Zscaler Security Analytics for SOC

SOC Goals and Key Processes: Covers real-time event monitoring, threat assessment, incident response, and vulnerability management.

1. **Best Practices for Security Policy**: Guidelines on configuring malware protection, advanced threat protection, DLP, firewall, IPS control, and URL filtering policies.
2. **Security Log Analysis**: Detailed explanation of using dashboards, insights, and logs for analyzing threat data.
3. **Zscaler Nanolog Streaming Service (NSS)**: Insights on log forwarding and configuration for seamless SIEM integration.
4. **Threat Detection Use Cases**: Includes phishing, malware, insider threats, and advanced persistent threat (APT) detection.
5. **MITRE ATT&CK Framework Alignment**: How Zscaler integrates with ATT&CK to enhance threat analysis.

This document is structured as a technical whitepaper, ideal for students looking to enhance their knowledge of SOC workflows, Zscaler's security tools, and logging strategies. If you need a curated section or a simplified presentation for your students, let me know, and I can extract or adapt specific content for your needs.

4o with canvas

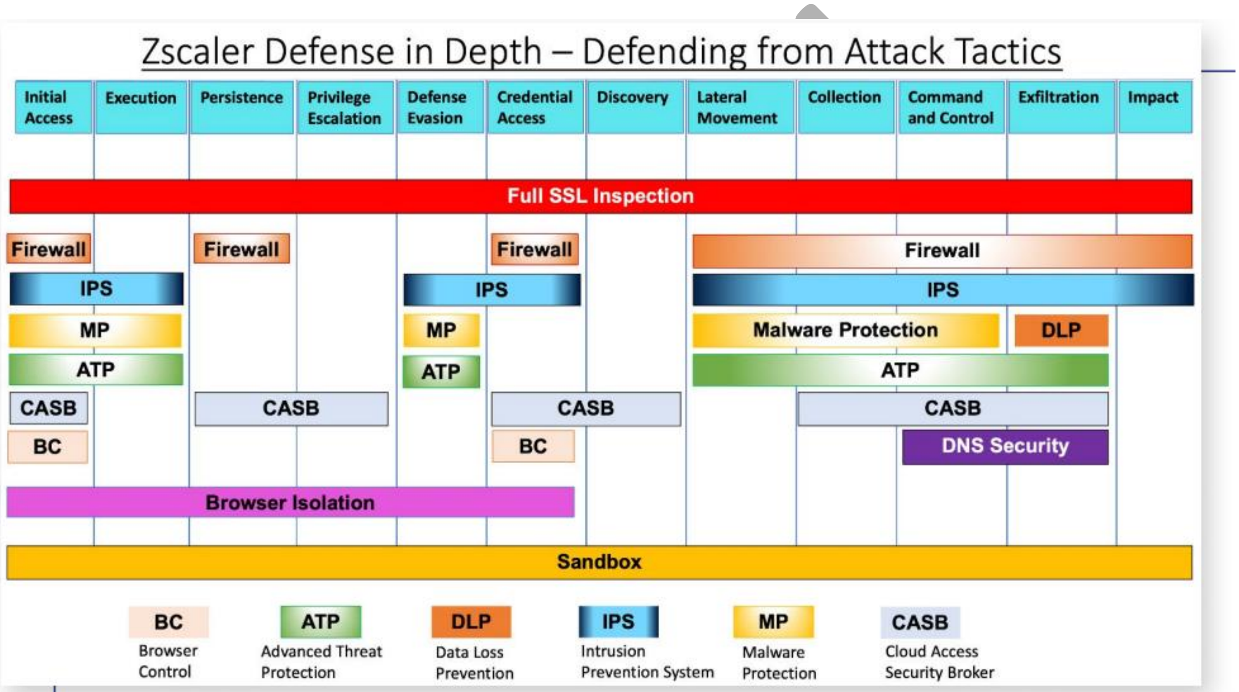
Here's a detailed breakdown of key sections from the uploaded Zscaler document that would be particularly valuable for your students. Each section focuses on foundational concepts, technical insights, and actionable best practices.

---

1. Overview of Security Operations (SOC Goals and Processes)

- **Real-time Event Monitoring, Classification, and Triage**:
  - Logs and analytics are used to detect signals of threats amid routine data.
  - Zscaler Internet Access (ZIA) generates real-time logs for monitoring via dashboards and exports them to SIEM systems.
- **Threat Assessment, Prioritization, and Analysis**:
  - Events are assessed based on threat intelligence (e.g., Zscaler ThreatLabZ, Microsoft Active Protections Program).
  - Analysts prioritize events with indicators of compromise (IoCs) and take steps based on the threat's potential impact.

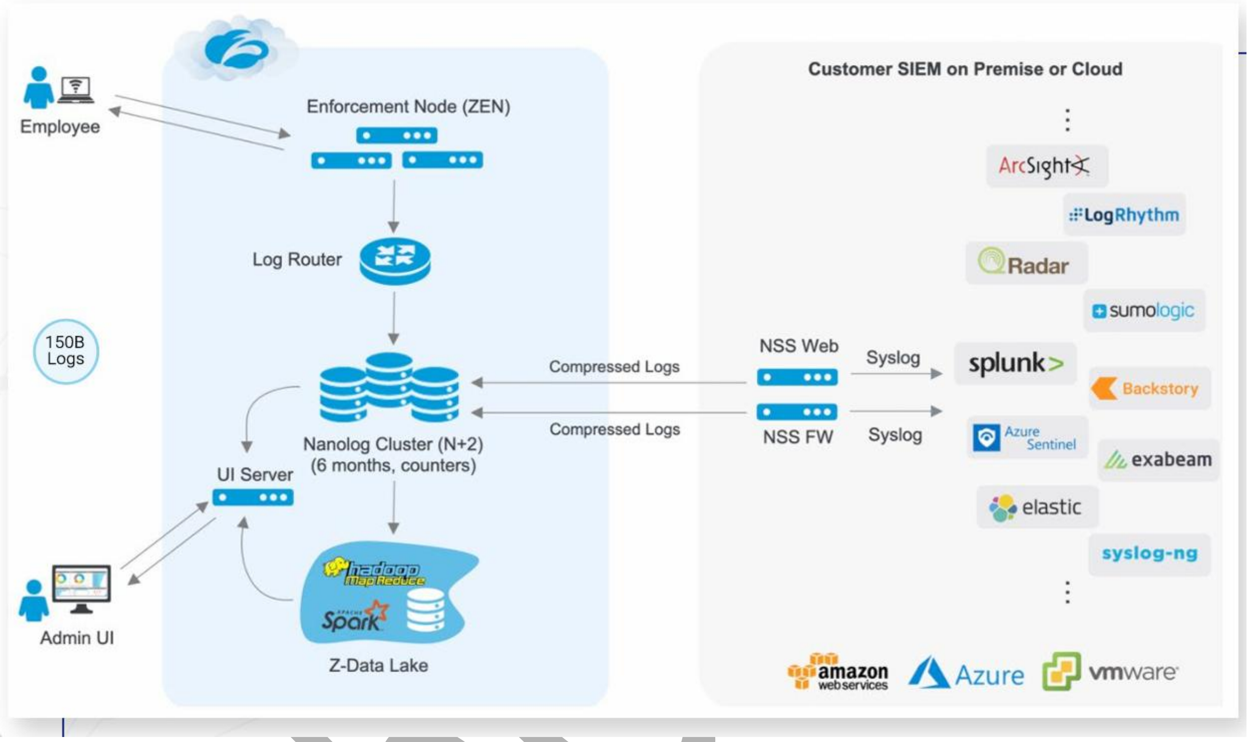
- **Incident Response, Remediation, and Recovery**:
  - Rapid detection and response to incidents help contain damage.
  - Zscaler's remediation tools include asset discovery and policy deployment capabilities to isolate impacted users or locations.
- **Vulnerability Assessment and Compliance**:
  - Zscaler enables automated audits and compliance checks through dashboards and detailed reporting.



2. Zscaler Nanolog and Analytics

- **Nanolog Streaming Service (NSS)**:
  - Centralized storage of logs across devices and locations, providing a rich source for analytics and threat hunting.
  - Logs include fields like risk score, threat type, action taken, and more.
  - Logs can be forwarded to SIEM in compressed formats for near-real-time analysis.
- **Dashboards and Reporting**:
  - Predefined dashboards for various use cases like security threats, firewall traffic, and DNS requests.

- Customizable widgets help track metrics such as phishing attempts, malware activities, and advanced threat events.



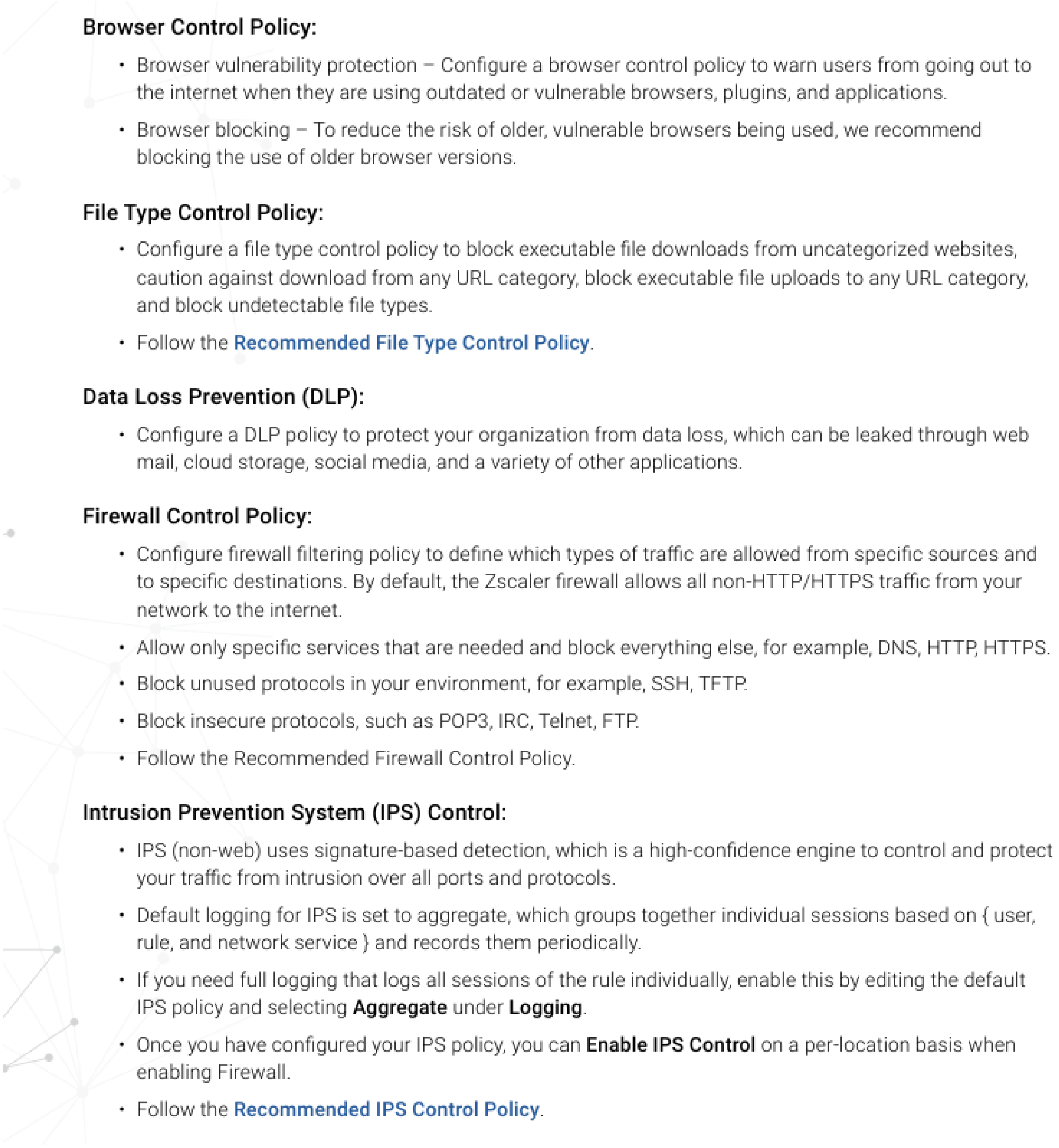
---

3. Security Policy Best Practices

- **Malware Protection**:
  - Enable inbound and outbound inspection.
  - Block password-protected and unscannable files.
- **Advanced Threat Protection (ATP)**:
  - Configure ATP to detect botnet activity, phishing, and malicious scripts.
  - Recommended page risk index threshold: 35 (modifiable based on organizational tolerance).
- **File Type Control**:
  - Block unauthorized executable downloads/uploads.
  - Enforce file type-specific policies for common vectors like Office documents or archives.
- **Data Loss Prevention (DLP)**:

  - Protect against leaks through cloud storage, email, or webmail by defining sensitive data policies.

- **SSL Inspection**:
  - Decrypt and inspect SSL traffic for hidden threats.
  - Create exceptions for compliance-critical or certificate-pinning URLs.



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**.

4. Threat Detection and Response Examples

- **Phishing Detection**:
  - Analyze logs for phishing URL categories and reputation-based blocks.
  - Configure alerts to notify teams of phishing spikes.
- **Malware Analysis**:
  - Logs include fields like malware class, category, and threat name for targeted analysis.
  - Use Sandbox policies to analyze unknown files.
- **Advanced Persistent Threats (APT)**:
  - Utilize logs to detect coordinated attack patterns over time.
  - Leverage Zscaler integrations with third-party tools for deep threat correlation.
- **Data Exfiltration**:
  - Detect abnormal data flows using tools like Insights and DLP.
  - Investigate large data uploads or usage of alternative protocols (FTP, DNS, etc.).

---

5. Integrating Zscaler with Other Tools

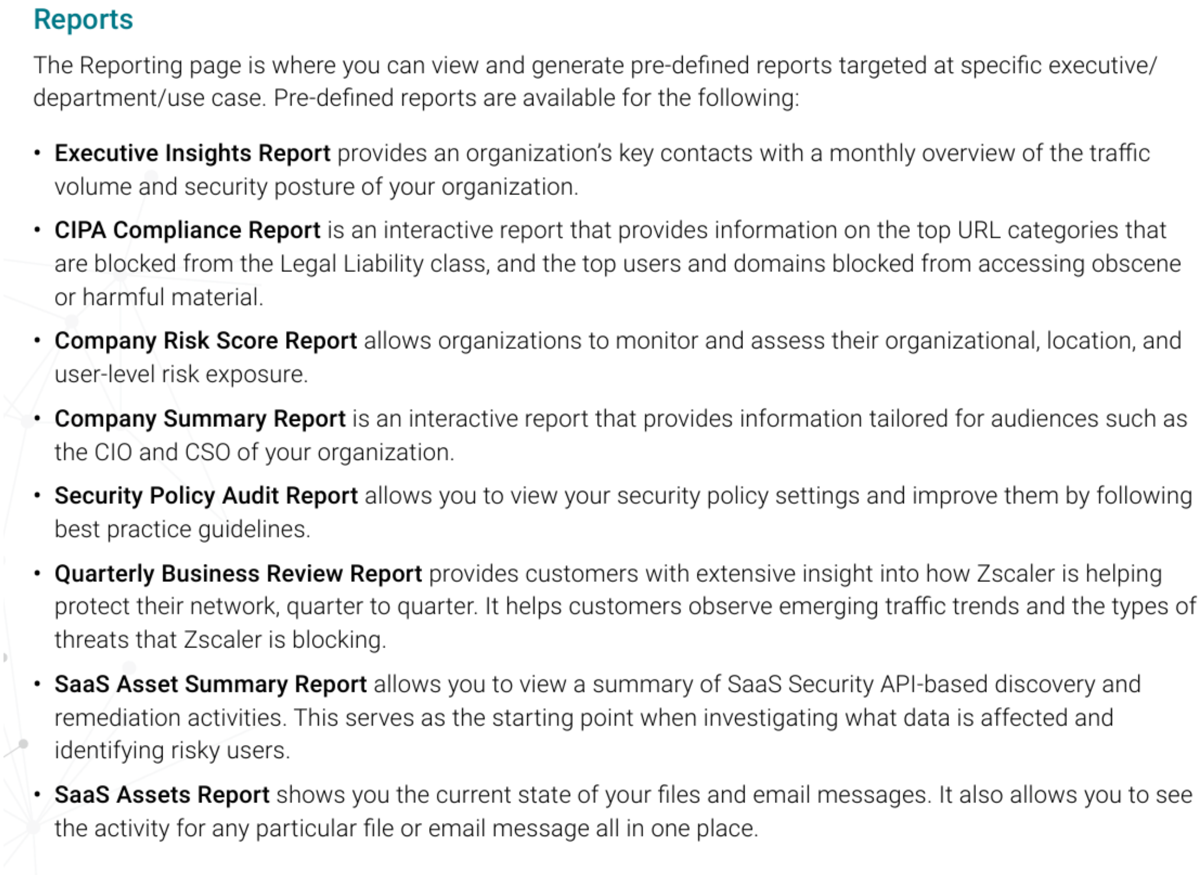
- **SIEM and SOAR Integration**:
  - NSS allows seamless log forwarding to on-premises or cloud-based SIEMs.
  - Leverage APIs for automated workflows, such as triggering alerts or isolating users after detecting suspicious activities.
- **Cloud Access Security Broker (CASB)**:
  - Control data in SaaS applications by monitoring traffic and enforcing access policies.

---

6. Advanced Reporting

- **Reports for Risk Assessment**:
  - **Company Risk Score Reports**: Identify the riskiest users or locations and assess trends over time.
  - **Anomaly Detection**: Spot unusual user activities, such as excessive file uploads or suspicious logins.
- **Custom Reporting**:

    - Generate tailored reports for specific use cases (e.g., file uploads/downloads, threat trends).



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.

---

7. Use Cases and Threat Scenarios

- **Phishing Attacks**:
    - Identify phishing campaigns through URL categorization and advanced filters.
    - Train students on how Zscaler's tools automate phishing detection.
- **Insider Threats**:
    - Use Zscaler dashboards to monitor anomalous behavior, such as unauthorized data access or file transfers.
- **Malware and Zero-Day Detection**:
    - Configure Sandbox policies to analyze and quarantine unknown files.
    - Extract IoCs (Indicators of Compromise) for retrospective analysis of patient-zero events.

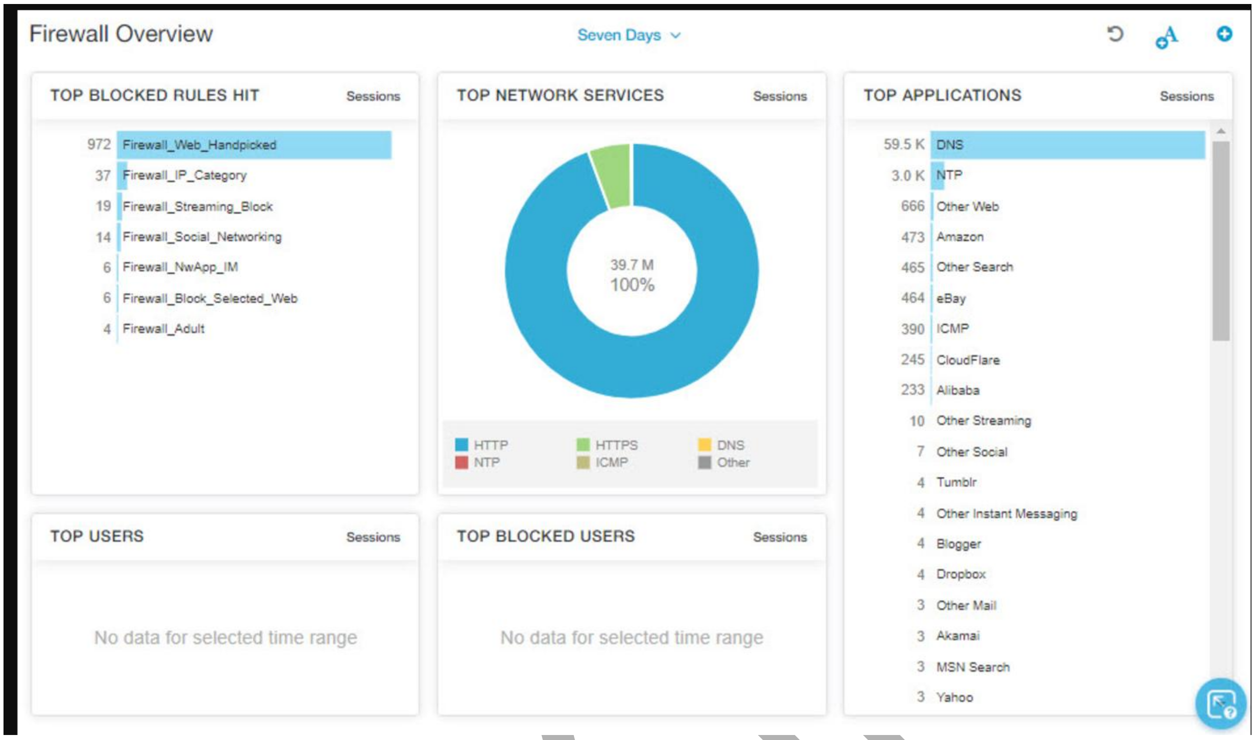
---

1. Log Analysis

Objective: Use Zscaler dashboards and Insights to identify and analyze specific threat types such as botnets and malware.

Steps:

1. **Access Zscaler Dashboards:**
   - **Log in to the Zscaler Admin Portal.**
   - **Navigate to the Security Dashboard or Advanced Threats Dashboard.**
2. **Identify Botnets:**
   - **Look for the "Botnet Callback" category in the Advanced Threat widget.**
   - **Click "View Logs" to investigate events.**
   - **Use filters such as Reason: Botnet Callback and URL Category: Botnet to narrow results.**
3. **Analyze Malware Logs:**
   - **Use the "Malware" filter in Web Insights.**
   - **Search for fields like malwareclass, malwarecat, and reason to identify blocked malicious files.**
4. **Take Notes:**
   - **Record observations such as threat source, destination, and risk score.**



Firewall Overview

Seven Days

TOP BLOCKED RULES HIT

Sessions	
972	Firewall_Web_Handpicked
37	Firewall_IP_Category
19	Firewall_Streaming_Block
14	Firewall_Social_Networking
6	Firewall_NwApp_IM
6	Firewall_Block_Selected_Web
4	Firewall_Adult

TOP NETWORK SERVICES

Sessions

TOP APPLICATIONS

Sessions	
59.5 K	DNS
3.0 K	NTP
666	Other Web
473	Amazon
465	Other Search
464	eBay
390	ICMP
245	CloudFlare
233	Alibaba
10	Other Streaming
7	Other Social
4	Tumblr
4	Other Instant Messaging
4	Blogger
4	Dropbox
3	Other Mail
3	Akamai
3	MSN Search
3	Yahoo

TOP USERS

Sessions

No data for selected time range

TOP BLOCKED USERS

Sessions

No data for selected time range

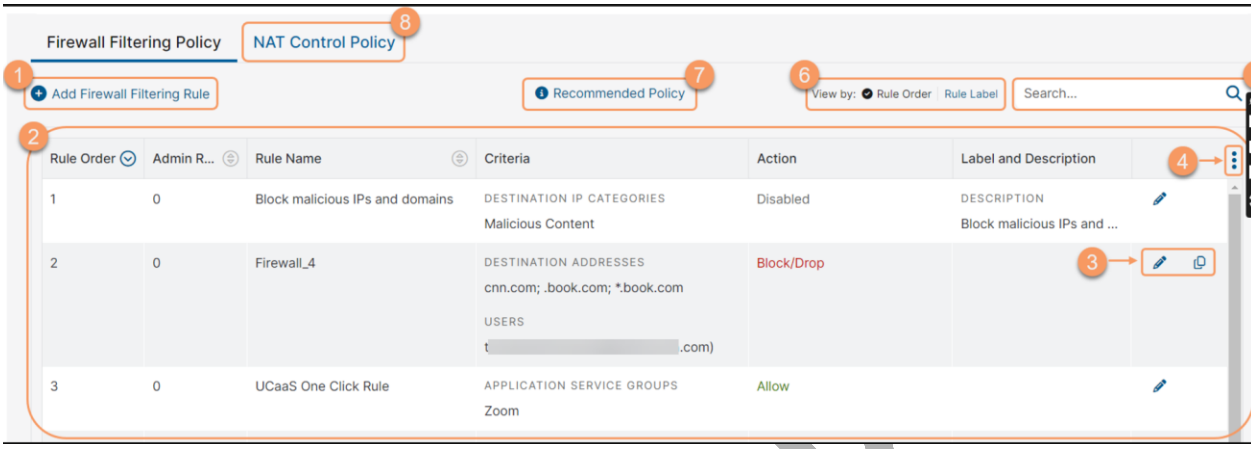
---

2. Policy Enforcement

Objective: Configure DLP or firewall rules to block unauthorized protocols or risky file types.

Steps:

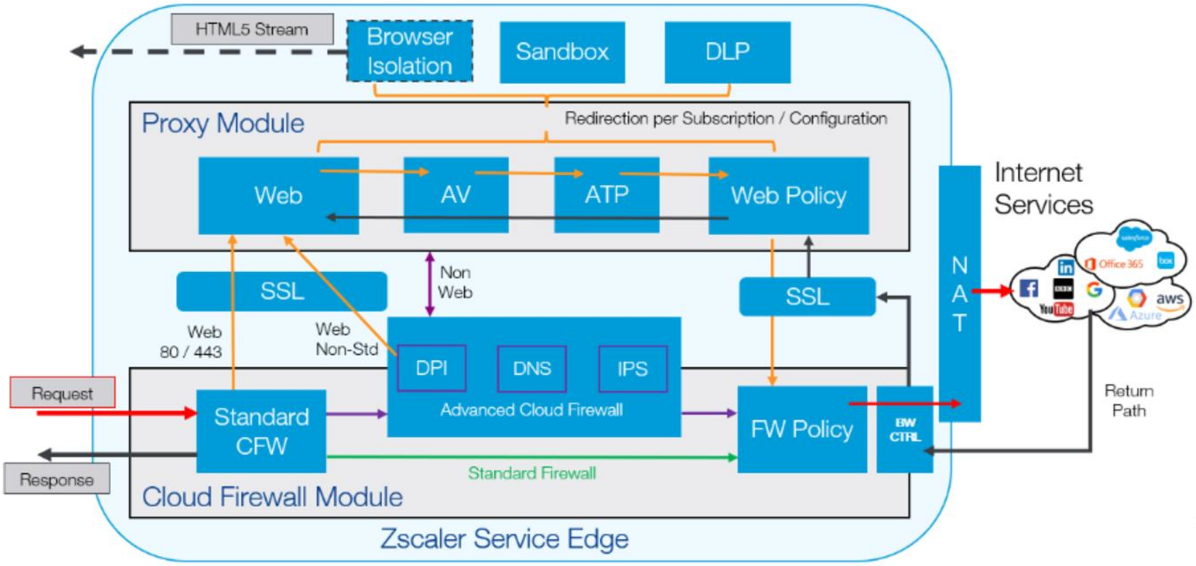
1. **Access Policy Configuration:**
   - **Log in to the Zscaler Admin Portal.**
   - **Navigate to "Policy" > "File Type Control" or "Firewall Control."**
2. **Configure Firewall Rules:**
   - **Create a new rule to block insecure protocols (e.g., FTP, Telnet).**
   - **Define source, destination, and application-based restrictions.**


Firewall Filtering Policy
NAT Control Policy
Add Firewall Filtering Rule
Recommended Policy
View by: ● Rule Order | Rule Label
Search...
1
2
3
4
6
7
8

Rule Order	Admin R...	Rule Name	Criteria	Action	Label and Description
1	0	Block malicious IPs and domains	DESTINATION IP CATEGORIES Malicious Content	Disabled	DESCRIPTION Block malicious IPs and ...
2	0	Firewall_4	DESTINATION ADDRESSES cnn.com; .book.com; *.book.com USERS t[redacted].com)	Block/Drop	
3	0	UCaaS One Click Rule	APPLICATION SERVICE GROUPS Zoom	Allow	

3. **Set Up DLP Policy:**
   - **Navigate to "Policy" > "DLP."**
   - **Configure rules to prevent sensitive data leaks (e.g., block credit card numbers).**
   - **Add exceptions for trusted users or locations.**
4. **Test Policies:**
   - **Generate test traffic matching the new rules and verify blocking behavior.**

ZIA Service Edge Modules



3. Sandbox Analysis

Objective: Submit files to Zscaler Sandbox and interpret results to detect unknown threats.

Steps:

1. **File Submission:**
    - **Upload files to the Zscaler Sandbox via a test machine with Zscaler Client Connector.**
    - **Ensure policies are set to "Submit Unknown Files for Analysis."**
2. **Analyze Results:**
    - **Access "Sandbox Reports" under the Analytics tab.**
    - **Look for fields such as malwareclass and malwarecat to understand verdicts.**
    - **Identify malicious behaviors like file encryption or unauthorized network calls.**
3. **Extract IoCs:**
    - **Record Indicators of Compromise (e.g., hash values, URLs) for further investigation.**

---

4. Real-Time Monitoring

Objective: Create custom widgets to monitor phishing or malware trends.

Steps:

1. **Customize Dashboards:**
    - **Go to "Dashboard" > "Add Widget."**
    - **Select "Threats" and filter for specific categories (e.g., phishing, malware).**
2. **Define Filters:**
    - **Use filters such as Advanced Threat Super Category: Phishing or Malware.**
    - **Add additional conditions like user location or risk score.**
3. **Analyze Trends:**
    - **Review charts for spikes in specific threats.**
    - **Pivot from widget data to detailed logs for deeper analysis.**
4. **Schedule Reports:**
    - **Schedule a daily or weekly report summarizing phishing/malware activity.**

---

5. SIEM Integration

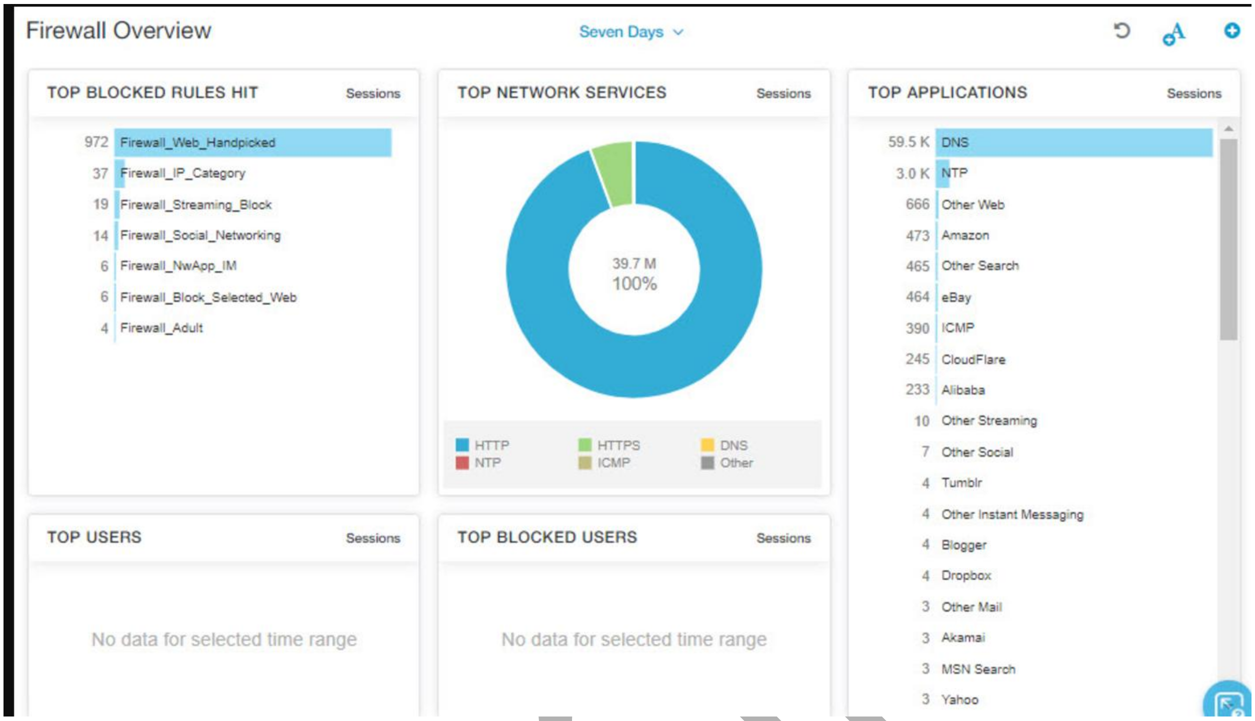
Objective: Practice forwarding Zscaler logs to a SIEM and run correlation queries for multi-vector threat analysis.

Steps:

1. **Set Up Nanolog Streaming Service (NSS):**
   - **Deploy NSS as a virtual appliance or cloud instance (e.g., AWS, Azure).**
   - **Configure NSS feeds for web, firewall, and alert logs.**
2. **Forward Logs to SIEM:**
   - **Point NSS output to the SIEM's IP and port.**
   - **Select fields like malwareclass, urlcat, and reason for analysis.**
3. **Run Correlation Queries:**
   - **Search for patterns in logs, such as repeated access to phishing sites followed by data exfiltration attempts.**
   - **Correlate Zscaler logs with other security tools (e.g., endpoint detection logs).**
4. **Analyze Results:**
   - **Identify anomalies and investigate threat chains.**
   - **Document findings and suggest remediation steps.**

Highlight:

1. **Log Analysis Report:**
   - **Screenshots of dashboard insights and observations on botnets/malware.**
2. **Policy Enforcement Logs:**
   - **Export of blocked events and policy configurations.**
3. **Sandbox Analysis Summary:**
   - **Report on sandbox findings, including IoCs and suspicious behaviors.**
4. **Custom Widgets:**
   - **Screenshots of custom widgets and trend analysis.**
5. **SIEM Correlation Findings:**
   - **Detailed log correlations and actionable insights.**



Firewall Overview

Seven Days

TOP BLOCKED RULES HIT

Sessions	
972	Firewall_Web_Handpicked
37	Firewall_IP_Category
19	Firewall_Streaming_Block
14	Firewall_Social_Networking
6	Firewall_NwApp_IM
6	Firewall_Block_Selected_Web
4	Firewall_Adult

TOP NETWORK SERVICES

Sessions

TOP APPLICATIONS

Sessions	
59.5 K	DNS
3.0 K	NTP
666	Other Web
473	Amazon
465	Other Search
464	eBay
390	ICMP
245	CloudFlare
233	Alibaba
10	Other Streaming
7	Other Social
4	Tumblr
4	Other Instant Messaging
4	Blogger
4	Dropbox
3	Other Mail
3	Akamai
3	MSN Search
3	Yahoo

TOP USERS

Sessions

No data for selected time range

TOP BLOCKED USERS

Sessions

No data for selected time range

For Content like this , visit our website – https://techclick.in