Assignment 18

1. Explain the different types of firewalls. Discuss the policies and rules of any firewalls. What are the benefits derived? Discuss the best practices for the firewall configurations.

Firewalls are the first line of defence for your network security. A firewall is a type of cybersecurity tool used to monitor and filter incoming and outgoing network traffic – from external sources, internal sources, and even specific applications. The primary goal of a firewall is to block malicious traffic requests and data packets while letting through legitimate traffic.

Firewalls are crucial security components that monitor and control incoming and outgoing network traffic based on predetermined security rules. They essentially act as barriers between trusted and untrusted networks to prevent unauthorized access while allowing legitimate communications to pass through.

There are many types of **firewall deployment architectures**, including network-based (software), host-based (hardware), and cloud-based. Every firewall operates based on predetermined rules to determine which outside networks and applications can be trusted. As such, firewalls are a key component of any network security architecture.

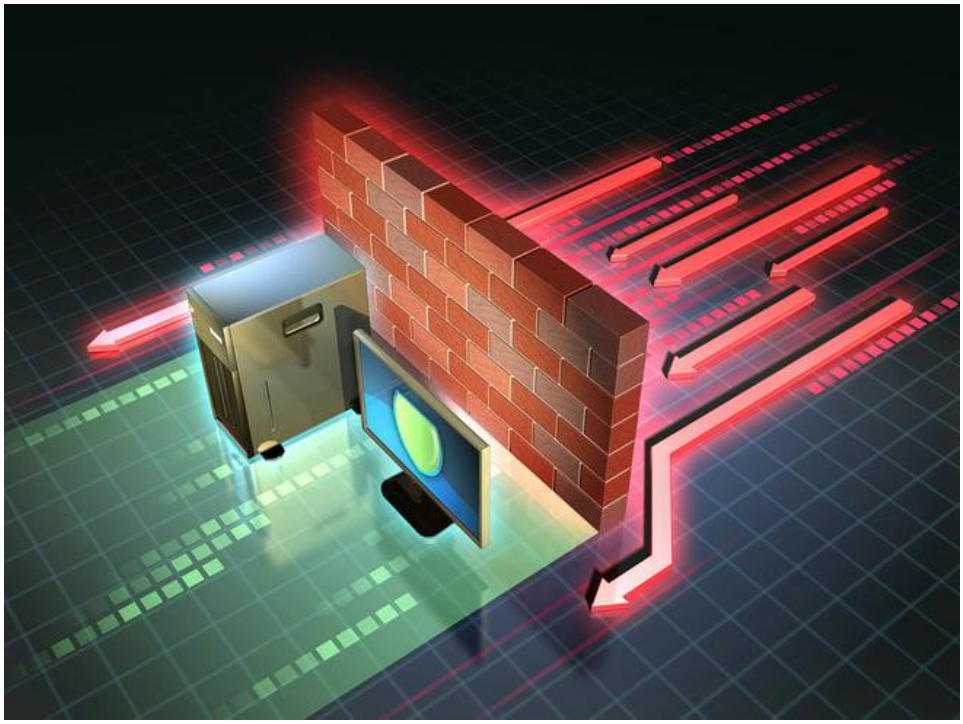
How Does A Firewall Function?

So, how do firewalls work? Simply put, a firewall shields your network from **suspicious data** by inspecting incoming data packets for threats. Firewalls analyse network traffic for data content, which firewall ports (or entry points) the data is trying to use, and where the data originated.

Different types of firewalls use different methods – or combinations of methods – to assess potentially malicious sources.

These firewall tools include packet-filtering, TCP verification, deep-layer inspections, and proxy checkpoints. Next-generation firewalls (NGFWs) go even further by employing preventative measures, such as using machine learning to detect unusual data behavior.

Types of Firewalls and Deployment Architectures



Firewall types can be divided into several categories based on their general structure, method of operation, and whether they offer basic or **advanced threat protection (ATP)**. Examples of firewalls can be found below.

Firewall Types:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls

Firewall Delivery Methods:

- Software firewalls
- Hardware firewalls
- Cloud firewalls

Type 1: Packet-Filtering Firewalls

Packet-filtering firewalls are the most “basic” and oldest type of firewall. The process of packet filtering involves creating a checkpoint at traffic router or switch. The firewall performs a simple check for the data packets coming through the router – inspecting information such as the destination and origination IP address, packet type, **port number,** and other surface-level details without opening the packet to examine its contents. It then drops the packet if the information doesn’t pass inspection.

The good thing about these firewalls is that they are not very resource-intensive. Using fewer resources means they are relatively simply and don’t meaningfully impact system performance. However, they are also relatively easy to bypass compared to firewalls with more robust inspection capabilities.

Type 2: Circuit-Level Gateways

Circuit-level gateways are another simple firewall type meant to quickly and easily approve or deny traffic without consuming considerable computing resources. Circuit-level gateways work by verifying the **transmission control protocol (TCP)** handshake. This TCP handshake check is designed to ensure the requested packet session is legitimate.

While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet had malware but also had the proper TCP handshake, it would easily pass through. Vulnerabilities like this are why circuit-level gateways are not enough to protect your business by themselves.

Type 3: Stateful Inspection Firewalls

Stateful inspection firewalls combine packet inspection technology and TCP handshake verification to offer more serious protection than either of the two architectures could provide alone. They also can keep a contextual database of vetted connections and draw on historical traffic records to make decisions about the depth of scrutiny each packet warrants.

However, these firewalls also put more of a strain on computing resources. This may slow down the transfer of legitimate packets compared to the other solutions.

Type 4: Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

Proxy firewalls (aka application-level gateways or cloud firewalls) operate at the application layer to filter incoming traffic between your network and the traffic source. These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.

This check assesses both the packet and TCP handshake protocol, similar to the stateful inspection firewall. Proxy firewalls may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it does not contain malware.

Once the check is complete and the packet is approved to connect to the destination, the proxy sends it off. This rates an extra layer of separation between the “client” – the system where the packet originated – and the individual devices on your network, creating additional anonymity and network protection.

The one drawback to proxy firewalls is that they can create a significant slowdown because of the extra steps in the data packet transfer process.

Type 5: Next-Generation Firewalls

Many recently-released firewall products are touted as “next-generation” architectures. However, there is no consensus on what makes a firewall genuinely next-gen.

Next-generation firewall architectures typically include the same core features as other firewall iterations – deep-packet inspection, TCP handshake checks, and surface-level packet inspection. They can also consist of other technologies, such as intrusion prevention systems (IPSs) that automatically stop application-level attacks and malware attacks against your network.

Since there is no one definition of a next-generation firewall, it is essential for you to verify what specific capabilities such firewalls have before investing.

Firewall Deployment Architecture

1: Software Firewalls

Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware or cloud server. The big benefit of a software firewall is that it is highly useful for providing in-depth security by isolating individual network endpoints from one another.

However, maintaining individual software firewalls on different devices can be difficult and time-consuming. Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

2: Hardware Firewalls

Hardware firewalls use a physical appliance that acts like a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by ensuring malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.

However, the major weakness of a hardware-based firewall is that it is often easier for insider attacks to bypass them. In addition, the actual capabilities of a hardware firewall may vary depending on the manufacturer – for example, some may have a more limited capacity to handle simultaneous connections than others.

3: Cloud Firewalls

Cloud firewall – also called firewall-as-a-service or FaaS – refers to any firewall delivery architecture that uses a cloud solution. Many consider cloud firewalls synonymous with proxy firewalls since a cloud server is often used in a firewall setup (although the proxy does not necessarily have to be on the cloud, it frequently is).

The primary benefit of having cloud-based firewalls is that they are straightforward to scale with your organization. As your needs grow, you can add additional capacity to the cloud server to filter larger traffic loads. Cloud firewalls, like hardware firewalls, excel at perimeter security.

State of Firewalls in 2024:

While numerous iterations of firewalls have emerged in the past decades, the continuous tenacity and adaptability of firewall technology consistently demonstrates that organizations with a **resilient firewall infrastructure** maintain a cybersecurity edge over those without firewalls.

Here are some trends to watch out for in 2024:

- Next-generation firewalls are trending towards increased usage of artificial intelligence (AI) and machine learning (ML) to automate security tasks and predict likely sources of anomalous traffic patterns.
- Cloud firewalls are being increasingly adopted by security-conscious businesses, and as a result, cloud-based threats are similarly on the rise.
- Hybridized cybersecurity architectures have become the norm, as companies are layering multiple firewall types and coordinating their firewall infrastructure with other network security tools.

Firewalls: Policies and Rules

The policies and rules governing firewalls:

Firewall Policies

A firewall policy is a set of rules that dictate how network traffic is handled. These policies are designed to balance security and functionality, ensuring that the network is protected without hindering legitimate operations. Key aspects of firewall policies include:

- **Access Control**: Decides which traffic is allowed or denied based on source and destination IP addresses, ports, and protocols.
- **Address Translation**: NAT (Network Address Translation) and PAT (Port Address Translation) are used to hide internal IP addresses and manage IP address allocation.
- **Logging and Auditing**: Specifies what data should be logged for monitoring and auditing purposes.
- **Security Levels**: Determines the security level for different types of traffic or network zones.

- **Resource Access**: Defines which internal resources external entities can access.

Firewall Rules

Firewall rules are the specific instructions within a policy that tell the firewall how to handle different types of network traffic. Rules are typically based on the following criteria:

- **Protocol**: UDP, TCP, ICMP, etc.
- **IP Address**: Source and destination.
- **Port Number**: Specific ports can be opened or closed.
- **Direction**: Traffic can be inbound, outbound, or both.
- **Action**: What the firewall should do—accept, drop, or reject the traffic.

Rule Precedence and Ordering

Firewalls process rules in order from top to bottom. The first rule that matches the traffic is applied. If no rule matches, the traffic is handled according to the default action, which is often "deny."

Stateful Inspection

Modern firewalls often use stateful inspection, where they keep track of the state of network connections. This ensures that only traffic that is part of an established connection is allowed to pass.

Dynamic Rules

Some firewalls support dynamic rules that can change based on external conditions, such as time of day, user status, or security alerts.

Access Control Lists (ACLs)

ACLs are used to define rules for specific traffic patterns. They can specify traffic types to allow or deny based on source and destination addresses, ports, and protocols.

Packet Filtering

The simplest form of firewall operation, packet filtering, involves checking each packet against the rules and deciding whether to forward or drop it.

Proxy Services

Some firewalls use proxy services to intercept and inspect traffic before it reaches the destination, providing an additional layer of security.

Security Zones

Firewalls often define security zones (such as DMZ, internal, and external) to control the level of access between different segments of the network.

High Availability and Redundancy

To ensure continuous operations, firewalls are often deployed in pairs, providing failover and load balancing capabilities.

Integration with Other Security Tools

Firewalls may integrate with intrusion detection systems (IDS), intrusion prevention systems (IPS), and other security tools to enhance overall network protection.

Regular Updates and Patching

Firewall rules and policies should be regularly reviewed and updated to adapt to changing security landscapes and organizational needs.

Firewalls play a pivotal role in securing networks against unauthorized access and attacks. Effective firewall policies and rules require careful planning, regular updates, and a deep understanding of network traffic patterns and security requirements. By tailoring these rules to specific organizational needs, organizations can significantly enhance their network security posture.

Firewalls monitor, filter, and control network traffic based on predetermined security rules.

Here are the primary benefits of using firewalls:

Protection against Malicious Traffic

Firewalls can block unauthorized access attempts and malicious traffic such as viruses, worms, and other cybersecurity threats.

They inspect incoming and outgoing traffic to ensure it meets the security policy, preventing harmful data from entering or leaving the network.

Access Control

Firewalls enable network administrators to control which internal systems are accessible from the internet.

They can restrict access to specific services or applications based on the source of the request, helping to prevent unauthorized access and use.

Prevention of DoS and DDoS Attacks

Firewalls can mitigate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks by identifying and blocking the traffic patterns associated with these types of attacks.

Masking Internal IP Addresses

By using Network Address Translation (NAT), firewalls can hide the IP addresses of internal networks from the outside world, making it more difficult for attackers to target specific systems.

Logging and Monitoring

Firewalls generate logs that can be used for monitoring network traffic and detecting potential security breaches.

These logs are also valuable for compliance purposes and can help in forensic analysis after an attack.

Quality of Service (QoS)

Advanced firewalls can prioritize certain types of network traffic, ensuring that critical applications receive the necessary bandwidth.

This is especially useful in networks where bandwidth is limited or where certain applications (like VoIP or video conferencing) require high-quality network conditions.

Gateway Antivirus and Antispyware Features

Some firewalls include virus and spyware scanning capabilities, which can prevent infected files from being downloaded or spread within the network.

URL Filtering and Content Control

Firewalls can block access to websites that are known to be malicious or inappropriate, helping to maintain a productive and safe work environment.

Integration with Other Security Tools

They can work in conjunction with intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) systems to provide a comprehensive security solution.

Scalability

Firewalls can be scaled to meet the needs of small businesses or large enterprises, making them suitable for various network sizes and complexities.

Economic Benefits

By preventing security breaches and downtime, firewalls can save organizations significant costs associated with recovery, lost productivity, and reputation damage.

Firewalls are essential components of a layered security approach, providing a critical line of defence against a wide range of cyber threats. They ensure that networks remain secure while maintaining the necessary level of access and functionality for users. Regular updates and management of firewall rules are crucial to maintaining its effectiveness against evolving threats.

Best practices for firewall configurations:

Default Deny Policy:

Implement a default deny policy to block all traffic unless explicitly permitted by rules. This ensures that only authorized traffic is allowed to pass through the firewall.

Least Privilege Principle:

Adhere to the principle of least privilege by creating rules that allow only necessary traffic. Avoid overly permissive rules that can expose the network to potential risks.

Rule Documentation:

Document firewall rules and policies clearly to ensure that administrators understand the purpose and impact of each rule. Regularly review and update rule documentation.

Rule Ordering:

Arrange firewall rules in a logical order to prioritize more specific rules over generic rules. This helps in efficiently processing traffic and resolving rule conflicts.

Stateful Inspection:

Enable stateful inspection to track the state of connections and allow only legitimate traffic that is part of an established connection. This enhances security by preventing unauthorized access.

Update Regularly:

Keep firewall firmware and software up to date to address security vulnerabilities and ensure optimal performance. Regular updates also include new threat intelligence updates.

Segmentation:

Implement network segmentation by creating separate security zones with specific firewall rules for different network segments. This limits the impact of breaches and prevents lateral movement of threats.

Logging and Monitoring:

Enable logging for firewall activities to track traffic, rule violations, and security events. Regularly monitor firewall logs to detect and respond to suspicious activities.

Testing Changes:

Test firewall rule changes in a controlled environment before deploying them in production. This helps identify any potential issues or conflicts that may arise from the changes.

Redundancy and High Availability:

Implement firewall redundancy and high availability configurations to ensure continuous protection and minimal downtime in case of a firewall failure

By following these best practices for firewall configurations, organizations can strengthen their security posture, mitigate risks, and ensure the effective management of network traffic.

2. Discuss the configuration and rule sets for ModSecurity. Explain briefly the features and functionalities of the Imperva SecureSphere WAF.

With over 70% of all attacks now carried out over the web application level, organizations need every help they can get in making their systems secure.

Web application firewalls are deployed to establish an external security layer that increases the protection level, detects and prevents attacks before they reach web-based software programs.

ModSecurity is an open-source web-based firewall application (or WAF) supported by different web servers: Apache, Nginx and IIS.

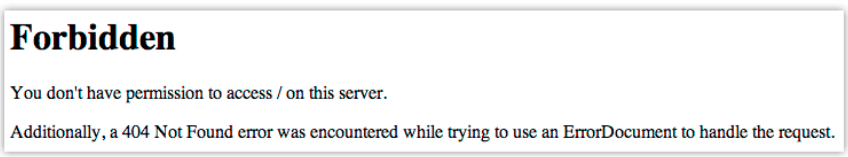
Usage

The module is configured to protect web applications from various attacks. ModSecurity supports flexible *rule engine* to perform both simple and complex operations. It comes with a Core Rule Set (CRS) which has various rules for:

- cross website scripting
- bad user agents
- SQL injection
- Trojans
- session hijacking
- other exploits

Most common errors

The most common error triggered by a mod security rule on our shared servers is **403 Forbidden** one:



It simply states that you do not have **permission** to access / on the server.

Depending on the exact link where you get the error, the path may vary.

ModSecurity works in the background, and every page request is being checked against various rules to filter out those requests which seem malicious. These can be the ones that have been run to exploit vulnerabilities in your website software with the only goal to hack the site.

Sometimes, due to poor website coding, mod_security may incorrectly determine that a certain request is malicious, while it is actually legitimate. When it happens, you still get a 403 error.

NOTE: Besides the 403 Forbidden error, you may also receive 404 Not Found or 500 Internal Server Error errors.

Configuring ModSecurity Rule Sets for Imperva SecureSphere WAF

When integrating ModSecurity with Imperva SecureSphere WAF, the configuration process involves setting up and customizing rule sets to ensure comprehensive protection against web-based attacks. ModSecurity, a widely used open-source web application firewall (WAF), is known for its flexibility and can be configured with various rule sets to address specific security requirements.

1. Understanding ModSecurity Rule Sets

ModSecurity uses rule sets to define security policies that can detect and block malicious requests. These rule sets can be tailored to include a mix of community-developed rules, such as the OWASP ModSecurity Core Rule Set (CRS), and custom rules to suit specific needs.

2. Configuration Steps in Imperva SecureSphere WAF

To configure ModSecurity rule sets in Imperva SecureSphere WAF, follow these steps:

Log in to the Imperva SecureSphere WAF Management Interface:

Access your Imperva SecureSphere WAF dashboard and sign in with your credentials.

Navigate to the WAF Rule Set Configuration:

Go to the security policy section within the dashboard to manage the rule sets.

Select or Import a Rule Set:

Choose from the provided rule sets or import a custom rule set if you have one.

Customize the Rule Set:

Adjust the parameters of each rule to fit your specific requirements. This includes setting thresholds for alerting, blocking, or logging actions.

Enable or Disable Rules:

Depending on your security posture, enable rules that are relevant to your web application's vulnerabilities and disable those that might cause false positives.

Test the Rule Set:

Before applying the rule set to a live environment, test it in a staging environment to ensure it does not block legitimate traffic or cause performance issues.

3. Implementing Custom Rules

Custom rules are essential to address specific vulnerabilities that are not covered by standard rule sets. When creating custom rules:

Identify Vulnerabilities:

Use web application vulnerability assessments to identify specific vulnerabilities that need to be addressed.

Craft Custom Rules:

Write custom rules to target these vulnerabilities. Ensure that the rules are well-written to avoid false positives.

Integrate Custom Rules:

Integrate the custom rules into the rule set configuration in the Imperva SecureSphere WAF dashboard.

4. Monitoring and Maintenance:

After deploying the rule sets, monitor the WAF logs and performance to ensure that the rules are effective and not causing unnecessary alerts or blocking legitimate traffic. Regularly update the rule sets to address new vulnerabilities and attack patterns.

5. Best Practices for Using ModSecurity Rule Sets

Stay Updated:

Regularly update your rule sets with the latest security patches and enhancements.

Customization:

Customize rule sets to fit your web application's specific needs and environment.

Testing:

Always test new rule sets in a non-production environment to avoid unexpected disruptions.

Documentation:

Maintain documentation of your rule set configurations for future reference and compliance purposes.

By following these guidelines, we can effectively configure ModSecurity rule sets within Imperva SecureSphere WAF to enhance the security of your web applications. This approach ensures that you have a robust defence against common web-based attacks while minimizing the impact on legitimate traffic.

Imperva SecureSphere - Web Application Firewall

Protect Critical Web Applications and Data

Your website receives a continuous barrage of attacks. If hackers uncover a crack in your defences, they can steal your application data, defraud your users, and take down your website.

The SecureSphere Web Application Firewall stops web attacks and prevents costly data breaches and downtime. Combining multiple defenses, SecureSphere accurately pinpoints and blocks attacks without blocking your customers. It offers drop-in deployment and automated management. Certified by ICSA Labs, SecureSphere satisfies PCI 6.6 compliance and provides ironclad protection against the OWASP Top Ten.

Imperva SecureSphere

The market-leading SecureSphere Web Application Firewall has transformed the way businesses protect their applications by automating web security and providing flexible, transparent deployment. With its comprehensive protection and low administrative overhead, SecureSphere is the ideal solution to secure valuable web assets and achieve PCI compliance. Imperva SecureSphere is available on physical and virtual appliances, and on Amazon Web Services.

Key Capabilities:

- Automatically learns protected applications and user behavior
- Updates Web defences with research-driven intelligence on current threats
- Accurately blocks attempts to exploit known and unknown vulnerabilities
- Identifies traffic originating from known malicious sources with **ThreatRadar**
- Correlates request attributes across security layers and over time to detect sophisticated, multi-stage attacks
- Virtually patches vulnerabilities by integrating with Web application vulnerability scanners, reducing the window of exposure and impact of emergency fixes
- Fully addresses **PCI 6.6**
- Offers high performance and transparent, drop-in deployment

Features:

Track Attack Sources on a Global Scale

Aggregating attack data from both third-party security providers and SecureSphere Web Application Firewalls, ThreatRadar provides a comprehensive defence against known malicious sources. ThreatRadar augments SecureSphere's existing layers of protection –such as Dynamic Profiling technology, attack signatures, and bot mitigation rules – to provide additional context on suspicious requests. SecureSphere owners can build custom policies that correlate ThreatRadar

reputation and geolocation data with other SecureSphere defences to accurately pinpoint attacks.

Continuous, Automated Feed of Current Attack Sources

ThreatRadar delivers multiple attack feeds, in near real time, to SecureSphere Web Application Firewalls. Security feeds identify sources that have recently executed SQL injection, cross-site scripting, DDoS, or other Web attacks. Imperva continuously updates the feeds, providing current protection against malicious traffic.

Dynamically Adapt Web Security Policies

As SecureSphere WAF receives attack source information, ThreatRadar dynamically adjusts Web security policies to alert or block traffic from newly identified attack sources. Furthermore, custom security rules can use information provided by the feeds to fine-tune the response for specific types of traffic, such as the ability to block only the traffic that comes from a malicious source exhibiting suspicious behavior.

Early Detection, Blocking of Malicious Sources

ThreatRadar dramatically reduces application visibility to attackers. By blocking Web requests based on user reputation, hackers have virtually no opportunity to explore the Web application for possible weaknesses and are less likely to launch a successful attack.

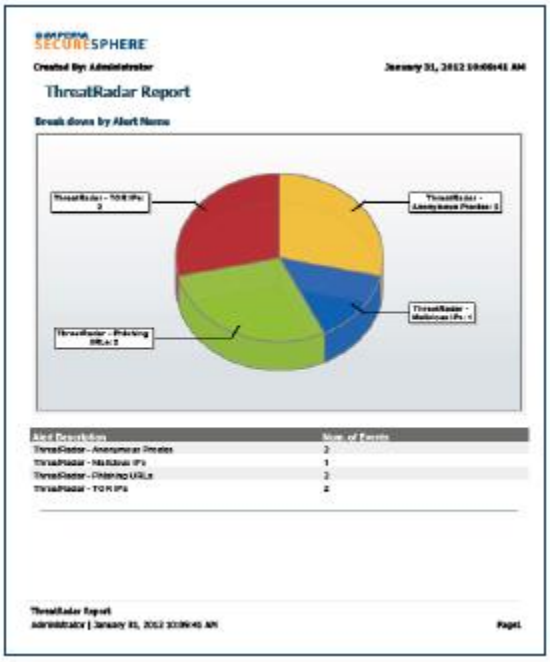
Crowd-Sourced Threat Intelligence to Identify New Attack Vectors

ThreatRadar Community Defense enables SecureSphere Web Application Firewalls to detect new attack patterns without blocking legitimate requests. Community Defence uses patent pending technology to gather suspicious Web requests, validate that requests are attacks, and transform identified attacks into signatures. Equipped with Community Defense, SecureSphere Web Application Firewalls can spot attacks witnessed by other SecureSphere-protected websites.

Streamlined Forensic Analysis with Clear, Relevant Alerts and Reports

ThreatRadar takes the guesswork out of security event analysis. User reputation and geographic location data provide additional context, enabling precise incident response and minimizing operational workload.

ThreatRadar Reputation Services provides geographical context on Web attacks.



Security alerts show requests from malicious sources. Reports summarize attacks from anonymous proxies, TOR networks, malicious IP addresses and phishing sites.

Imperva SecureSphere WAF: Key Functionalities

The key functionalities of the Imperva SecureSphere WAF:

Advanced Threat Protection

Intrusion Prevention System (IPS): Blocks known attack patterns and zero-day exploits.

SQL Injection Prevention: Guards against SQL injection attacks that target database vulnerabilities.

Cross-Site Scripting (XSS) Protection: Prevents malicious scripts from being executed on user browsers.

Bot Detection and Defence: Identifies and mitigates automated attacks from bots.

Compliance and Security Enforcement

PCI-DSS Compliance: Ensures adherence to the Payment Card Industry Data Security Standard.

OWASP Top 10: Adheres to the Open Web Application Security Project's guidelines on the top 10 web application security risks.

GDPR Compliance: Helps organizations comply with the General Data Protection Regulation by securing personal data.

Traffic Management

DDoS Protection: Defends against Distributed Denial of Service attacks by filtering out malicious traffic.

Rate Limiting: Controls the speed of incoming traffic to prevent overloading the application.

Data Security

Data Masking: Hides sensitive information that could be exposed to attackers.

Data Leakage Prevention (DLP): Monitors and prevents sensitive data from being unintentionally exposed.

Inspection and Monitoring

Protocol Inspection: Analyzes HTTP/HTTPS traffic for anomalies and malicious intent.

Real-Time Monitoring: Provides visibility into web application traffic and security events.

Policy Management

Customizable Security Policies: Allows for the creation of detailed policies to fit specific business needs.

Automated Policy Enforcement: Automatically applies security policies based on traffic and threat intelligence.

Reporting and Analytics

Comprehensive Reporting: Offers detailed reports on security events, compliance status, and performance metrics.

Analytics: Analyzes traffic patterns to identify potential threats and anomalies.

Integration and Scalability

API Support: Integrates with other security tools and platforms through APIs.

Cloud and On-Premises Deployment: Supports deployment in cloud environments, on-premises, or in a hybrid model.

Scalable Architecture: Designed to handle high traffic volumes without compromising performance.

User-Friendly Management

Centralized Management Console: Provides a single interface for managing multiple WAF instances.

Easy Configuration: Simplifies the setup process with intuitive interfaces and wizards.

Support and Updates

24/7 Technical Support: Offers round-the-clock assistance for technical issues.

Regular Updates: Ensures the WAF is up-to-date with the latest security patches and threat intelligence.

The Imperva SecureSphere WAF is a robust solution that helps organizations secure their web applications and data from a wide range of cyber threats while maintaining compliance with industry standards. Its advanced features and customizable policies make it a versatile tool for different types of web environments.

3. Discuss the features of the Barracuda Web Application Firewall (BWAF). Explain the use-case example of this firewall, including scenarios, challenges, solutions, and benefits.

The Barracuda Web Application Firewall protects your web, mobile and API applications from being compromised, prevents data breaches, ensure protection from web attacks and provide control access and authentication.

The Barracuda WAF App analyzes traffic flowing through the Barracuda WAF and provides pre-configured dashboards that allow you to monitor WAF traffic as well to analyze various types of attacks detected both by Barracuda and Sumo Logic's own Threat Intelligence database.

Log types

The Barracuda WAF App uses the following log types:

- **System Logs**. Events generated by the Barracuda Web Application Firewall system.
- **Web Firewall Log**. All actions and events on the web firewall. These logs help the administrator to analyze traffic for suspicious activity and fine tune the web firewall policies.
- **Access Logs**. All web traffic activities. These logs help the administrator obtain information about website traffic and performance.
- **Audit Logs**. The audit logs record the activity of the users logged in to the GUI of the Barracuda Web Application Firewall. These logs are used for administration purposes.
- **Network Firewall Logs**. The network traffic passing through the interfaces (WAN, LAN and MGMT) that matches the configured Network ACL rule. These log entries provide information on every packet that is allowed or denied by Barracuda Web Application Firewall based on the Action specified in the ACL rule. This information helps identify where the network traffic originated, its destination, and the action applied.

Sample log messages

The following table shows sample log messages for the corresponding log types.

Log Type	Sample
System Log	<129>1 2019-04-19T00:52:58-07:00 WAFNEW 2019-04-19 - 00:52:58.985 -0700 WAFNEW SYS PROCMON ALER 50009 Log storage exceeds 10%
Web Firewall Log	<129>1 2019-04-09T03:57:49-07:00 WAFNEW 2019-04-09 - 03:57:49.304 -0700 WAFNEW WF ALER PYTHON_PHP_ATTACKS_MEDIUM_IN_URL 182.69.208.134 50910 10.0.1.90 80 security-policy GLOBAL DENY NONE [type\="python-php-attacks-medium" pattern\="python-cfm-command-substrings" token\="/exec/"] GET 13.234.142.236/dvwa/vulnerabilities/exec/ HTTP "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36" 182.69.208.134 50910 "-" http://13.234.142.236/dvwa/vulnerabi...ge=include.php 16a01bf34f8-f9a544ae
Access Log	<134>1 2019-04-15T15:46:53.460+0530 WAF 2019-04-15 - 15:46:53.460+0530 -0700 WebSite TR 10.1.1.90 80 141.138.107.86 50915 "-" "-" POST HTTPS 202.191.66.53 HTTP/1.0 403 2411 1609 0 22 10.0.2.200 80 0 "-" SERVER DEFAULT PROTECTED VALID /favicon.ico "-" http://www.bing.com/search?q=sumo%20...ox&FORM=IE11SR "-" "Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1467.0 Safari/537.36" 182.69.208.134 50915 "-" "-" "-" "-" 16a01bf4be9-fca462a6

Log Type	Sample
Audit Log	<13>1 2019-04-16T12:55:10+00:00 ip-10-0-1-200 2019-04-16 - 05:55:10.006 -0700 WAF12 AUDIT sourabh GUI 111.93.54.106 55035 CONFIG 86 config SET user_system_ip Siteminder Session Sync user_system_ip_log "Off" "On" []
Network Firewall Log	<13>1 2019-04-19T06:10:58+00:00 ip-10-0-1-200 2019-04-18 - 23:10:58.647 -0700 WAF12 NF INFO TCP 37.204.127.164 39410 10.0.1.20 22 ALLOW SSH MGMT/LAN/WAN interface traffic:allow

Sample queries

Sample Query is from **Top Clients by Bandwidth** panel of the **Barracuda WAF - Client Traffic** dashboard.

```
_sourceCategory=Labs/loggen/barracuda " TR "
| parse regex "(?<Unit_Name>[^ ]+) TR(?<Log>.*)"
| split Log delim=' ' extract 4 as Client_Ip, 13 as Bytes_Sent, 2 as Service_Ip, 3 as Service_Port
| round((Bytes_Sent / 1024),2) as Bandwidth
| sum(Bandwidth) as Bandwidth_Consumed_KB by Client_Ip
| sort by Bandwidth_Consumed_KB
| limit 5
```

Collecting Logs for Barracuda WAF app

This section shows you how to configure collection for the Barracuda WAF App to use with the predefined searches and dashboards.

The Barracuda WAF App provides detailed analytics on system, firewall, and network security so you can protect your environment from malicious attacks. Security Analysis dashboards provide insights into the types of attacks, severity, malicious IPs, blocked and allowed content, and attacks by services. Traffic Analysis dashboards provide detailed information on client, server, and service traffic, as well as errors, bandwidth trends, and service performance.

Step 1: Configure a Collector

To create a new Sumo Logic Hosted Collector, perform the steps in Configure a Hosted Collector.

Step 2: Configure a Source

Cloud syslog collection supports Barracuda Firmware version 9.2.1 or later. You must be running Barracuda Firmware version 9.2.1 or greater to use cloud syslog as an export server.

This section shows you how to configure a source for log collection. In this task you specify the Source Category metadata field, which is a fundamental building block for organizing and labeling sources.

To configure a source, do the following:

1. Perform the steps in Configure a Cloud Syslog Source. and configure the following Source fields:

i. **Name**. (Required) Enter a name. The description is optional.
ii. **Source Category**. (Required) Provide a realistic Source Category for this data type. For example: **prod/barracuda/waf**. For more information, see Best Practices.

2. In the Advanced section, specify the following configurations:

i. **Enable Timestamp Parsing**. True
ii. **Time Zone**. Logs are in UTC by default
iii. **Timestamp Format**. Auto Detect

3. Click **Save**.
4. Copy and paste the **token** in a secure location. You will need this when you configure Barracuda Cloud Syslog Settings.

Step 3: Configure Logging in Barracuda WAF

This section shows you how to configure logging in Barracuda WAF for use with the preconfigured searches and dashboards of the Sumo Logic App for Barracuda WAF.

To configure logging in Barracuda WAF, do the following:

1. Log in to your Barracuda account and go to **ADVANCED > Export Logs.**
2. Go to the **Add Export Log Server**.
3. In the **Add Export Log Server** window, specify values for the following:

- **Name**. Enter a name for the SumoLogic service.
- **Log Server Type**. Select Cloud Syslog Service.
- **IP Address or Hostname**. Enter the IP address or hostname of the SumoLogic service. For example: syslog.collection.your_deployment.sumologic.com
- **Port**. Enter the port associated with the IP address of the SumoLogic service. The default Port is 6514.
- **Token**. Enter the token for Sumo Logic service, such as: 9HFxoa6+lXBmvSM9koPjGzvTaxXDQvJ4POE/ExAMpleTOkenForTAsk3mSEKxPl0Q@41123, where the number 41123 is the sumo PEN and is included as part of the customer token.
- **Log Timestamp and Hostname**. Click **Yes** to log the date and time of the event, and the hostname configured in the BASIC > IP Configuration > Domain Configuration section.
- **Comment**. (Optional) Enter a comment describing the setting.

4. Click **Add**.
5. Go to **ADVANCED** > **Export Logs.**
6. To send all logs to sumologic, in the **export log setting**, change the settings as shown in the following screenshot.

- **Export Log Settings**. Every Log should be marked as **Enable.**

- **Export Log Filters**. Select the severity as per the Logs that need to send. For example, if set to 5-Notice, then logs with 0-5 are sent to the syslog server i.e, 0-Emergency, 1-Alert, 2-Critical, 3-Error, 4-Warning, 5-Notice
  - 0-Emergency: System is unusable (highest priority)
  - 1-Alert: Response must be taken immediately
  - 2-Critical: Critical conditions
  - 3-Error: Error conditions
  - 4-Warning: Warning conditions
  - 5-Notice: Normal but significant condition
  - 6-Information: Informational messages (on ACL configuration changes)
  - 7-Debug: Debug level messages (lowest priority)
7. **Syslog Settings**. Keep as default.
8. Click **Save**.
9. Go to **ADVANCED** > **Export Logs**.
10. In the **Logs Format** tab, make sure every Log format is set to **default** as the app support Default log formats.

Field Extraction Rules

The following shows field extraction rules for different log formats.

System Log

```
parse regex "(?<Unit_Name>[^ ]+) SYS(?<Log>.*)"
| parse field=log " * * * *" as Module_Name, Log_Level, Event_Id,
Log_Details
```

Web Firewall Log

```
parse regex "(?<Unit_Name>[^ ]+) WF(?<Log>.*)"
| parse field=Log " * * * * * * * * * * [*] * * * * \"*\" * * * * *" as
Severity, Attack_Type, Client_Ip, Client_Port, Service_Ip, Service_Port,
Rule, Rule_Type, Action, Follow_Up_Action, Attack_Details, Method, URL,
Protocol, Session_Id, User_Agent, Proxy_Ip, Proxy_Port, User, Referrer, UID
```

Access Log

```
parse regex "(?<Unit_Name>[^ ]+) TR(?<Log>.*)"
| parse field=Log " * * * * * * * * * * * * * * * * * * * * * * * * * * *
\"*\" * * * * * * *" as Service_Ip, Service_Port, Client_Ip, Client_Port,
Login, Cretificate_User, Http_Method, Http_Protocol, Domain, HttpVersion,
Response_Code, Bytes_Sent, Bytes_Received, Cache_Hit, Time_Taken,
Backend_Server, Backend_Server_Port, Server_Time, Session_Id,
Response_Type, Profile_Matched, Protected, WF_Matched, URL, Query_String,
Referrer, Cookie, User_Agent, Proxy_ip, Proxy_Port, Authenticated_User,
Custom_Header_1, Custom_Header_2, Custom_Header_3, UID
```

Audit Log

```
parse regex "(?<Unit_Name>[^ ]+) AUDIT(?<Log>.*)"
| parse field=Log " * * * * * * * * * * * * * *" as Admin_Name,
Client_Type, Login_Ip, Login_Port, Transaction_Type, Transaction_Id,
Command_Name, Change_Type, Object_Type, Object_Name, Variable_Name,
```

```
Old_Value, New_Value, Additional_Data
```

Network Firewall Log

```
parse regex "(?<Unit_Name>[^ ]+) NF(?<Log>.*)"
| parse field=Log " * * * * * * * * * *" as Log_Level, Protocol, Source_Ip,
Source_Port, Destination_Ip, Destination_Port, ACL_Policy, ACL_Name,
Log_Details
```

Install the Barracuda WAF app

This section provides instructions for installing the Barracuda WAF App, as well as examples and descriptions for each of the app dashboards.

Now that you have configured log collection for Barracuda WAF, install the Sumo Logic App for Barracuda WAF, and take advantage of predefined Searches and dashboards.

To install the app, do the following:

1. Select **App Catalog**.
2. In the **Search Apps** field, search for and then select your app.
   Optionally, you can scroll down to preview the dashboards included with the app.
3. To install the app, click **Install App**.
4. Click **Next** in the **Setup Data** section.
5. In the **Configure** section of the respective app, complete the following fields.

i. **Key.** Select either of these options for the data source.
- Choose **Source Category**, and select a source category from the list for **Default Value**.
- Choose **Custom**, and enter a custom metadata field. Insert its value in **Default Value**.

6. Click **Next**. You will be redirected to the **Preview & Done** section.

Your app will be installed in the **Installed Apps** folder and dashboard panels will start to fill automatically.

Each panel slowly fills with data matching the time range query and received since the panel was created. Results will not immediately be available, updating with full graphs and charts over time.

Upgrading the Barracuda WAF app (Optional)

To update the app, do the following:

1. From the Sumo Logic navigation, select **App Catalog**.

2. In the **Search Apps** field, search for and then select your app Optionally, you can identify apps that can be upgraded in the **Upgrade available** section.
3. To upgrade the app, click **Upgrade**.

i. You will be redirected to the **Preview & Done** section if the upgrade did not have any configuration or property change.
ii. You will be redirected to **Setup Data** page if the upgrade has any configuration or property change.

a. In the **Configure** section of the respective app, complete the following fields.
   - **Key.** Select either of these options for the data source.
   - Choose **Source Category**, and select a source category from the list for **Default Value**.
   - Choose **Custom**, and enter a custom metadata field. Insert its value in **Default Value**.
b. Click **Next**. You will be redirected to the **Preview & Done** section.

Your upgraded app will be installed in the **Installed Apps** folder and dashboard panels will start to fill automatically.

Uninstalling the Barracuda WAF app (Optional)

To uninstall the app, do the following:

1. From the Sumo Logic navigation, select **App Catalog**.
2. In the **Search Apps** field, search for and then select your app.
3. Click **Uninstall**.

Viewing Barracuda WAF dashboards

All dashboards have a set of filters that you can apply to the entire dashboard. Use these filters to drill down and examine the data to a granular level.

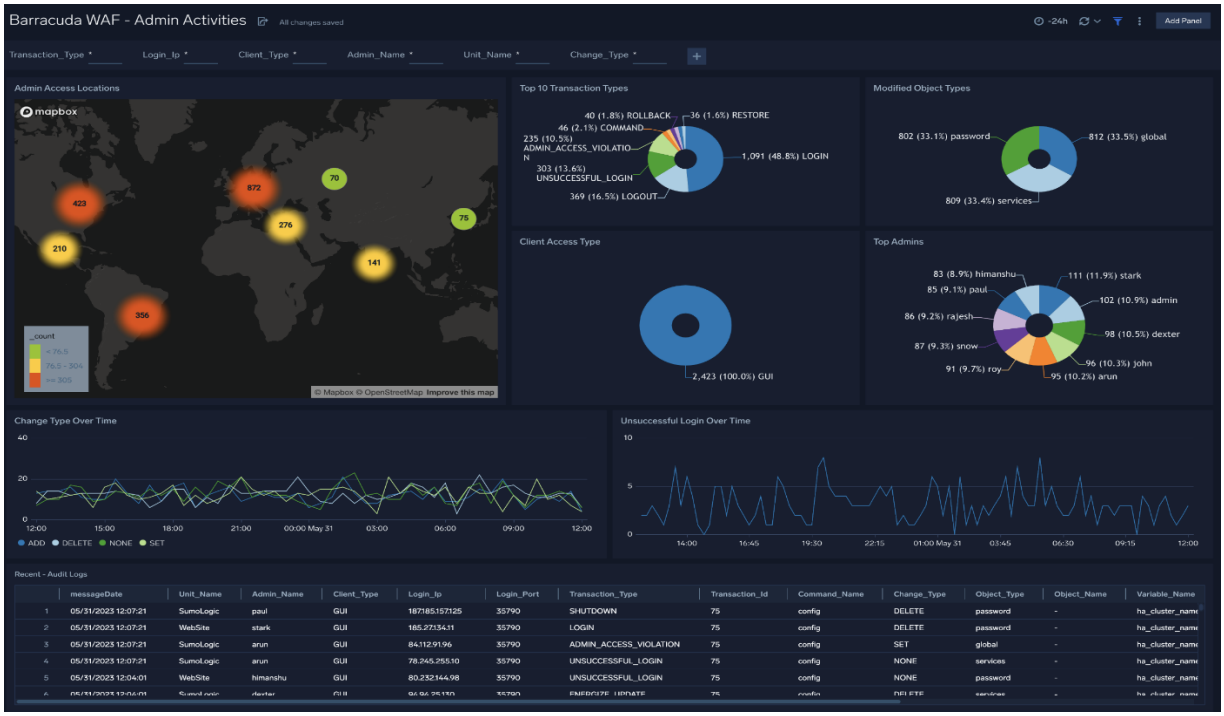
- You can change the time range for a dashboard or panel by selecting a predefined interval from a drop-down list, choosing a recently used time range, or specifying custom dates and times.
- You can use template variables to drill down and examine the data on a granular level. For more information, see Filter with template variables.
- Most Next-Gen apps allow you to provide the **scope** at the installation time and are comprised of a key (_sourceCategory by default) and a default value for this key. Based on your input, the app dashboards will be parameterized with a dashboard variable, allowing you to change the dataset queried by all panels. This eliminates the need to create multiple copies of the same dashboard with different queries.

Admin Activities

The **Barracuda WAF - Admin Activities** dashboard provides insights into all administrative activities performed on the WAF.

Use this dashboard to:

- Make sure admins are accessing WAF units from expected physical locations.
- Monitor admin actions as they relate to transaction types, modified object types, and client access types.
- View trends for unsuccessful logins and change types.
- Drill down into recent audit logs based on search templates.

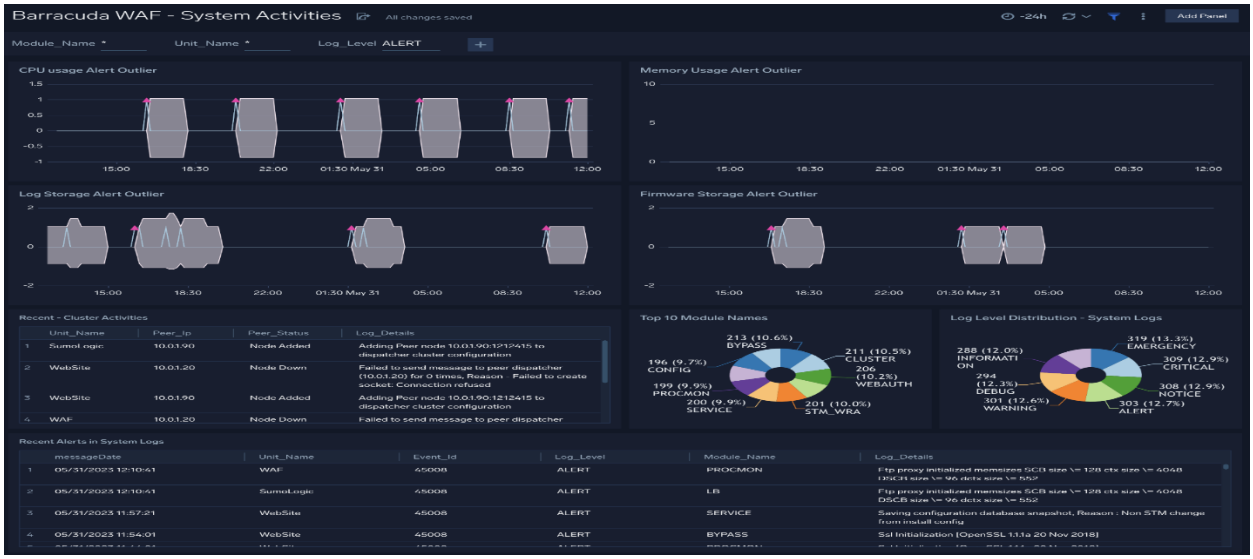


System Activities

The **Barracuda WAF - System Activities** dashboard provides insights into the performance of WAF units, cluster activities and recent alerts.

Use this dashboard to:

- Review the top modules invoked and monitor log level severity.
- Review recent cluster activities for troubleshooting WAF configuration issues.
- Monitor and take action on recent alerts.

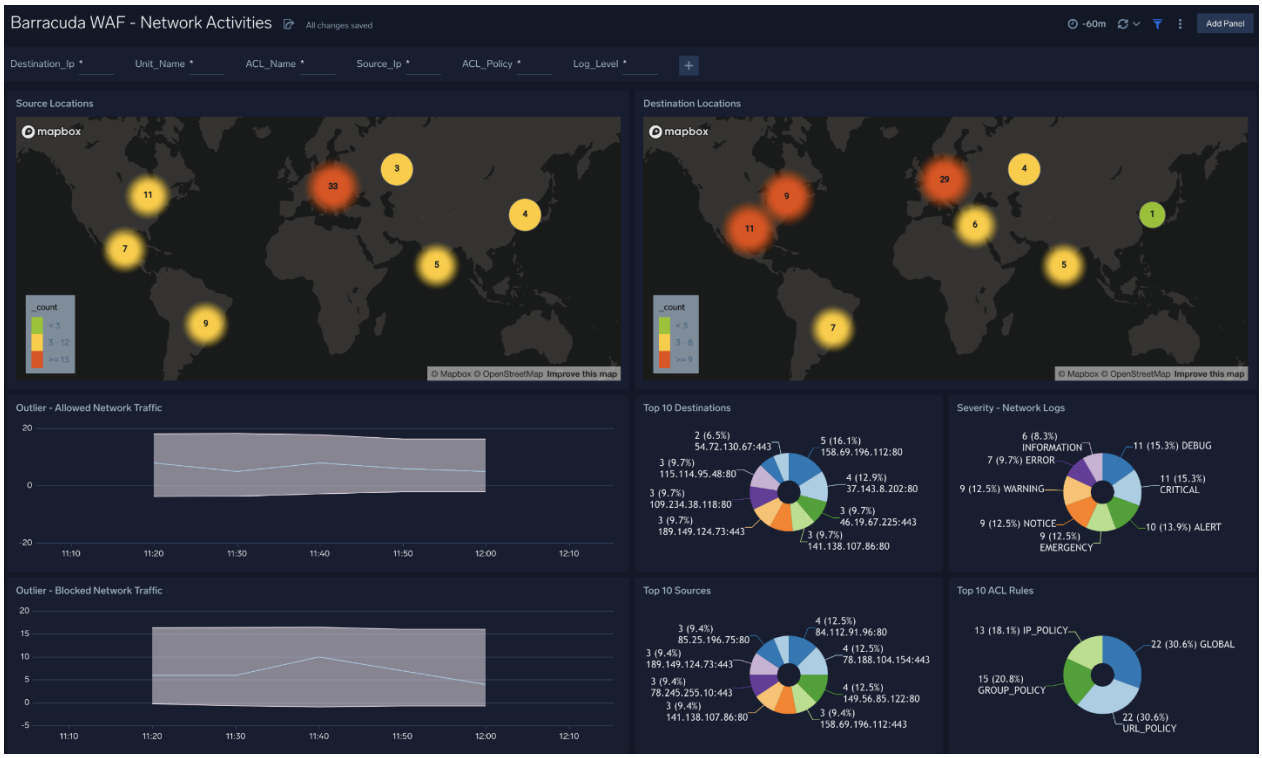


Network Activities

The **Barracuda WAF - Network Activities** dashboard provides insights into blocked/allowed network traffic, source and destination locations, network log level severity and ACL rules.

Use this dashboard to:

- Monitor source and destination traffic locations.
- Monitor the severity of network log messages and unusual allowed and blocked traffic patterns.
- Monitor the top 10 sources, destinations and ACL rules.



Security Overview

The **Barracuda WAF - Security Overview** dashboard provides an at-a-glance view of alerts, WAF rules triggered and attacks detected by both Sumo Logic Threat Intel and Barracuda WAF.

Use this dashboard to:

- Get a high-level overview of your WAF security posture by understanding attack vectors and trends and rules triggered.
- Determine which attack types, sources, and WAF rules that need further investigation.

Threat Analysis

The **Barracuda WAF - Threat Analysis** dashboard provides detailed insights into attacks and rules triggered on the Barracuda WAF.

Use this dashboard to:

- Monitor threats allowed through the WAF and those blocked by the WAF.
- Investigate details of attacks detected by both the WAF and Sumo Logic Threat Intel.
- Fine tune the WAF to prevent future attacks and eliminate false positives.

Traffic Overview

The **Barracuda WAF - Traffic Overview** dashboard provides an at-a-glance view of client geographic locations, performance and cache hit percentage, and unusual behaviours across the number of incoming requests and performance.

Use this dashboard to:

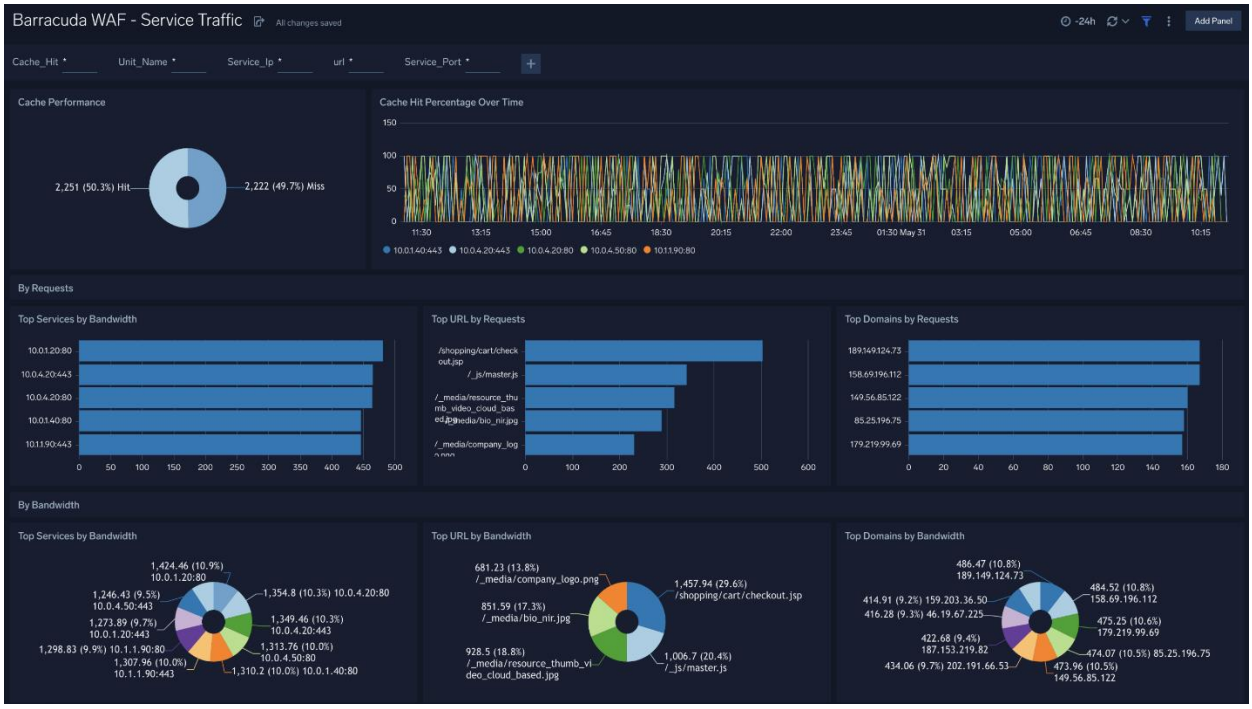
- Monitor requests and performance across services.
- Investigate how to improve performance via cache hit rates.
- Analyze trends for requests and performance by Service IP.
- Monitor client locations.
- Monitor unusual patterns of client/server errors and service performance.

Service Traffic

The **Barracuda WAF - Service Traffic** dashboard provides detailed insight into cache hit performance, request traffic and bandwidth.

Use this dashboard to:

- Monitor trends for cache performance trends.
- Monitor top services, URLs, and domains by both number of requests and bandwidth.
- Improve performance by fine-tuning the cache and other WAF configurations.

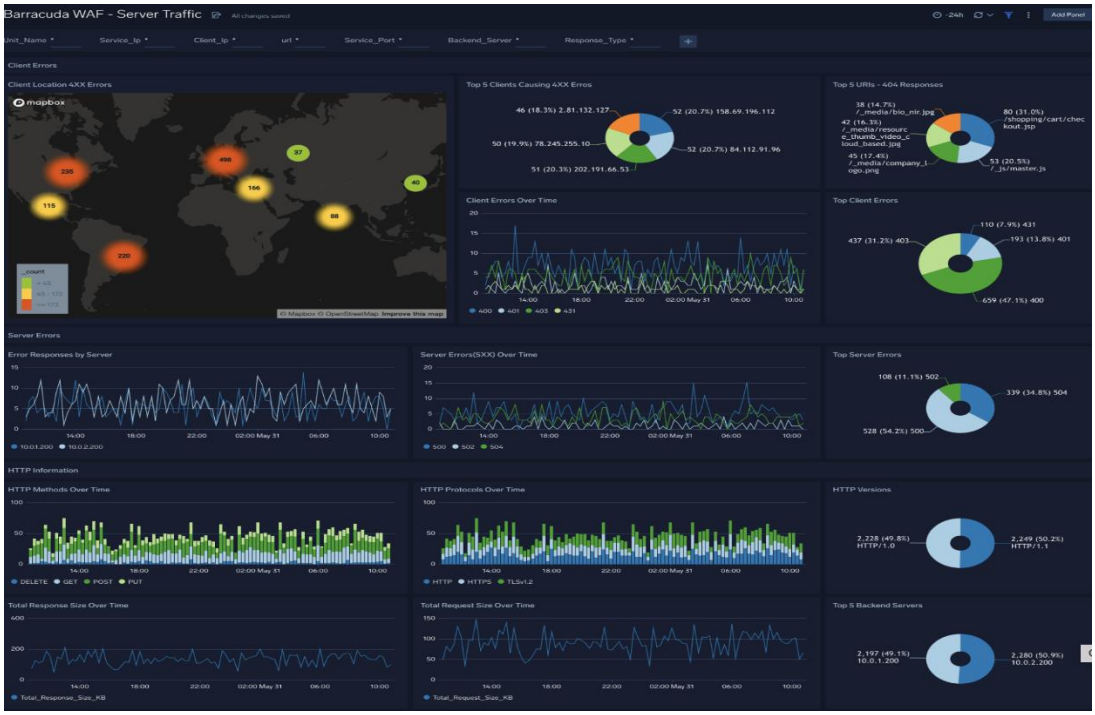


Server Traffic

The **Barracuda WAF - Server Traffic** dashboard provides a detailed information on server traffic, such as client and server errors, and HTTP request and response information. The dashboard is divided into three parts so you can compare client errors, server errors, and HTTP protocol information.

Use this dashboard to:

- Identify trends across client/server errors, requests and responses.
- Identify which clients and servers are responsible for the most errors and use this information to change the WAF configuration.



Client Traffic

The **Barracuda WAF - Client Traffic** dashboard provides detailed information on clients, such as visits by country, user agent, platform, operating system (OS), devices, and top referrers.

Use this dashboard to:

- Monitor incoming web traffic metrics to understand client geographical locations, browsers, and operating systems.
- Determine top clients accessing your web applications and optimize WAF configurations as needed.

Barracuda Web Application Firewall (BWAF): Key Features and Capabilities

The Barracuda Web Application Firewall (BWAF) is designed to protect web applications from various web-based attacks by filtering and monitoring HTTP traffic between the web application and the Internet. It is a robust solution that offers a range of features to ensure the security and performance of web applications. Here are the key features and capabilities of the Barracuda WAF:

Threat Protection

- **OWASP Top 10 Protection:** The BWAF includes protection against the OWASP Top 10 vulnerabilities, which are the most critical web application security risks, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
- **Signature-Based Threat Protection:** It uses a comprehensive set of signatures to detect and block known threats.
- **Anomaly Detection:** The system can detect anomalies in web traffic that might indicate an attack, even if no specific signature is available.
- **Bot Management:** BWAF has mechanisms to identify and control web scraping and other bot activities, which can be harmful to web applications.
- **DDoS Protection:** It offers protection against Distributed Denial of Service (DDoS) attacks that can overload and crash web applications.

Security Policies and Customization

- **Advanced Policy Editor:** BWAF provides a policy editor that enables the creation of complex rules using logical operators, allowing for precise control over which traffic is allowed or blocked.
- **Custom Rule Creation:** Users can create and modify rules to address specific threats or to fine-tune the protection to match their own web application needs.
- **Policy Management:** It includes tools for managing, testing, and deploying security policies across multiple web applications and servers.

Compliance and Reporting

- **Compliance Reporting:** BWAF can generate reports that help organizations meet compliance requirements such as PCI DSS, HIPAA, and others.
- **Detailed Logging and Reporting:** It offers detailed logging and reporting capabilities that can help in forensic analysis and compliance auditing.
- **Security Analytics:** The system provides analytics to help understand the security posture of the web application and trends in attack patterns.

Performance and Scalability

- **Advanced Caching:** BWAF can cache static and dynamic content to improve load times and reduce the load on back-end servers.
- **Content Delivery Network (CDN) Integration:** It can be integrated with a CDN to improve web application performance and availability.
- **Scalability:** The system can scale to handle high volumes of traffic and adapt to growing web application demands.

Ease of Use and Integration

- **User-Friendly Interface:** BWAF features a user-friendly administration interface that makes it easy to configure and manage.
- **API Integration:** It offers API integration capabilities, allowing for automation and integration with other security solutions.
- **Cloud and On-Premises Deployment:** BWAF can be deployed in the cloud or on-premises to meet the specific needs of the organization.

Multi-Tenancy

- **Support for Multiple Web Applications:** BWAF can protect multiple web applications running on the same server or across different servers within the same organization.
- **Isolation and Customization:** Each protected web application can have its own security policies and configurations.

High Availability and Redundancy

- **Load Balancing and Failover:** BWAF supports load balancing and failover to ensure the web application remains accessible and secure even in the event of a system failure.

By combining these features, Barracuda Web Application Firewall provides a comprehensive solution for protecting web applications from a wide range of threats, while also ensuring optimal performance and reliability.

Barracuda Web Application Firewall (BWAF) Use-Case Example Scenario:

Imagine a financial institution, Golden Fin Securities, which operates a critical online trading platform accessible to its customers. This platform handles sensitive information such as personal details, financial transactions, and investment strategies. Given the high value of the data and the potential impact of security breaches, Golden Fin Securities is particularly concerned about web-based attacks, including SQL injection, cross-site scripting (XSS), and distributed denial of service (DDoS) attacks.

Challenges:

Web Application Vulnerabilities: The trading platform, built with a complex codebase, has various vulnerabilities that can be exploited by malevolent actors.

DDoS Attacks: The platform has been experiencing sporadic DDoS attacks, causing service disruptions and financial losses.

Regulatory Compliance: The Company must adhere to strict financial regulations regarding data protection and privacy, which requires robust security measures.

Lack of In-House Expertise: Golden Fin Securities has limited in-house security expertise to manage sophisticated web security challenges.

Solutions:

To address these challenges, Golden Fin Securities decides to deploy the Barracuda Web Application Firewall (BWAF) as a critical component of its security infrastructure.

Advanced Threat Protection: BWAF implements multiple layers of security, including intrusion detection and prevention, to safeguard against common and emerging web application attacks.

DDoS Mitigation: Through BWAF's DDoS protection capabilities, GoldenFin Securities can effectively manage and mitigate DDoS attacks, ensuring service availability and minimizing downtime.

Compliance and Auditing: BWAF supports compliance with industry standards and regulations, offering detailed logs and reports that help in demonstrating adherence to security policies and legal requirements.

Centralized Management and Monitoring: BWAF provides a centralized management console, enabling Golden Fin Securities to easily monitor and manage security policies and configurations, even with limited IT security resources.

Benefits:

Enhanced Security: By deploying BWAF, Golden Fin Securities significantly enhances its web application security, protecting customer data and maintaining trust.

Improved Compliance: The use of BWAF aids in meeting regulatory requirements, reducing the risk of fines and legal issues.

Cost-Effective Solution: BWAF offers a scalable and cost-effective solution compared to building and maintaining an in-house security team and infrastructure.

Operational Efficiency: Centralized management and automated security features reduce the operational burden, allowing the IT team to focus on core business activities.

In summary, the Barracuda Web Application Firewall (BWAF) is a powerful tool that addresses the specific security needs of Golden Fin Securities, providing a robust defence against web threats while also assisting in regulatory compliance. This deployment ensures the integrity and availability of their critical online trading platform.