="Advanced Security Risk"

urlcat="Adv Security," "Phishing," "Botnets," "Malicious URLs," "Peer-to-peer," "Unauthorized Communication," "Cross-site Scripting," "Browser Exploit," "Suspicious Destinations," "Suspected Spyware or Adware," "WebSpam," "PageRisk," "Adware/Spyware Sites," "Cryptomining"

Sample Advanced Threat Protection Log

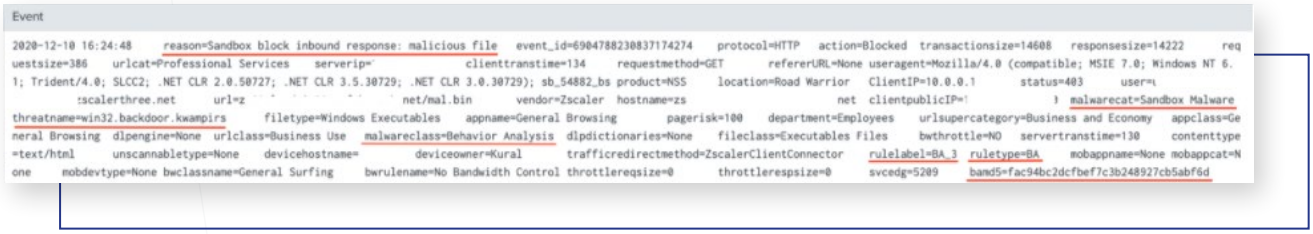


Sandbox – Known Malicious (Cloud Effect) Logs

The Sandbox environment is used to detonate unknown file samples to determine if there's malicious behavior. When files are submitted to the Sandbox for analysis, the end user may be quarantined or allowed to download the file, which is determined by customer-specific sandbox policies. This type of log includes verdicts for unknown files submitted to the sandbox that the sandbox determined to be malicious.

The following key fields and search parameters are useful to dissect the weblog to identify traffic blocks due to sandbox determined malicious behavior: **ruletype**="BA"
malwarecat="Sandbox Malware", "Sandbox Adware", "Sandbox Anonymizer"

Sample Known Sandbox Malicious log



If your organization has Advanced Cloud Sandbox and API license, you can get a Sandbox Detail Report based on the MD5 parameter that you retrieve from your logs in the SIEM. If the MD5 is not included in the log, you can add the key field "**bamd5**" to your feed to retrieve it from the weblog. You can use the Cloud Sandbox API to retrieve a full detail report for the MD5 hash. Please refer to the API reference link below for syntax on how to retrieve this report: **https://help.zscaler.com/zia/api**

Sandbox – Submissions (Unknown) Logs

The Sandbox environment is used to detonate unknown file samples to determine if there's malicious behavior. When files are submitted to the Sandbox for analysis the end user may be quarantined or allowed to download the file, which is determined by customer-specific sandbox policies. This type of log includes unknown files submitted to the sandbox and will go through the sandbox execution phases.

The following key fields and search parameters are useful for dissecting the weblog to search/identify files that have been submitted for sandbox analysis:

ruletype="BA"
malwarecat="Sent for Analysis"

Mapping Actions/Events to Engines and Policy Reason

The "reason" field included in the weblog is a verbose descriptor of event type and engine that detected the threat event. There are over 100 possible values that map nicely to individual security/policy engines. For example, "Malware block: malicious file" is detected by "Malware Protection" engine, "IPS block inbound response: anonymization site" is detected by Cloud IPS in "Advanced Threat Protection" engine, and so on. To learn more: **https://help.zscaler.com/zia/policy-reasons**

Dissecting a Firewall Log

The Firewall Log provides access to log data related to NGFW, DNS, and IPS (non-web) transactions and security events. IPS events are sent along with Firewall events. DNS events are sent in a separate feed. Firewall log provides threat context that is spread over 50 fields. Broadly, there are three different categories of security logs that can be dissected from the firewall log for investigation:

- **Firewall** (session, device, network services and applications, destination)
- **IPS** (non-web)
- **DNS**

While there are many fields that are included in the firewall log for each category, in general, the following key fields can be used to search/identify the different categories of security logs mentioned above for your investigation:

Firewall Log Field	Firewall Insights Log Field	Description & Example
Rulelabel	Rule Name	Name of the rule that was applied to the transaction e.g., Recommended Firewall Rule
nwsvc	Network Service	The network service that was used e.g., HTTP, DNS
nwapp	Network Application	The network application that was accessed e.g., Skype
cdip / cdport	Client Destination IP / Client Destination Port	Client Destination IP/Port e.g., 198.51.100.54, 53
tsip	Client Tunnel IP	Tunnel IP address of the client (source) e.g., 192.0.2.15
destcountry	Country	Country of the destination IP address e.g., United States
ipsrulelabel	IPS Rule Name	Name of the IPS policy that was applied to the Firewall session e.g., Default Cloud IPS Rule
threatcat	Threat Category	Category of the threat in the Firewall session by the IPS engine e.g., Botnet Callback
threatname	Threat Name	Name of the threat detected in the Firewall session by the IPS engine e.g., Win32.Trojan.DNSpionage
ipcat	Server IP Category	URL category that corresponds to the server IP address e.g., Internet Services

DNS Log Field	DNS Insights Log Field	Description & Example
reqtype	DNS Request Type	DNS record being requested e.g., A record
req	Requested Domain	Fully Qualified Domain Name (FQDN) in the DNS request e.g., mail.safemarch.com
res	DNS Response	DNS response e.g., 198.51.100.54
sport	Server Port	Server port of the request e.g., 53
domcat	IP Domain Category	URL Category of the FQDN in the DNS request e.g., Professional Services

Zscaler API

Zscaler supports a number of open APIs for customer utilization, which include read and write functions. The cloud service API gives you programmatic access to the following Zscaler Internet Access (ZIA) features:

- Creating and downloading an audit log report of policy changes made in the ZIA Admin Portal and in the API
- Getting admin roles and managing admins
- Getting and updating VPN credentials for specific locations
- Getting Sandbox Detail Reports
- Managing individual users, groups, and departments
- Managing IPSec VPN tunnels for SD-WAN partner integrations
- Managing locations and sub-locations
- Managing root certificates, Certificate Signing Request (CSRs), and intermediate certificate chains
- Managing and updating URL Categories
- Managing URL white lists and black lists

Full specifications for the Zscaler API can be found here: **https://help.zscaler.com/zia/api**

Sandbox

The Zscaler Cloud Sandbox service provides an additional layer of security against unknown and zero-day threats and Advanced Persistent Threats (APTs) through Sandbox analysis, an integrated file behavioral analysis. When files are submitted to the Sandbox for analysis the end user may be quarantined or allowed to download the file, which is determined by customer specific sandbox policies. To learn more: **https://help.zscaler.com/zia/configuring-sandbox-policy**

The results of the sandbox detonations can be of significant interest to customers, as a malicious verdict may indicate a user is compromised and/or engaging in behavior introducing risk to themselves and the customer's business. As such, Zscaler has made full Sandbox reporting a feature of the product, and this includes the capability to pull API detailed sandbox post-detonation reports.

If your organization has Advanced Cloud Sandbox, you can open a Sandbox Detail Report based on the MD5 parameter that you retrieve from your logs in the SIEM. To learn more:
https://help.zscaler.com/zia/viewing-sandbox-reports-data

Audit Logs

As administrators access the Zscaler console, and make changes within the console, an Audit log is generated. These events often need to be archived outside of Zscaler, and Zscaler has made these events available via the Zscaler API.

Zscaler Alerts

Alert subscription service provides the ability to send email to specific individuals when certain events occur, such as when a security or access control event, system and compliance violation alert, or patient-zero event occurs. To learn more about alerts and how to define an alert, refer to the help text article:
https://help.zscaler.com/zia/about-alerts

Security Operations Best Practices

Security Policy Best Practices

Malware Protection Policy:

- Configure a malware protection policy to protect your organization from viruses, trojans, worms, malware, ransomware, unwanted applications, adware/spyware, etc.
- Enable both inbound and outbound traffic inspection.
- Security exception – we recommend blocking password-protected files and unscannable files if these types of files are not in day-to-day use in your organization.
- Follow the **Recommended Malware Protection Policy**.

Advanced Threat Protection (ATP) Policy:

- Configure an ATP policy to protect your organization from fraud, botnet activity, unauthorized communication, cross-site scripting (XSS), command-and-control traffic, risky applications, such as ToR and BitTorrent, phishing sites, suspicious destination (country), and other malicious objects and scripts.
- Page Risk setting – this is a Suspicious Content Protection (Page Risk Index) value and is calculated dynamically for every web page in real time. This score is then evaluated against the value that you set. The recommended setting is 35. You can set it to a different value based on your organization's risk aversion. Higher value means more risk.

- Security exceptions – You can use "Do Not Scan Content from these URLs" setting to add URLs of sites you do not want scanned, such as your organization's public site or other trusted sites that may be failing due to antivirus, anti-spyware, or anti-malware policies. The service allows users to download content from these URLs without inspecting the traffic. To learn more: **https://help.zscaler.com/zia/whitelisting-urls**
- Follow the **Recommended Advanced Threat Protection Policy**.

Browser Control Policy:

- Browser vulnerability protection – Configure a browser control policy to warn users from going out to the internet when they are using outdated or vulnerable browsers, plugins, and applications.
- Browser blocking – To reduce the risk of older, vulnerable browsers being used, we recommend blocking the use of older browser versions.

File Type Control Policy:

- Configure a file type control policy to block executable file downloads from uncategorized websites, caution against download from any URL category, block executable file uploads to any URL category, and block undetectable file types.
- Follow the **Recommended File Type Control Policy**.

Data Loss Prevention (DLP):

- Configure a DLP policy to protect your organization from data loss, which can be leaked through web mail, cloud storage, social media, and a variety of other applications.

Firewall Control Policy:

- Configure firewall filtering policy to define which types of traffic are allowed from specific sources and to specific destinations. By default, the Zscaler firewall allows all non-HTTP/HTTPS traffic from your network to the internet.
- Allow only specific services that are needed and block everything else, for example, DNS, HTTP, HTTPS.
- Block unused protocols in your environment, for example, SSH, TFTP.
- Block insecure protocols, such as POP3, IRC, Telnet, FTP.
- Follow the Recommended Firewall Control Policy.

Intrusion Prevention System (IPS) Control:

- IPS (non-web) uses signature-based detection, which is a high-confidence engine to control and protect your traffic from intrusion over all ports and protocols.
- Default logging for IPS is set to aggregate, which groups together individual sessions based on { user, rule, and network service } and records them periodically.
- If you need full logging that logs all sessions of the rule individually, enable this by editing the default IPS policy and selecting **Aggregate** under **Logging**.
- Once you have configured your IPS policy, you can **Enable IPS Control** on a per-location basis when enabling Firewall.
- Follow the **Recommended IPS Control Policy**.

URL Filtering and Cloud App Control Policy:

- Configure URL filtering to limit your exposure to liability by managing access to web content based on a site's categorization.
- Configure Cloud App Control to granularly control access to only sanctioned cloud applications and related activities, such as instant messaging (e.g., Google Hangouts, chat, and file transfer), social networking (e.g., Facebook viewing and posting), streaming media (e.g., YouTube viewing/listening and uploading), webmail (e.g., Yahoo webmail viewing, sending, and sending attachments).
- By default, Cloud App Control takes precedence over the URL filtering policy. To change this behavior and apply the URL filtering policy even if it has already applied a Cloud App Control policy, enable **Allow Cascading to URL Filtering** under **Administration > Advanced Settings**.
- Enable the Newly Registered Domain lookup setting to use it in URL filtering policy.
- Configure URL filtering policy to caution the user when visiting uncategorized URLs, newly registered domains, or misc/unknown categories.
- Follow the **Recommended URL & Cloud App Control Policy**.

SSL Inspection:

- We recommend enabling SSL decryption and inspection for all possible traffic as more and more malware is hidden within encrypted traffic.
- Define a "Do not inspect SSL" list:
  i. Per compliance requirements of customer or local government
  ii. Sites that require client certificate-based authentication
  iii. Sites that perform certificate pinning
  iv. IDP URLs, such as Okta, Azure AD
- Enable SSL inspection through location settings: **ZIA Admin Portal > Administration > Location Management** > (Location Policy) **> Enable SSL Inspection**.
- Enable SSL inspection for road warrior clients through SSL Inspection Settings: **ZIA Admin Portal > Policy > SSL Inspection > Policy for Zscaler Client Connector** section.
- If SSL inspection is disabled, use the "If SSL inspection is disabled, block https to these sites" setting to block HTTPS to high-risk URL categories.
- We recommend enabling the "Block Undecryptable Traffic" setting.
- To learn more about SSL inspection, refer to **About SSL Inspection**.

Sandbox Policy:

- Configure a sandbox policy to inspect unknown files and block unknown and zero-day threats.
- You can use Quarantine or Allow & Scan policy actions depending on your risk tolerance vs. your performance requirement.
- We recommend configuring Quarantine action for executables and Office document downloads from high-risk categories, such as nudity, pornography, anonymizer, miscellaneous, or unknown categories, etc.
- We recommend configuring Allow & Scan for all other file types followed by **P-0 alert** setup.
- Follow the **Recommended Sandbox Policy**.

Block non-rfc compliant HTTP traffic through **ZIA Admin Portal > Administration > Advanced Settings** page.

Enable auto proxy forwarding for HTTP/HTTPS/FTP/DNS/RTSP/PPTP when they are using non-default ports through **ZIA Admin Portal > Administration > Advanced Settings** page.

Security Log Analysis Best Practices

ZIA Dashboards, Insights, and Logs:

1. **Dashboards** show near real-time data. You can start with a Security **Dashboard** as a place to monitor threat events, rollover a chart to obtain more info and pivot to Logs or Insights from the events directly by clicking on the event as it occurs.

2. Use "**Role-based administration**" to define an admin role and ensure only authorized users have access to dashboards and at appropriate levels, such as **View Only** or **Full Access**.

3. **Customizing Dashboards**: You can customize the dashboard by adding, editing, or deleting widgets to view the events that you are interested in. Adding a "**Threat Category**" custom dashboard helps with a quick view of all different threat category events for your organization. If you are interested in a specific threat category view, such as phishing events, you can use the "Phishing" filter under "Advanced Threat Super Category" data type to create a customized widget as shown in the table below.

You can also edit the default dashboard to include additional filters that you want to include. For example, add a "Location" if you are interested in seeing the events specific to that location or use "Protocol" as a filter to look for stealthy threats that use HTTP, HTTPS, or SSL.

4. **Dashboard Refresh:** We recommend that you set your dashboards to automatically refresh every 15 minutes. This prevents your session from timing out and also keeps the information in your window up to date. Go to **Administration > My Profile** to enable automatic refresh.

5. To add a widget to a dashboard, click the **Add Widget** icon. You can add widgets for web, mobile, firewall, and DNS events. A dashboard can contain up to 12 widgets.

6. Insights and Logs pages allow access to the Nanolog data that includes rich threat context spread over 70+ fields. As a best practice, you can start from the dashboard events and pivot to the Logs and use filters to narrow down your search or access directly from the Insights section under Analytics Tab and clicking on Logs.

7. While there are many filters that are available in the Insights log, in general, it is a best practice to start with one or more of the following key filters and include others, such as user, location, etc., to narrow the search further.

NSS Best Practices

Web Insights Log Filters:

Web Insights Log Filter	Usage
Advanced Threat Super Category	Use this filter to limit the data to a specific advanced threat category, such as “Adware/Spyware Sites,” “Browser Exploit,” “Cross-site Scripting,” “Crypto Mining & Blockchain,” “Phishing,” etc.
Policy Type and Rule Name	Use this filter to view transactions matching specified policy type and the configured rule name.
Sandbox	Use this filter to view file downloads based on the Sandbox result: Sandbox Adware, Sandbox Anonymizer, Sandbox Benign, Sandbox Malware, Sent for Analysis
Threat Category	Use this filter to limit the data to a specific threat category, such as “Exploit,” “Proxy,” “Ransomware,” “Trojan,” “Worm,” etc.
Threat Super Category	Use this filter to limit the data to a specific threat super category, such as “Malware” or “Virus,” etc.
Threat Class	Use this filter to look for transactions associated with a specific threat class, such as “Advanced Threats,” “Viruses & Spyware.”
Threat Name	Use this filter to look for transactions associated with a specific threat that you are particularly interested in.
Unscannable Type	Use this filter to look for file scan failures due to reasons, such as “Encrypted File,” “Undetectable File,” or “Unscannable File.”
URL Category	Use this filter to limit the data to a specific URL category. You can choose to include or exclude certain categories.
Protocol	Use this filter to search for stealthy threats that use HTTP, HTTPS, or SSL.

For more data types and filters: **https://help.zscaler.com/zia/web-data-types-and-filters**

Mobile Insights Log Filters:

Mobile Insights Log Filter	Usage
Mobile Application Category	Use this filter to limit the data to a specific mobile application category, such as “Malware App,” “Social Networking,” “Streaming Media,” “Vulnerable App,” etc.
Mobile Device Type	Use this filter to limit the data to traffic associated with a specific type of mobile device, such as “Apple iPad,” “Google Android,” “Samsung Galaxy S,” “Windows Mobile,” etc.
Protocol	Use this filter to limit the data to traffic to protocols of the mobile traffic, such as “HTTP,” “HTTPS,” “SSL,” etc.

For more data types and filters: **https://help.zscaler.com/zia/mobile-data-types-and-filters**

Firewall Insights Log Filters:

Firewall Insights Log Filter	Usage
Client IP/Port	Use this filter to limit the display to a specific client source/destination IP address or port.
Client Tunnel IP	Use this filter to limit the display to a specific client tunnel IP address.
Server IP/Port	Use this filter to limit the display to a specific server source/destination IP address or port.

For more data types and filters: **https://help.zscaler.com/zia/firewall-data-types-and-filters**

DNS Insights Log Filters:

DNS Insights Log Filter	Usage
DNS Request Type	Use this filter to limit the data to the traffic associated with a specific type of DNS request.
DNS Response	Use this filter to limit the data to the traffic associated with a specific DNS response including DNS error codes.
IP Domain Category	Use this filter to limit the data to the traffic associated with the URL category of the requested domain.
Requested Domain	Use this filter to limit the data to the traffic associated with the domain for which DNS resolution was requested.
Server IP/Port	Use this filter to limit the data to traffic associated with a specific server IP address or server port.

For more data types and filters: **https://help.zscaler.com/zia/dns-data-types-and-filters**

Tunnel Insights Log Filters:

Tunnel Insights Log Filter	Usage
Tunnel Source/Destination IP	Use this filter to view metrics associated with a specific source/destination IP address.
Tunnel Type	Use this filter to view metrics based on different types of tunnels, such as GRE and IPSec.

For more data types and filters: **https://help.zscaler.com/zia/tunnel-data-types-and-filters**

SaaS Security Insights Log Filters:

Saas Security Insights Log Filter	Usage
Application Category	Use this filter to limit the data to a specific SaaS application category, such as “CRM,” “Email,” “File,” “Repository.”
Application	Use this filter to limit the data to a specific SaaS application, such as “Box,” “Dropbox,” “Google Drive,” “OneDrive,” “ShareFile,” “SharePoint.”
DLP Dictionary	Use this filter to see the dictionary that triggered the event, such as “Credit Cards,” “Social Security Numbers,” Salesforce.com Data,” etc.
DLP Engine	Use this filter to view scans associated with specific DLP engines, such as “Credit Card Numbers,” “HIPAA,” “PCI,” “Social Security Numbers,” etc.
Incident Type	Use this filter to view scans associated with a specific incident type, such as “DLP” or “Malware Detection.”
Tenant	Use this filter to view scans associated with a specific tenant.
Threat Category	Use this filter to view scans associated with a specific threat category. These threats are detected by Malware Protection.
Threat Super Category	Use this filter to view scans associated with a specific threat super category, such as “Advanced Threat,” “Malware Detection,” “Sandbox,” “Spyware,” or “Virus.”

For more data types and filters: **https://help.zscaler.com/zia/saas-security-insights**

1. Deploy NSS on AWS or Azure for seamless Zscaler cloud-to-SIEM cloud integration.
2. The default NSS weblog feed output format includes more than 30 fields. You can add more fields by following the **NSS Feed Output Format: Weblogs**.
3. In general, it is recommended to include no more than 50 fields in the NSS feed to accommodate for syslog message size limits. However, if your SIEM is able to ingest larger message sizes, you can configure more than 50.

Security Log Reporting Best Practices

1. Use role-based administration to ensure that only authorized admins are allowed to generate reports.
2. Run the **Security Policy Audit Report** to make sure all recommended settings are followed.
3. Run the "Which users had advanced threat incidents" report from **Interactive Reports > Standard Reports > Security Threats** section periodically to identify risky users and do further investigation on those specific users using either Web Insights or SIEM.
4. Run the "Top threat names" report from **Interactive Reports > Standard Reports > Security Threats** section periodically to spot web as well as non-web threat trends, such as the start of a phishing campaign or command-and-control/botnet activity and pivot to logs to do further investigation using either Web Insights or SIEM.
5. Run the "Distribution of Traffic by Protocol" report from **Interactive Reports > Standard Reports > Secure Browsing** section periodically to spot threat trends in encrypted vs. unencrypted protocols. For example, if you see more threats being blocked under "SSL," it's time to reevaluate your SSL decryption policy to include more traffic for SSL inspection.
6. Run the "Firewall Application & Services Overview" report from **Interactive Reports > Standard Reports > Firewall Activity** section periodically to spot any unusual application or volume of traffic that is suspicious and do further investigation using either Web Insights or SIEM.
7. Run the **Company Risk Score** report daily:
   - to understand your organization's overall security risk exposure score, risk score trend, risk score compared to others in the same industry and overall cloud customer;
   - to identify events that contributed to a high risk score, such as botnet activity, malicious content, phishing, etc.;
   - to identify top risky users, their behavior, and their contribution to the risk score, including the top 1% riskiest users who contributed the most to the risk score;
     - » You may find it useful to run this report periodically to find the top risky users/locations and pivot to the Web insights log or SIEM to do further investigation on them.
8. Run the **Anomaly Detection** report daily:
   - to understand your organization's anomalous user activity summary and threat activity;
   - to spot potential data exfiltration events, malicious insider activity, and suspicious activity;
   - to identify anomalous user behavior, such as correlated file uploads/downloads trends, sanctioned vs.

unsanctioned application usage, impossible travel scenario for login attempts, data leakage attempts, etc.;

- to identify organization-level anomalous activity, such as anomalous upload and dsownload traffic patterns when using cloud applications;
- to identify top users who contributed to these anomalous behaviors compared to peer users within the group who have similar application access and usage patterns;
  - » You may find it useful to run this report periodically to find the top risky users/locations and pivot to Web Insights Log or SIEM to do further investigation on them.

9. Use Custom Reports to see events that you are interested in. Some of the weekly reports that customers are usually interested in include:

   - File Upload Report, which lists the users who have uploaded files in the past week, which sites they have uploaded them to, and what the file names/types were.
   - Executable Download Report, which lists the users that have downloaded an executable or script file in the past week, which sites they downloaded them from, and what the file names/types were.
   - Example: **Interactive Reports > Custom Reports > New Report** > choose **Web** > Add Filter **File Share Activity** > Add Filter **Upload / View / All**, Add more filters, such as users and Add a **Widget**.

10. Run **Sandbox Files Found Malicious Report** weekly to highlight unknown files that were sent to the Sandbox for analysis and found to be malicious.

Security Operations Incident Response Best Practices

1. **Botnet activity detection:**

   - Look for the **Botnet Callback** category in the **Advanced Threats** widget under Security Dashboard and click View Logs.
   - Look for high-confidence content blocks by searching for "IPS block inbound response: botnet command-and-control traffic" or "IPS block outbound request: botnet command-and-control traffic" in the **reason** weblog field or **Policy Action** Insights field.
   - For lower-confidence blocks (reputation-based), you can search for "Reputation block outbound request: botnet site" in the **reason** weblog field or **Policy Action** Insights field. Check out the **policy reason string article**.
   - Configure Botnet Callback alert to receive an email when botnet callback activity is detected.

   Note: Reputation block based on destination IP, domain, or URL is prone to "False Positives" as a given site's reputation changes may be delayed.

2. **Phishing activity detection:**

   - Look for the **Phishing** category in the **Advanced Threats** widget under Security Dashboard and click View Logs.
   - Use **Top Users/Locations for Advanced Threats** widget to see which user is targeted the most with advanced threats, such as phishing.
   - You can also create a custom dashboard widget to view top users who are targeted for phishing by

selecting "User" as "Data Type" and selecting "Phishing" under the "Advanced Threat Super Category" filter.

- From the weblogs, search for "Phishing" or "WebSpam" URL Category in Advanced Threat Protection Logs.
- Look for high-confidence content blocks by searching for "IPS block inbound response: phishing content" in the weblog reason field or Policy Action Insights field.
- Look for a reputation-based block using "Reputation block outbound request: phishing site" in the **reason** weblog field or **Policy Action** Insights field.
- You can also configure an **Alert** for "Phishing" to receive an email when phishing activity is detected and reaches a certain threshold, such as 100 occurrences within five minutes.

3. **Detecting suspicious outbound connections:**

- Create a custom dashboard widget for Network Services under Firewall Overview Dashboard to look for any suspicious service(s) in use, such as SSH.
- Search the firewall logs/insights for unusual "Network Application" or "Network Service" being used, such as SSH.
- From the firewall logs, search for unusual applications/services in the "nwapp" or "nwsvc" fields.
- From the weblogs, search for "Suspicious Destination" URL Category in Advanced Threat Protection logs.

4. **Data exfiltration activity detection:**

- Exfiltration over alternative protocol – look for unusual volume of data exchanged in alternate protocols, such as FTP, SMTP, DNS, SMB, etc.
- Exfiltration over HTTP/S – look for abnormal volumes of data exchanged.
- Look for uncommon data flows, such as "client sends significantly more data than the server," "client maintains long connection and consistently sends fixed size data packets or at regular intervals," etc.
- Look for data transfer over encrypted archives that are suspicious.
- Search the firewall logs/insights for unusual "Network Application" or "Network Service" being used, such as FTP, DNS, SMTP, SMB, etc., for large amount of data transfers/unusual volumes.
- From the weblogs, search for protocols, such as FTP, DNS, SMTP, SMB, etc., and Suspicious Destinations URL Category in Advanced Threat Protection logs.
- Configure DLP policy to block sensitive data exchanged, such as credit card numbers.

5. **Detect potentially unwanted applications in use – Tor, proxy, anonymizer, or peer-to-peer apps**

- Look for the "Peer-to-Peer" or "Unauthorized Communications" category in **Advanced Threats** widget under Security Dashboard and click View Logs.
- Use the **Top Users/Locations for Advanced Threats** widget to see which user is a top threat who uses a peer-to-peer anonymizer application, such as Tor or unauthorized communications.
- You can also create a custom dashboard widget to view Top Users who use peer-to-peer application or unauthorized communication by selecting "User" as "Data Type" and selecting "Peer-to-Peer" or "Unauthorized communication" under "Advanced Threat Super Category" filter.
- From the weblogs, Search for the "Peer-to-Peer" or "Unauthorized Communication" URL Category in

Advanced Threat Protection Logs

- Configure to block Tor traffic under Advanced Threat Protection policy if it is not a sanctioned app to use in your environment.

6. **Detect malicious tunneling activities – IRC tunneling, SSH tunneling, DNS tunneling**

- From the weblog or Insights log, look for high-confidence content blocks by searching for "IPS block inbound response. IRC use/tunneling" or "IPS block outbound request. IRC use/tunneling" or "IPS block: SSH use/tunneling" in the **reason** field in weblog or **Policy Action** field in Insights.
- Look for "DNS Tunnels" Category in **DNS Overview** Dashboards and click View Logs.
- To learn more about DNS Tunnel Detection: **https://help.zscaler.com/zia/about-dns-tunnel-detection**

7. **Detect malicious domain fronting activities:**

- Ensure TLS inspection is enabled for all traffic.
- Add "df_hostname" weblog field to your NSS feed format.
- Search & Compare this field value with the actual "host" field value for any discrepancy.
- Create an alert in the SIEM that runs a case-insensitive comparison between "host" (the HTTP host header) with "df_hostname" (the SNI) and aggregate the result based on the df_hostname to reduce the number of alerts.

  Note: Domain fronting can be used for genuine purposes as well. You should first study the results of the recommended alert and optimize the search to reduce false positives.

8. **Malware activity detection:**

- Start from the **Viruses & Spyware** category in Security Dashboard and click View Logs.
- Use the **Top Users/Locations for Viruses & Spyware** widget to see which user is targeted with the most with malware.
- From the weblog, search for "Malware block: malicious file" in the **reason** weblog field or **Policy Action** in the Insights field.
- Look for a reputation-based content block using "Reputation block outbound request malicious URL" in the **reason** weblog field or **Policy Action** field in Insights.
- Look for user activities and logs around the time block was reported to see if there was any other suspicious activity that may have been successful.

9. **Detect insecure protocols in use:**

- Start from the Firewall Overview Dashboard to see any insecure applications being used that are in the top usage, such as HTTP, FTP, etc.
- Search for insecure/unencrypted protocols in use, such as "FTP, HTTP, IMAP, IRC, Telnet, POP3, etc., under the Network Services filter in Firewall Insights or "nwapp" or "nwsvc" field in the firewall log.
- Run the "Distribution of Traffic by Protocol" report from **Interactive Reports > Standard Reports > Secure Browsing** section periodically to spot threat trends in encrypted vs. unencrypted protocols.

10. **Use the Zscaler Threat Library to drill down on threat names.**

11. **Sandbox activity – unknown files:**
    - Look for "Sent for Analysis" in the "malwarecat" weblog field. Even as a Basic Sandbox customer, we would send a subset of your files for sandbox analysis.
    - To view the verdict, you would need to pivot to the Zscaler "Web Insights" Log View and do a search for the MD5 hash or leverage the **Sandbox Report Dashboard**.
    - You can also use **Sandbox Report API** to get details of the Sandbox-analyzed files using the MD5 hash.
12. **Sandbox activity – found malicious files:**
    - Run **Sandbox Files Found Malicious Report** weekly. To run this report, go to:

      ZIA Admin Portal > Analytics > Choose **Sandbox Files Found Malicious** from **Sandbox Activity Report** drop-down.
    - Use SOAR/IR workflow to scan for the MD5 via EDR for the presence of this malware and who downloaded it previously.
    - **P-0 alert** – set up automatic IR workflows in response to high-fidelity P-0 email alerts (**help article**).
13. **Sandbox activity – known malicious files**
    - Look for "Sandbox Malware" or "Sandbox Adware" or "Sandbox Anonymizer" in the "malwarecat" weblog field. In case a file had been previously sent for analysis (by any Zscaler customer) and was found to be malicious, we will indicate the Sandbox verdict in this weblog field.
    - Files that were sent for analysis and had no known reputation or weren't blocked by one of our AV engines could be considered high risk.
    - You can also extract IOCs from **Sandbox Detail Report API**.
14. Pivot from Threat Insights Globe to your SIEM. Some customers display the Zscaler Threat Insights Globe on a large screen in their SOC. It is refreshed every 24 hours and you may find it useful to get a quick snapshot of the active threats in your environment.
    To learn more: **https://help.zscaler.com/zia/about-threat-insights**
15. Retrospective threat detection – whenever you detect a security block (reputation, AV engine, advanced threat), you may find it useful to look back a few days (or even months!) for the first sightings of the MD5 hash/domain/URL/IP indicator to identify the patient-zero event and how long a threat may have been lingering on your network.
16. Whenever you detect a security block (reputation, AV engine, advanced threat), you may find it useful to look for user traffic activity and logs around the time the block was reported to see if there was any other malicious activity that succeeded.

Zscaler Alerts Subscription Best Practices

1. As a best practice, configure alerts to receive an email for the following high risk security activities:
   - Botnet callback with a threshold
   - Incoming malware/spyware/viruses
   - Phishing with a threshold
   - Sandbox adware, anonymizer, malware with a threshold
   - Suspicious destination
   - Patient-zero alert
2. You can create up to 128 alerts.
3. After the alerts are defined, you can use the "Publish Alerts" to subscribe to alerts and send emails to different recipients based on the alert category and severity.

Conclusion

Zscaler's unique architecture secures customers with comprehensive coverage and extensibility to enable a defense-in-depth approach.

Visibility into user traffic and security activity is key for a SOC team to be able to identify, isolate, and respond to security threats. The Zscaler Nanolog service provides consolidated threat logs from all users, locations, and devices globally into a central repository that is determined by customers in which administrators can view and mine transaction data by user, device, application, and location in real time. Zscaler Nanolog is a very verbose record in a compressed format that includes rich threat context and other useful information for event classification and threat hunting.

These logs power our analytics capabilities, such as Dashboards, Insights, and Reporting to provide visibility into user and threat activity in real time. Zscaler also supports forwarding this log to your on-premises or cloud SIEM in near-real time using NSS (Nanolog Streaming Service), enabling real-time alerting, correlation with the logs of your firewall and other devices, and long-term local log archival.

In addition, the best practices outlined in this article will help you make the best use of the capabilities provided to identify threats and respond to them faster.

Appendix A–Threat Detection Use Cases and Examples

Phishing Attacks

Phishing typically involves the use of spoofed and customized messages that appear to be for genuine business purposes designed to lure users into giving sensitive information. Such messages contain malicious links or attachments. Phishing can be targeted, which is known as spearphishing. With spearphishing, a specific individual, company, or industry will be targeted by the adversary.

MITRE ATT&CK Relevant Tactics, Techniques, and Sub-Techniques

Zscaler Detection Engines

Initial Access >	
Phishing (3) >	Spearphishing Attachment >
	Spearphishing Link >
	Spearphishing via Service >

The Zscaler security logs useful for detecting phishing attacks are:

- Advanced Threat Protection: Phishing websites/Domain/IP detection reputation based
- Sandbox: Unknown File attachments

Investigation

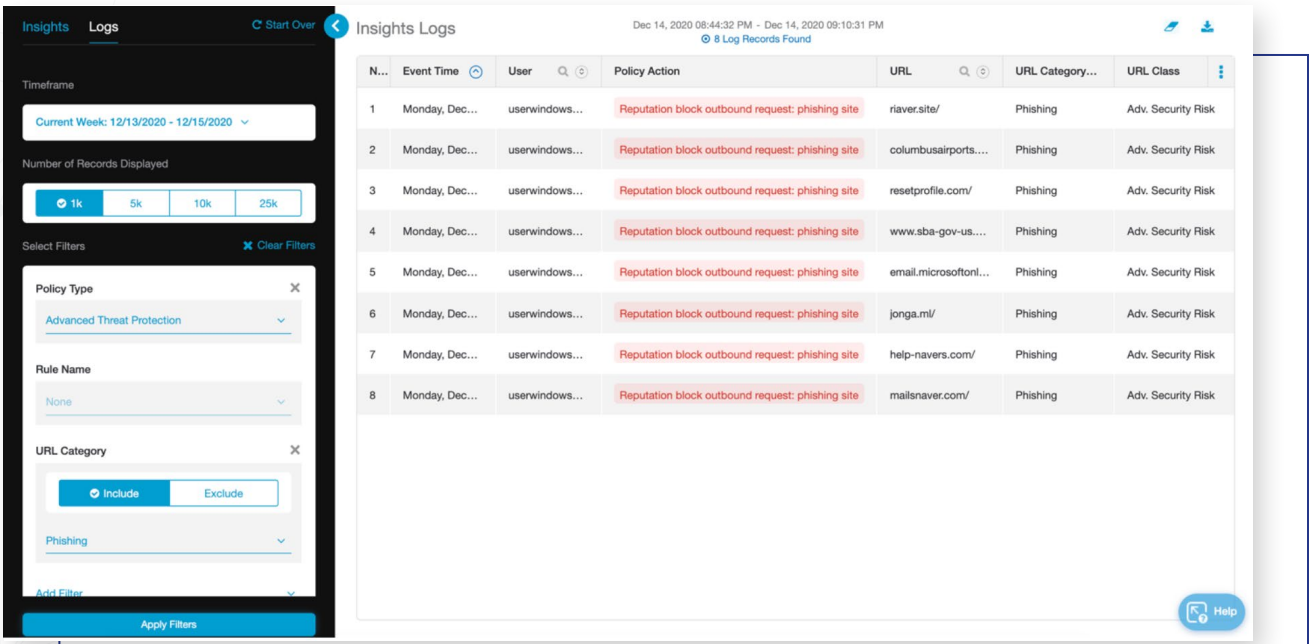
Using Web Insights

The following key fields and search parameters are useful for filtering the Insights log to identify phishing attempts:

Policy Type="Advanced Threat Protection", **URL Category**="WebSpam"
Policy Type="Advanced Threat Protection", **URL Category**="Phishing", **URL Class**="Advanced Security Risk"

Using NSS Weblog

Sample Web Insights Search for Phishing Attempts

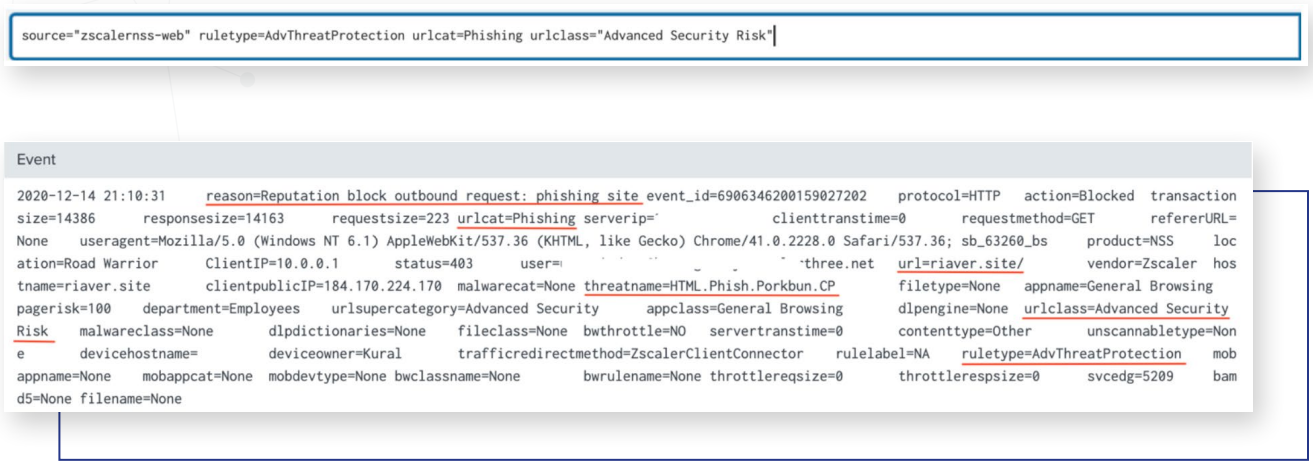


The following key fields and search parameters are useful to dissect the NSS weblog to identify phishing attempts:

ruleType="AdvThreatProtection", **urlCat**="WebSpam"
ruleType="AdvThreatProtection", **urlCat**="Phishing", **urlclass**="Advanced Security Risk"

Prevention/Mitigation Suggestions

Sample NSS Weblog search for Phishing Attempts



Pre-incident:

- Anti-spam filtering
- Regular phishing defense protection checks
- Regular phishing security awareness (based on audit of successful cases and active ones over the net)
- Incident Response Team trained and ready to handle cases (cases, process, users aware of who to join)
- Restrict web traffic to suspicious URL categories and higher Page Risk URLs
- Antivirus/Antimalware

Post-incident:

- Upgrade alert level
- Inform affected/aligned users
- Run antivirus

Preventive Maintenance:

This step includes all actions taken to make successful attacks more difficult, including regularly maintaining and updating existing systems; updating firewall policies; patching vulnerabilities; and whitelisting, blacklisting and securing applications.

Detection of Malware

Botnets and Command-and-Control Traffic

Description

Command and control is a tactic used by adversaries to communicate remotely with the systems under their control within a victim network and may use a multitude of techniques to establish control with various levels of stealth. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.

MITRE ATT&CK Relevant Tactic, Techniques and Sub-techniques

Command and Control >	
Application Layer Protocol (4) >	Web Protocols >
	File Transfer Protocols >
	Mail Protocols >
	DNS >
Communication Through Removable Media >	
Data Encoding (2) >	Standard Encoding >
	Non-Standard Encoding >
Data Obfuscation (3) >	Junk Data >
	Steganography >
	Protocol Impersonation >
Dynamic Resolution (3) >	Domain Generation Algorithms >
	Fast Flux DNS >
	DNS Calculation >
Encrypted Channel (2) >	Symmetric Cryptography >
	Asymmetric Cryptography >
Fallback Channels >	
Ingress Tool Transfer >	
Multi-Stage Channels >	
Non-Application Layer Protocol >	
Non-Standard Port >	
Protocol Tunneling >	

Proxy (4) >	Internal Proxy >
	External Proxy >
	Multi-hop Proxy >
	Domain Fronting >
Remote Access Software >	
Traffic Signaling (1) >	Port Knocking >
Web Service (3) >	Dead Drop Resolver >
	Bidirectional Communication >
	One-Way Communication >

Zscaler Detection Engines

The Zscaler security logs that are useful for detecting command-and-control traffic are:

- Advanced Threat Protection: Botnet/Command-and-control traffic/Reputation block
- Sandbox: Unknown file attachments

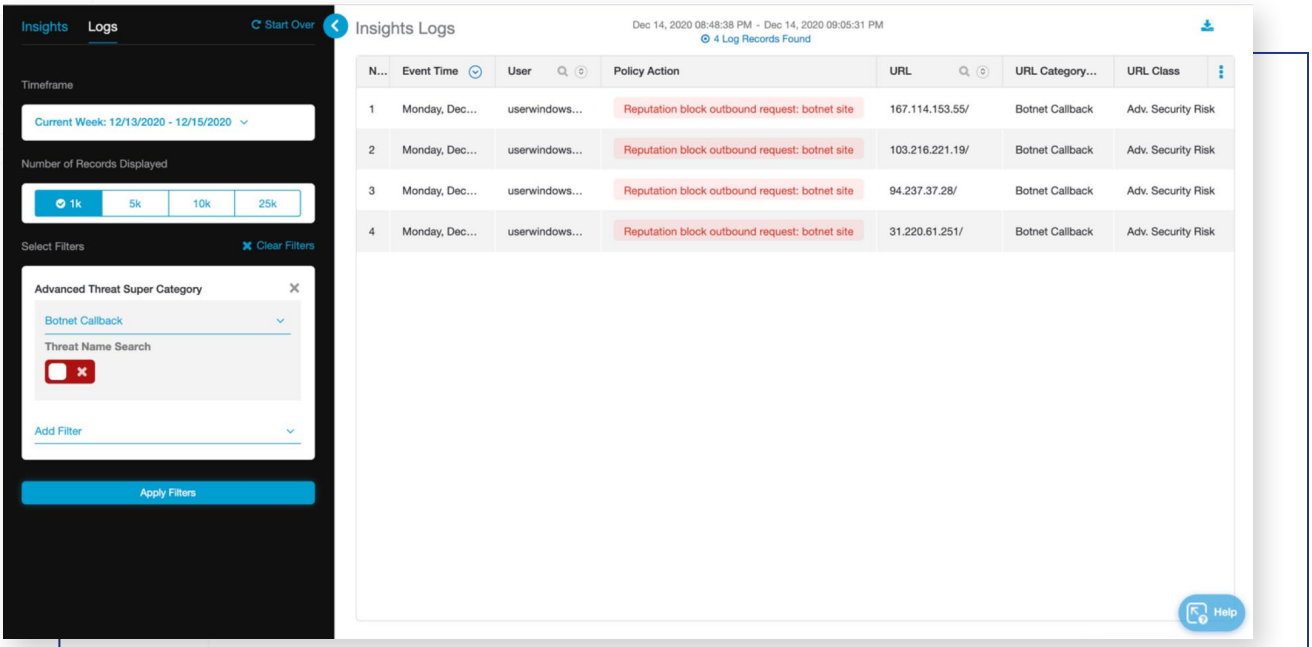
Investigation

Using Web Insights

The following key fields and search parameters are useful for filtering the Insights log to identify botnets/command-and-control traffic:

Advanced Super Threat Category= “Botnet Callback”
Policy Type="Advanced Threat Protection", **URL Category**="Botnet Callback"

Sample Web Insights Search for Botnet/Command and Control Traffic



Using NSS Weblog

The following key fields and search parameters are useful to dissect the NSS weblog to identify botnets/ command-and-control traffic:

ruleType="AdvThreatProtection", **urlCat**="Botnets"
ruleType="AdvThreatProtection", **urlCat**="Botnets", **urlclass**="Advanced Security Risk"
reason="IPS block outbound request: botnet command and control traffic"
reason="Reputation block outbound request: botnet site"

Sample NSS Weblog search for Botnet/Command and Control Traffic

```
source="zscalernss-web" ruletype=AdvThreatProtection urlcat=Botnets urlclass="Advanced Security Risk"
```

Event

```
2020-12-14 21:05:31 reason=Reputation block outbound request: botnet site event_id=6906344911668838402 protocol=HTTP action=Blocked transaction
size=14392 responsesize=14167 requestsize=225 urlcat=Botnets serverip= clienttranstime=0 requestmethod=GET refererURL=
None useragent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36; sb_63199_bs product=NSS loc
ation=Road Warrior ClientIP=10.0.0.1 status=403 user= net url=31.220.61.251/ vendor=Zscaler hos
tname=31.220.61.251 clientpublicIP=184.170.224.170 malwarecat=None threatname=Win32.Backdoor.Drovorub.LZ filetype=None appname=General Browsing
pagerisk=100 department=Employees urlsupercategory=Advanced Security appclass=General Browsing dlpengine=None urlclass=Advanced Security
Risk malwareclass=None dlpdictionaries=None fileclass=None bwthrottle=NO servertranstime=0 contenttype=Other unscannabletype=Non
e devicehostname= deviceowner= trafficredirectmethod=ZscalerClientConnector rulelabel=NA ruletype=AdvThreatProtection mob
appname=None mobappcat=None mobdevtype=None bwclassname=None bwrulename=None throttlereqsize=0 throttlerespsize=0 svcedg=5209 bam
d5=None filename=None
```

Prevention/Mitigation Suggestions

Pre-incident:

- Keep antivirus software up to date
- Keep operating system and patches up to date
- Educate users not to click on suspicious links or download attachments from unknown sources
- Scan the network to flag any abnormalities or suspicious activities

Post-incident:

- Investigate (find the infection vector and check if some other asset might be compromised)
- Antivirus scan
- Rebuild machine

Malware Trojan/RAT/Password Stealer/Worm

Description

A trojan is a type of malicious code or software that looks legitimate but can take control of your computer.

Zscaler Detection Engines

The various Zscaler detection engines useful for detecting malware trojan/RAT/password stealer/worm are:

- Malware Protection (reputation, AV, Yara)
- Advanced Threat Protection (reputation, IPS)

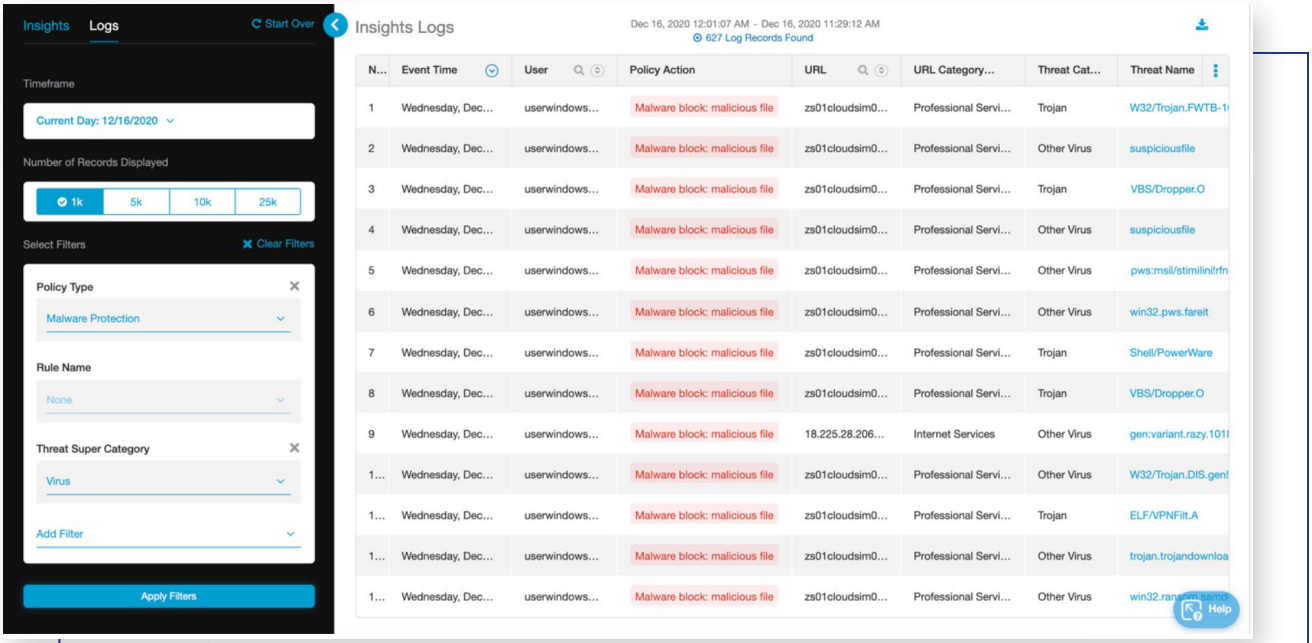
Investigation

Using Web Insights

The following key fields and search parameters are useful for filtering the Insights log to identify malware/trojan/RAT/Password Stealer/Worm attempts:

Policy Type="Advanced Threat Protection", “Malware Protection”
Threat Super Category="Virus"
Threat Category=”Macro Virus," “Malware Tool,” “Password Stealer,” “Trojan,” “Worm,” “Unrecognized Virus,” “Other Virus,” “Other Malware,” “Boot Virus”

Sample Web Insights Search for Malware Trojan

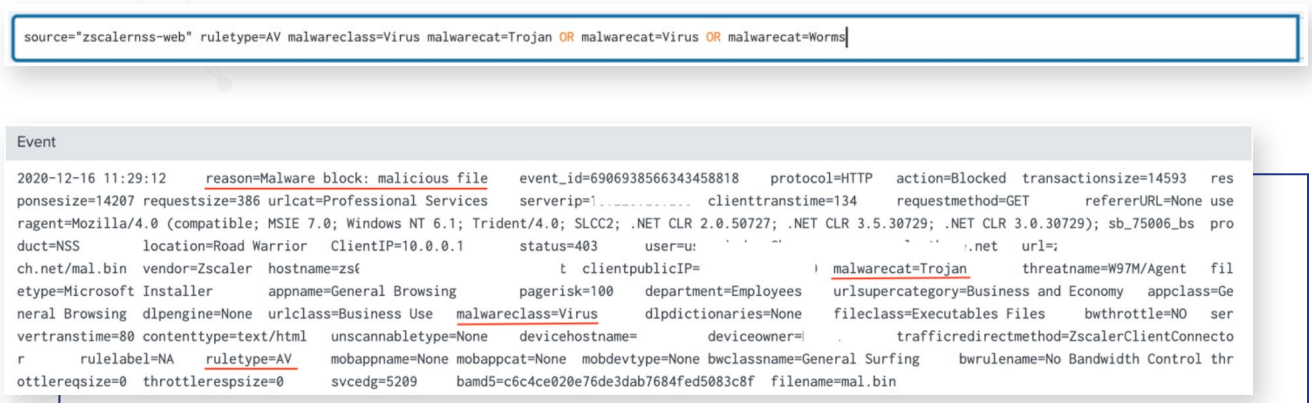


Using NSS Weblog

The following key fields and search parameters are useful to dissect the NSS weblog to identify malware/trojan/RAT/password stealer/worm attempts:

ruleType="AV" **malwareclass**="Virus"
malwarecat="Trojan." "Macro Virus," "Malware Tool," "Password Stealer," "Worms," "Unrecognized Virus"
reason="Malware block:malicious file"
urlclass="Advanced Security Risk"
urlcat="Malicious URLs", "Suspected Spyware or Adware"
urlclass="Advanced Security Risk"

Sample NSS Weblog search for Malware Trojan



Prevention/Mitigation Suggestions

Pre-incident:

- Keep your antivirus up to date
- Keep your operating system and patches up to date
- Don't download or install software from a source you don't trust completely

Post-incident:

- Investigate (find the infection vector and check if some other asset might be compromised)
- Antivirus scan
- Rebuild machine

Advanced Persistent Threat

Malware Ransomware

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to systems and network resources. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible.

Zscaler Detection Engines

The Zscaler detection engine useful for detecting malware ransomware is:

- **Malware Protection** (reputation, AV, Yara)

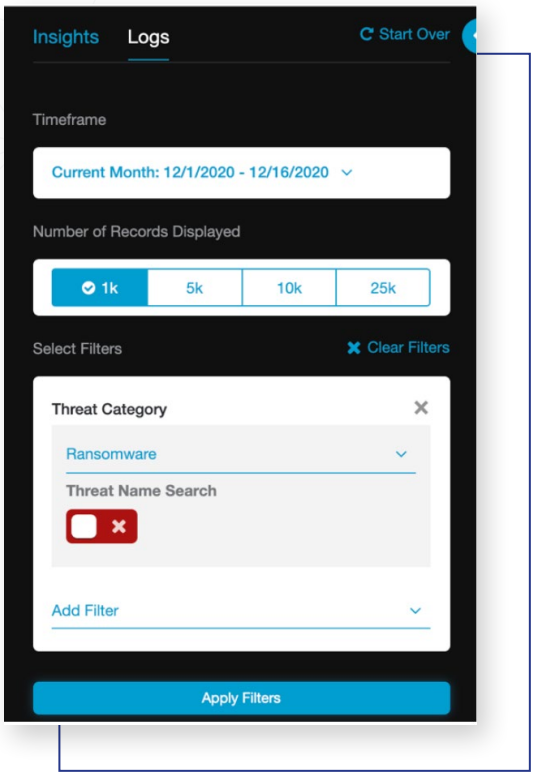
Investigation

Using Web Insights

The following key fields and search parameters are useful for filtering the Insights log to identify ransomware attempts:

Threat Category=" Ransomware"

Sample Web Insights Search for Ransomware



Using NSS Weblog

The following key fields and search parameters are useful for dissecting the NSS weblog to identify cryptomining attempts:

ruleType="AV", **malwareclass**="Virus", **malwarecat**= "Ransomware", **reason**="Malware block:malicious file"

Sample NSS Weblog search query for Cryptomining

```
"ruletype=advthreatprotection" "urlclass=Advanced Security Risk" urlcat=cryptomining
```

Prevention/Mitigation Suggestions

Pre-incident:

- Keep your antivirus up to date
- Keep your operating system and patches up to date
- Don't download or install software from a source you don't trust completely

Post-incident:

- Investigate (find the infection vector and check if some other asset might be compromised)
- Antivirus scan
- Immediately secure backup data or systems by taking them offline
- Contact law enforcement

Insider Threat

Track malicious activity, such as cryptomining, that uses corporate resources.

Cryptomining Malware

Description

Cryptomining malware refers to a malware program that is developed to take over a computer's resources and use them for mining cryptocurrency without a user's explicit permission.

Zscaler Detection Engines

The Zscaler detection engine useful for detecting cryptomining is:

- Advanced Threat Protection (IPS)
- Sandbox

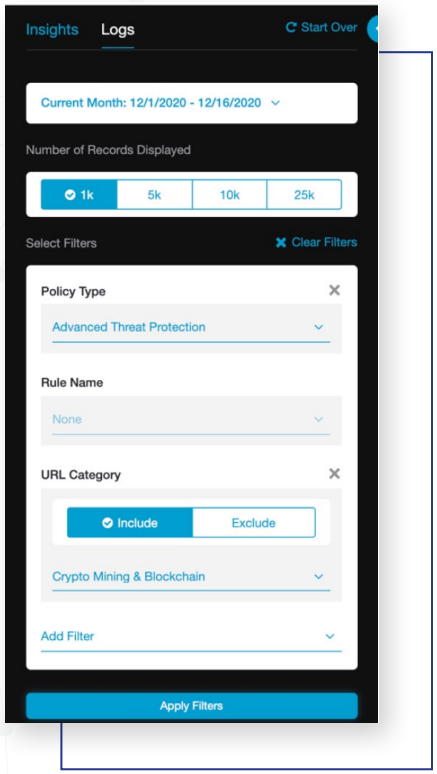
Investigation

Using Web Insights

The following key fields and search parameters are useful for filtering the Insights log to identify cryptomining attempts:

Policy Type="Advanced Threat Protection"
URL Category= "Crypto Mining & Blockchain"

Sample Web Insights Search for Cryptomining



Using NSS Weblog

The following key fields and search parameters are useful for dissecting the NSS weblog to identify cryptomining attempts:

The following parameters are useful for dissecting security logs:

ruleType="AdvThreatProtection", **urlCat**="Cryptomining", **urlclass**="Advanced Security Risk", **reason**="IPS block"

Sample NSS Weblog search query for Cryptomining

```
"ruletype=advthreatprotection" "urlclass=Advanced Security Risk" urlcat=cryptomining
```

Prevention/Mitigation Suggestions

Pre-incident:

- Monitor the network for suspicious activity
- Incorporate cryptomining threat into your security awareness training
- Install anti-cryptomining extension on web browsers

Post-incident:

- Investigate (find the infection vector and check if some other asset might be compromised)
- Antivirus scan
- Rebuild machine

Threat Detection using Advanced Cloud Sandbox

Detecting Unknown Malware

Description

Most security solutions rely on some form of signature to detect malicious traffic. Sandboxing uses dynamic analysis to monitor file behavior in an isolated environment to protect users from zero-day threats. Zscaler Cloud Sandbox uses advanced behavioral analysis techniques to find and block unknown malware threats. 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.

Zscaler Detection Engines

The Zscaler detection engine useful for detecting unknown and potential zero-day malware is:

- Sandbox

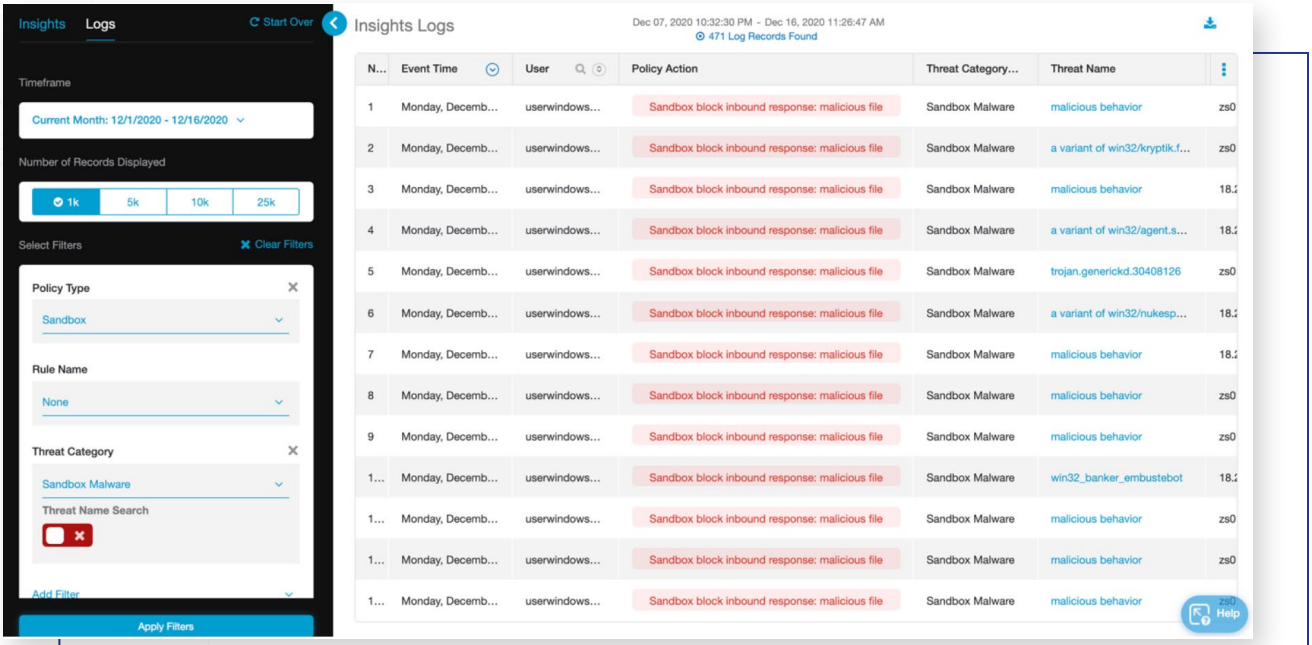
Investigation

Using Web Insights

The following key fields and search parameters are useful for filtering the Insights log to identify unknown files sent to sandbox:

Policy Type="Sandbox"
Threat Category= "Sent for Analysis," "Sandbox Adware," "Sandbox Anonymizer," "Sandbox Malware"

Sample Web Insights Search for Sandbox Malware



Using NSS Weblog

The following key fields and search parameters are useful for dissecting the NSS weblog to identify unknown files sent to the sandbox:

ruleType="BA"
malwarecat="Sent for Analysis," "Sandbox Malware," "Sandbox Adware," Sandbox Anonymizer"
reason="Allowed - No Active Content,' "Quarantined," "Sandbox block inbound response: malicious file," "Allowed and No Scan"

If your organization has Advanced Cloud Sandbox and an API license, you can get a Sandbox Detail Report based on the MD5 parameter that you retrieve from your logs in the SIEM. If MD5 is not included in the log, you can add the key field "bamd5" to your NSS feed to retrieve it from the weblog. You can use the Cloud Sandbox API to retrieve a fully detailed report for the MD5 hash. Please refer to the API reference link below for syntax on how to retrieve this report.

https://help.zscaler.com/zia/api

Sample NSS Weblog search to find Unknown files sent to Sandbox

```
source="zscalernss-web" ruletype=BA "malwarecat=Sandbox Malware" OR "malwarecat=Sandbox Adware" OR "malwarecat=Sent for Analysis" OR "malwarecat=Sandbox Anonymizer"
```

Event

```
2020-12-16 11:26:47     reason=Sandbox block inbound response: malicious file   event_id=6906937943573200897    protocol=HTTP   action=Blocked  transaction
size=14410      responsesize=14228      requestsize=182 urlcat=Professional Services    serverip=               clienttranstime=83      requestmethod=GET
refererURL=None useragent=python-requests/2.22.0; sb_74966_bs   product=NSS     location=Road Warrior   ClientIP=10.0.0.1       status=403      user=userwi
ndo                     three.net       url=z                                   skqlqx      vendor=Zscaler  hostname=z                              :  clientpubli
cIP=                    malwarecat=Sandbox Malware      threatname=win32_trojan_badcall filetype=Windows Executables    appname=General Browsing        pag
erisk=100       department=Employees    urlsupercategory=Business and Economy   appclass=General Browsing       dlpengine=None  urlclass=Business Use   mal
wareclass=Behavior Analysis     dlpdictionaries=None    fileclass=Executables Files     bwthrottle=NO   servertranstime=81      contenttype=Other       uns
cannabletype=None       devicehostname=         deviceowner=            trafficredirectmethod=ZscalerClientConnector    rulelabel=BA_3  ruletype=BA     mob
appname=None    mobappcat=None  mobdevtype=None bwclassname=General Surfing     bwrulename=No Bandwidth Control throttlereqsize=0       throttlerespsize=0
svcedg=5209     bamd5=c6f78ad187c365d117cacbee140f6230  filename=None
```

Prevention/Mitigation Suggestions

Pre-incident:

- Implement patch management
- Use a Host Intrusion Protection System (HIPS)
- Use only essential applications

Post-incident:

- Investigate
- Contain – host-level and network-level
- Preserve volatile data

Appendix B–Zscaler Integrations with Third-Party Security Intelligence and Automation Tools

Zscaler's Technology Partner Program advances customers' objectives for greater security and cloud agility by streamlining integration with leading technology solutions. Zscaler integrates with the following security operations technology partners to enable efficient and effective risk and compliance management with information enrichment and automation.

Security Information and Event Management (SIEM) and Analytics

By using NSS, Zscaler customers can send weblog data to their SIEM system to facilitate log correlation from multiple sources, thus allowing organizations to analyze traffic patterns across their entire networks. Additionally, organizations can leverage weblog data in the SIEM to conduct extended historical analyses (> 6 months). Zscaler customers can also ensure compliance with regulatory mandates through local log archival.

Zscaler integrates with a number of SIEM partners for a seamless integration.
https://www.zscaler.com/partners/technology/siem-analytics

- **AT&T AlienVault - https://www.zscaler.com/press/alienvault-and-zscaler-announce-partnership-provide-customers-increased-security-visibility-and-control**
- **BT - https://www.zscaler.com/resources/solution-briefs/partner-bt-assure.pdf**
- Exabeam
- Expel
- **Gigamon - https://www.zscaler.com/resources/solution-briefs/partner-gigamon-threat-insight.pdf**
- JASK
- LogRhythm
- **IBM Security - https://www.zscaler.com/resources/solution-briefs/partner-qradar.pdf**
- **SecBI - https://www.zscaler.com/resources/solution-briefs/partner-secbi.pdf**
- **Splunk - https://www.zscaler.com/resources/solution-briefs/partner-splunk.pdf**
- **Sumo Logic - https://www.zscaler.com/resources/solution-briefs/partner-sumo-logic.pdf**
- **WitFoo - https://www.zscaler.com/resources/solution-briefs/partner-witfoo.pdf**

Security Orchestration, Automation and Response (SOAR)

Zscaler supports integrations with leading SOAR platforms, which help SOC teams enforce and automate event lookups, reputation checks and blocking actions with Zscaler. By delivering a streamlined SOAR and Zscaler workflow, security teams can ensure real-time enforcement of updated policies and better protection of users, on- or off-network.

Zscaler integrates with a number of SOAR partners for a seamless integration.
https://www.zscaler.com/partners/technology/soar

- **D3Security - https://www.zscaler.com/resources/solution-briefs/partner-d3security.pdf**
- **Demisto - https://www.zscaler.com/resources/solution-briefs/partner-demisto.pdf**

- Exabeam
- **LogicHub - https://www.zscaler.com/resources/solution-briefs/partner-logichub.pdf**
- **SecBI - https://www.zscaler.com/resources/solution-briefs/partner-secbi.pdf**
- **Siemplify - https://www.zscaler.com/resources/solution-briefs/partner-siemplify.pdf**
- **Splunk Phantom - https://www.zscaler.com/resources/solution-briefs/partner-splunk.pdf**
- **Swimlane - https://www.zscaler.com/resources/solution-briefs/partner-swimlane.pdf**

Threat Intelligence Platforms (TIPs)

The Zscaler ThreatLabZ research team analyzes a number of leading threat intel feeds alongside the 150B+ transactions and 100M+ blocked attacks that occur every day in the Zscaler cloud in order to continually update detections and product features for the benefit of all Zscaler customers.

Additionally, Zscaler integrates with leading TIPs to ensure SOC teams can easily operationalize the threats that matter within their Zscaler installation. Zscaler automatically consumes user-defined IOCs from TIPs to help enforce real-time policies and ensure all branch offices, and all users on- or off network, get complete protection from emerging threats and targeted attacks.

Zscaler integrates with the below TIP partners for a seamless integration:
https://www.zscaler.com/partners/technology/threat-intelligence-platform

- **Anomali - https://www.zscaler.com/resources/solution-briefs/partner-anomali.pdf**
- **Intsights - https://www.zscaler.com/resources/solution-briefs/partner-intsights.pdf**
- **Recorded Future - https://www.zscaler.com/resources/solution-briefs/partner-recorded-future-integration-deployment-guide.pdf**
- **SecLytics - https://www.zscaler.com/resources/solution-briefs/partner-seclytics.pdf**

CASB

The Zscaler Cloud Security Platform provides full inline CASB functionality to protect all users, on- or off-network, and gives you real-time visibility into all incoming and outgoing traffic along with granular controls. In addition to Zscaler's own out-of-band visibility and control capabilities for SaaS applications, Zscaler has partnered with select CASB vendors to help joint customers perform risk assessments and enforce application control on their cloud services and shadow IT.

Zscaler integrates with the below CASB partners for a seamless integration:
https://www.zscaler.com/partners/technology/cloud-access-security-broker

- **Bitglass - https://www.zscaler.com/resources/solution-briefs/partner-bitglass-casb.pdf**
- **Microsoft - https://www.zscaler.com/resources/solution-briefs/partner-microsoft-cloud-app-security.pdf**
- **McAfee - https://www.zscaler.com/resources/solution-briefs/partner-mcafee-mvision-deployment-guide.pdf**
- **Proofpoint - https://www.zscaler.com/resources/solution-briefs/proofpoint-deployment-guide.pdf**

Firewall

Enterprises rely on multivendor firewall management tools to ensure that all firewalls in the environment consistently enforce corporate policies to manage risk. Leading firewall management partners integrate with Zscaler through APIs to review rules and track changes for compliance audit and access analysis.

Zscaler integrates with the below firewall partners for a seamless integration:
https://www.zscaler.com/partners/technology/firewall-policy-management

- **Firemon - https://www.zscaler.com/resources/solution-briefs/partner-firemon.pdf**
- **Skybox Security - https://www.zscaler.com/resources/solution-briefs/partner-skybox-security.pdf**

Endpoint (EDR)

Zscaler enables endpoint-to-cloud security through integrations with leading Endpoint Protection Platforms (EPPs) and Endpoint Detection and Response (EDR) solutions. With these integrations, Zscaler can control connectivity to corporate assets by validating the endpoint's security posture and isolating infected devices via API integrations to prevent lateral movement of threats. Zscaler shares and receives threat intelligence from EPP/EDR clouds to deliver endpoint reporting to enterprise customers.

Zscaler integrates with the below endpoint protection partners for a seamless integration:
https://www.zscaler.com/partners/technology/endpoint-security

- VMware Carbon Black
- CrowdStrike
- SentinelOne

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com