Barracuda Web Application Firewall
Security and Performance Testing

November 2017

DR170818H

Miercom.com

www.miercom.com

Contents

1.0 Executive Summary

Enterprises use local and public web applications for services and sales. The frequent use of web applications makes them perfect targets for attackers. They use vulnerabilities as doors for hijacking communication sessions. The result is malicious network control or data theft.

Traditional firewalls offer application control but not visibility. A Web Application Firewall (WAF) secures applications against attacks and vulnerabilities which a network firewall cannot.

Barracuda engaged Miercom to confirm security and performance of the Barracuda WAF 960. The product was subjected to exploits, network attacks, data breaches and high-volume traffic. Test results determined the capability and capacity of the web application security solution.

Key Findings of the Barracuda WAF 960

- Detected 100 percent of cross-site scripting; cross-site tracing; SQL injection; system command injection and file inclusion vulnerabilities
- No exposed ports or security weaknesses found
- Alerted of network data breaches during theft attempts
- Outperformed rated HTTP performance at 7.6 Gbps throughput
- Proved nearly 2 Gbps performance for encrypted HTTPS traffic
- Showed excellent performance in connection and transaction handling over HTTP and HTTPS
- Deployed in one hour – from unboxing to full operation
- Offered an easily manageable and detailed reporting interface and useful security and application features

Based on the results of our testing, the Barracuda Web Application Firewall displayed impressive vulnerability detection, robust protection and high performance, earning it the ***Miercom Performance Verified*** award.

Robert Smithers

CEO

Miercom

2.0 Test Summary

Vulnerabilities	
Cross-Site Scripting	Pass; 100% detection
Cross-Site Tracing	Pass; 100% detection
SQL Injection	Pass; 100% detection with latest software update
System Command Injection	Pass; 100% detection with strict protection
File Inclusion	Pass; 100% detection
Management Protocol Protection	Pass
Nmap Port Scan	Pass
Nessus Vulnerability Scan	Pass; no vulnerabilities found
Network Attacks	
Denial-of-Service (DoS)	Pass; 100% detection
Buffer Overflow	Pass; 100% detection
Data Breaches	
Lawful Interception	Pass; for HTTP responses only
Performance	
Maximum Throughput	HTTP – 7,600 Mbps
	HTTPS – 1,958 Mbps
Maximum Connection Rate	HTTP – 69,870 connections/second
	HTTPS – 9,838 connections/second
Maximum Transaction Rate	HTTP – 118,800 transactions/second
	HTTPS – 43,980 transactions/second

3.0 Product Overview

Attackers use vulnerable web applications to perform attacks or data theft. But WAF solutions identify vulnerabilities before they compromise local or remote networks. These attacks, like injection and application-layer DoS, put an entire enterprise at risk.

WAF products should screen threats using positive, or whitelisting, methods. Approved applications pass through the network, and the WAF rejects the rest. This ensures tighter security against external and internal threats.

Not all WAF solutions are the same; some combine application security with DoS or content filtering. Others are better able to integrate with other network security products. The benefits should be the same - detect threats, adapt to the environment, enhance incident response and place minimal effect on performance. Deployment and use should be simple, intuitive and efficient.

Barracuda Web Application Firewall

Source: Barracuda

Model: 964

Firmware: v9.0.0.008

Virus definition: v3.7.0.5197

Attack definition: v1.120

- 2U rackmount
- Supports HTTP/S 0.9/1.0/1.1, FTP/S, XML, IPv4/IPv6/JSON
- Reverse-proxy architecture
- Protects against malware and attacks such as SQL injection and cross-site scripting
- Integrates with vulnerability scanning
- Uses IP-reputation to prevent DoS attacks
- Scans file uploads for viruses
- Provides XML firewall and outbound data theft protection
- Maintains performance with built-in caching, compressing and connection pooling
- Achieves maximum throughput of 7+ Gbps
- Offers system, web firewall, access and audit logging
- Licenses are not restricted to user-based or module-based packages

4.0 How We Did It

Miercom's hands-on testing replicated real-world threat environments, to challenge and provide a realistic assessment of a product's security efficacy and performance.

The Device Under Test (DUT) was subjected to increased loads of application layer traffic, high-level network attacks and breach scenarios to determine the level of proactive security and prevention it provided an enterprise network.

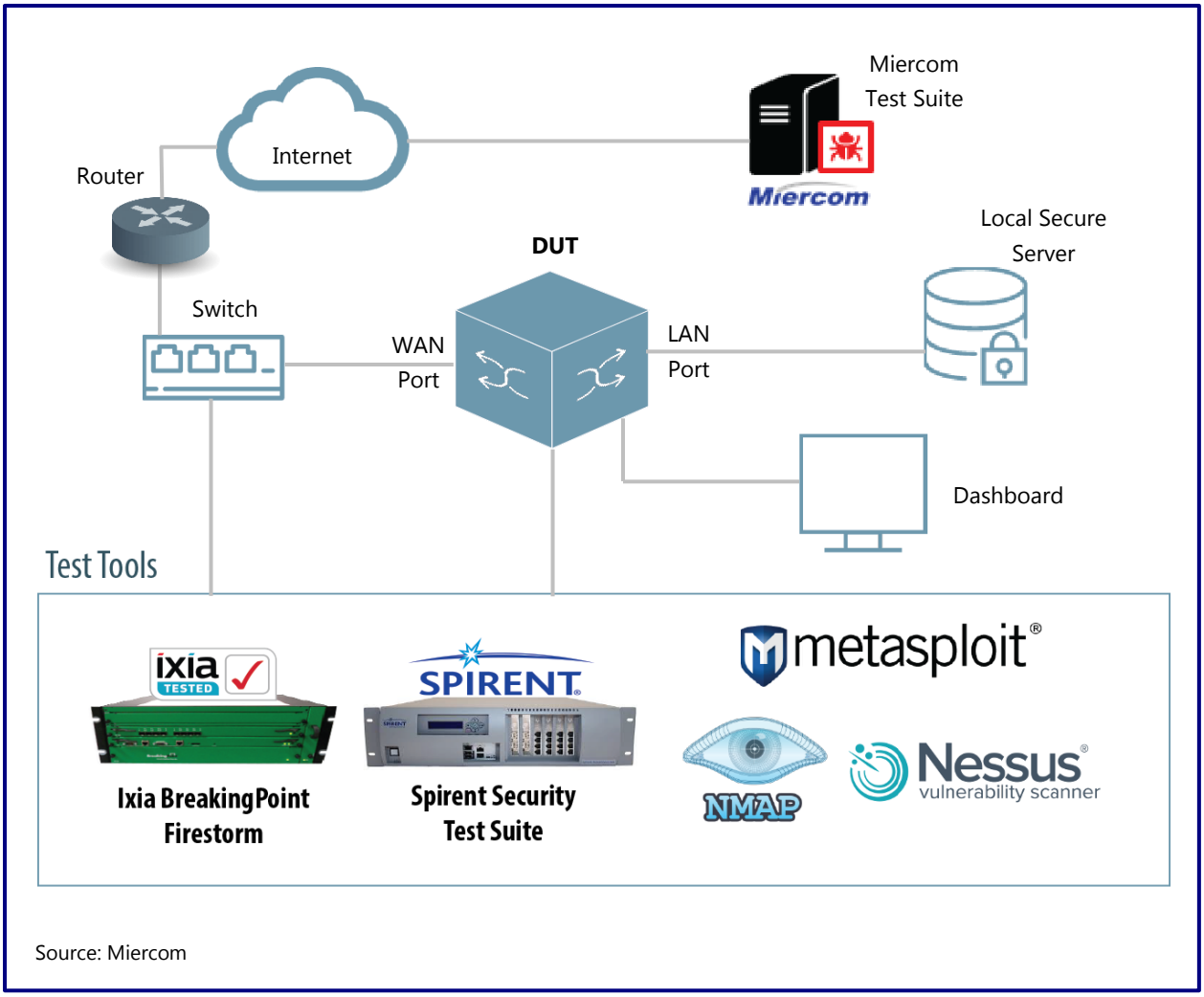
Test Tools

Multiple test tools were used to subject the test network to various attacks.

Source: Miercom

The test tools featured above were used for traffic and threat generation, real-time monitoring and capturing of network activity. Miercom used a unique blend of custom, proprietary attack scripts with globally collected samples to carry out attacks.

Test Bed Diagram



Source: Miercom

The DUT operated in reverse-proxy mode and was configured for 12 servers under the same service with unlimited keep-alive requests. Session timeout varied, depending on the test case. The Ixia BreakingPoint traffic generator enabled HTTP/1.1 and HTTPS/TLS 1.0, with a maximum of 50 concurrent TCP connections per user.

5.0 Security

The following times were tested to evaluate the DUT for its security against multiple web application attack vectors.

5.1 Web Application Vulnerabilities

5.1.1 Cross-Site Scripting (XSS)

Attacks from the browser-side of a website use malicious code injection to gain access to the client's private server. An unwanted HTTP request is inserted into a web application object such as JavaScript, HTML or Flash.

Expected Behavior

The DUT was expected to thoroughly review the web application code to identify vulnerabilities and block sites that grant unauthorized network access.

Results

Cross-Site Scripting Attack	
Barracuda WAF 960	Pass; 100% detected

5.1.2 Cross-Site Tracing

A combination of XSS and Microsoft's TRACE or TRACK methods are used to hijack communications between the client and web application. This attack uses a JavaScript object to steal the user's cookies to gain credentials. These credentials are forwarded to the attacker's webserver for unauthorized access and control of the end point.

Expected Behavior

The DUT should find vulnerabilities in the web application code that make this type of attack scenario possible.

Results

Cross-Site Tracing Attack	
Barracuda WAF 960	Pass; 100% detected

5.1.3 SQL Injection

The SQL query injection between the client and web application can result in direct database access and manipulation. An attacker can perform spoofing, tamper with data or transactions or gain administrative control.

Expected Behavior

The DUT was expected to thoroughly review the web application code to identify vulnerabilities and block sites that grant unauthorized network access.

Results

SQL Injection Attack	
Barracuda WAF 960	Pass • 100% detected with latest software update to the default settings

5.1.4 System Command Injection

This attack uses vulnerable web applications to command the host operating system. Exposed cookies or other data stored in applications create a trail to the system shell. With administrative privilege, the attacker can then infiltrate the network.

Expected Behavior

The DUT should secure such an application vulnerability to prevent unauthorized access.

Results

System Command Injection Attack	
Barracuda WAF 960	Pass • 100% detected when System Command Injection protection was enabled; with a stricter setting, this vulnerability detection mechanism performed significantly better than its default setting

5.1.5 File Inclusion

An attacker can insert arbitrary, local or remote files by exploiting application-level code. Once downloaded, this can lead to XSS execution, DoS attacks or data breaches on the client or server side.

Expected Behavior

The DUT should assess any invalid file indexing to ensure no attack surface is available for manipulation.

Results

File Inclusion Attack	
Barracuda WAF 960	Pass; 100% detected

5.1.6 Management Protocol Protection

Enabled FTP and Telnet leave the management interface vulnerable to remote access. These insecure methods allow malicious web scripts upload (FTP) and exposed passwords (Telnet).

Expected Behavior

The DUT should have FTP and Telnet disabled by default. More secure protocols such as SSH, IPSec, SFTP should be available.

Results

Management Protocol Vulnerability	
Barracuda WAF 960	Pass • Can manually set up FTP, if desired • Telnet port is not open

5.1.7 Nmap Port Scan

Nmap attempts to request responses from active IPs and open ports. Using a database of over 2,200 known services to correspond to ports (e.g. SMTP, HTTP), it scans for vulnerabilities.

Expected Behavior

The DUT should have no ports visible from outside the local network, so attackers cannot listen in on or penetrate the network.

Results

Nmap Port Scan Vulnerability	
Barracuda WAF 960	Pass; no open ports found. Port 80 was open for standard traffic purposes.

5.1.8 Nessus Vulnerability Scan

Nessus scans for vulnerabilities on IPv4, IPv6 and hybrid networks. It identifies missing system patches, faulty device configurations, and poor cloud application configurations.

Expected Behavior

The DUT should have no exploitable points of entry.

Results

Nessus Vulnerability Scan	
Barracuda WAF 960	Pass • No vulnerabilities found • Gives information only

5.2 Network Attacks

5.2.1 Denial-of-Service (DoS) Attacks

DoS attacks use floods of traffic to overwhelm the system and cause failure to process data. This leaves the network vulnerable to threats and unauthorized access. The following types of attacks were used:

- High packet traffic load (data and control plane)
- ICMP flood (Layer 3)
- UDP flood (Layer 4)
- TCP flood (Layer 4)
- HTTP flood (Layer 7)

Expected Behavior

The DUT should have bandwidth-limiting capabilities on different network layers and protocols. No DoS attacks should allow penetration or threats from an untrusted source.

Results

DoS Attacks	
Barracuda WAF 960	Pass; 100% detected

5.2.2 Buffer Overflow

Floods of HTTP, HTTPS and FTP traffic are generated to determine bandwidth capacity and resiliency of the DUT. The memory and processing of the DUT can only handle so much traffic before failure occurs, leaving the network vulnerable to attack.

Expected Behavior

The DUT should have a threshold for unwanted connections to prevent system failure vulnerability.

Results

Buffer Overflow Attack	
Barracuda WAF 960	Pass; 100% detected

5.3 Data Breaches

5.3.1 Lawful Interception

A network breach exposes personal or sensitive data that can have devastating consequences. Attackers may hold this data to secure a ransom or use for other malicious purposes. Examples of sensitive data include: credit card numbers, social security numbers and intellectual property. Using files with this information, we tested the DUT for lawful interception.

Expected Behavior

The DUT should block all breach attempts and notify the administrator.

Results

Lawful Interception	
Barracuda WAF 960	Pass • Identified HTML responses in HTTP/HTTPS connections • Generic credit card and social security numbers were detected

6.0 Performance

When introducing security to a network, it is expected that traffic policing and processing will degrade performance. This impact is dependent on many factors such as load conditions, protocols used and encryption. Regardless, the WAF should aim to protect the network by monitoring HTTP and HTTPS traffic for suspicious activity while upholding a realistic throughput.

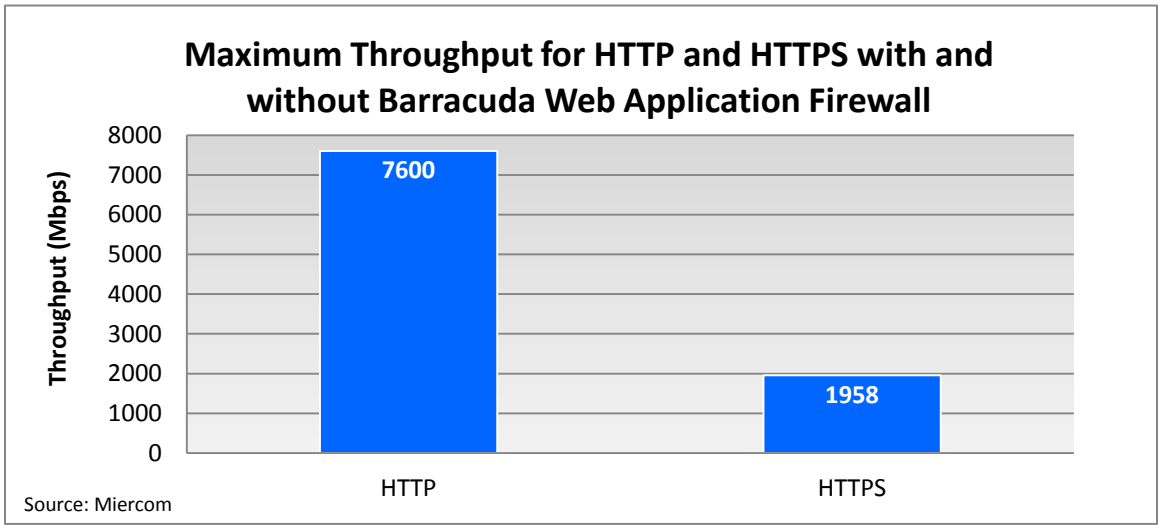
6.1 Maximum Throughput

The rated throughput of the WAF 960 is 5 Gbps. To test this, the network was assessed for the maximum achievable throughput, in megabits per second (Mbps), with the DUT deployed to determine the impact of security on traffic processing. A 1 MB file was transferred between simulated end points using HTTP/1.1 and HTTPS/TLS 1.0. Traffic was increased gradually, maintaining 100 percent successful transactions, until packets began to drop. The test was terminated at the first transaction failure, and the maximum throughput was recorded.

Expected Behavior

The DUT was expected to process 5 Gbps or greater while transferring files via HTTP between simulated end points.

Results



The Barracuda WAF 960 model datasheet performance was 7+ Gbps and proved this 7.6 Gbps throughput over HTTP. As expected, HTTPS throughput was lower, at a little less than 2 Gbps.

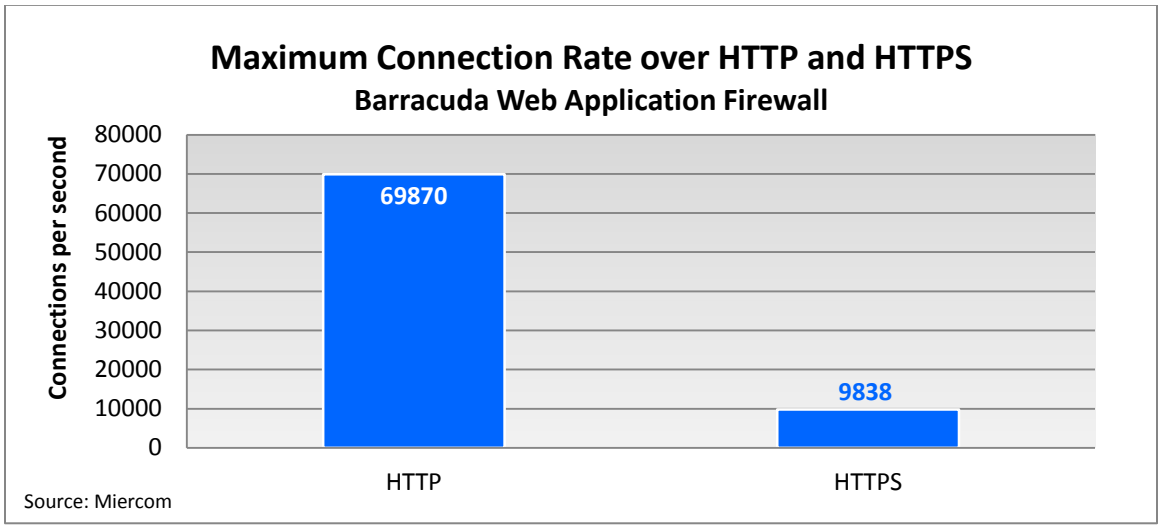
6.2 Maximum Connection Rate

The maximum number of concurrent connections shows the capacity of the DUT to handle simultaneous, open TCP/IP sockets. The connection rate, in connections per second (cps), reflects the ability of the DUT to open and close connections after a 1 KB file has been transferred between endpoints with a 60 second session time out. HTTP/1.1 and HTTPS/TLS 1.0 requested 1 GET request per connection for 50 concurrent connections per user.

Expected Behavior

The DUT was expected to handle at least 65,000 cps over HTTP.

Results



The Barracuda WAF 960 was expected to have a connection rate of 65,000 cps over HTTP. It outperformed its datasheet performance by almost 5,000 cps. Over HTTPS, its connection rate was much less, at 9,838 cps.

6.3 Maximum Transaction Rate

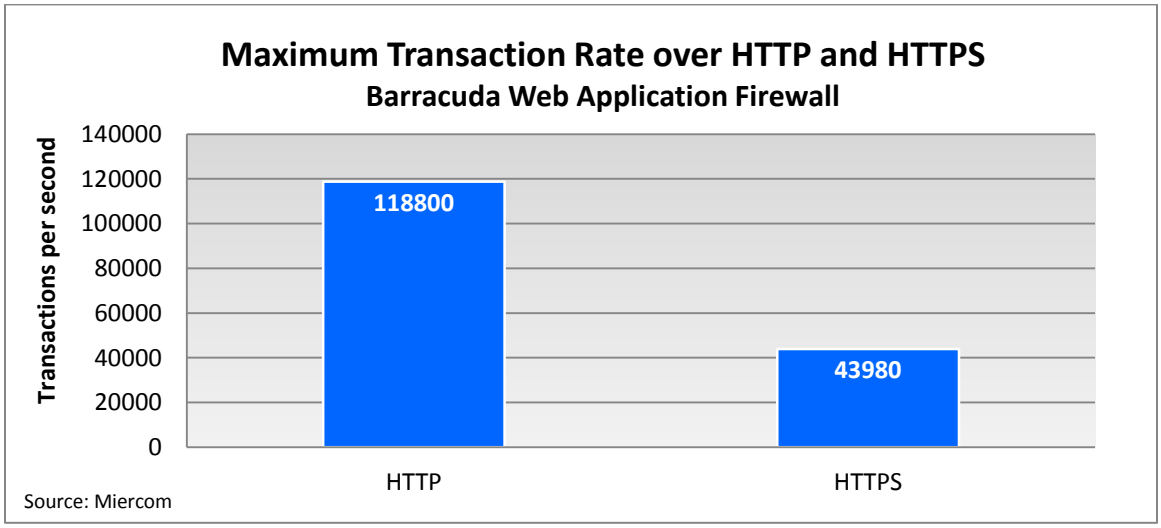
The maximum number of transactions is the capacity of the DUT to open a connection, send multiple requests and close a connection. Unlike maximum connection rate, all sockets remain open until the transactions are complete between client and server.

The payload size used was a 1 KB random binary file. HTTP/1.1 and HTTPS/TLS 1.0 requested 10 GET requests within the same established TCP connection from client to server.

Expected Behavior

The DUT was expected to reach a maximum rate of transactions per second while delivering a 1 KB binary file payload over HTTP and HTTPS.

Results



The Barracuda WAF achieved a transaction rate of 118,800 transactions per second over HTTP and 43,980 transactions per second over HTTPS.

7.0 User Experience

7.1 Deployment and Configuration

The DUT was deployed with the default policy for each test. No policy was manipulated for performance or security optimization; it was tested as-is. But a customer does have the ability to change these settings to fit their needs. Deployment requires only LAN/WAN and service setup. All web servers were set up in the DUT local network.

Deployment was completed in approximately one hour. The time was recorded from DUT unboxing to full-operation mode.

The service was set up with a virtual IP address within the same WAN interface subnet. All security policies used the default settings. Ports 80 and 443 were selected for HTTP and HTTPS, respectively.

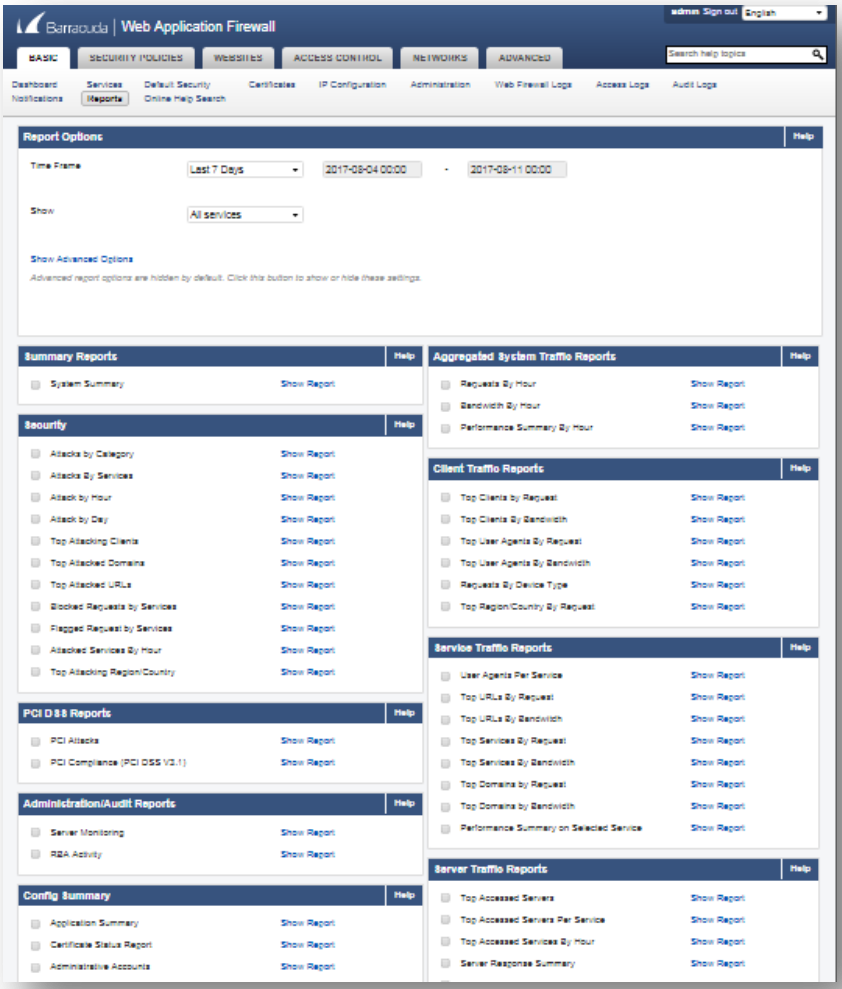
7.2 Management and Reporting

7.2.1 Active Logging

The dashboard shows traffic status, active threat summaries and resource usage (CPU, memory). The access log, audit log and notifications were found under the Basic tab. The Access Log shows all the requests sent to the server, client IP addresses and request methods.

7.2.2 Reporting

Reporting was also found under the Basic tab. A report was generated with a variety of options: summary, security, system traffic, client traffic and configuration summary. This report could be downloaded in HTML or PDF format, or it was delivered through email or FTP. The Frequency of Delivery could be set to a daily, weekly or monthly basis.



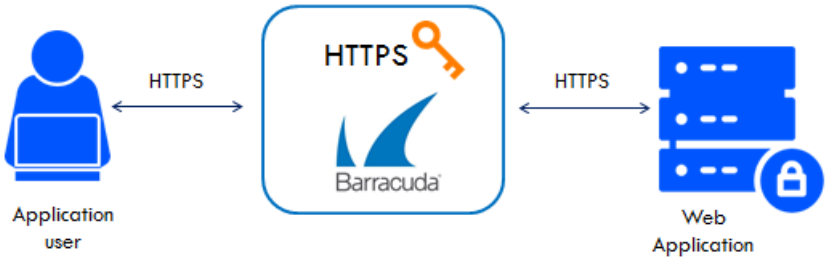
Reporting was organized, clear and concise for easy remediation.

7.3 Security Features

Barracuda offers many security features that benefit both the application and network against attackers and vulnerabilities. Miercom verified the functionality of these features by observing live attacks and real-time WAF responses.

7.3.1 SSL Features

Secure Socket Layer (SSL) cryptography can be enabled by importing public certificates. Inbound traffic from the public network is encrypted, but data going to the backend is not. SSL sessions are terminated at the WAF.



Source: Miercom

Certificates are stored on the WAF. Using the SSL feature, an RSA certificate can be issued and named. There is also the option to disable certain protocols that are no longer considered the most secure (SSL 3.0, TLS 1.0), but some networks may keep these enabled for legacy reasons.

While the administrator can choose a custom cipher, the Barracuda WAF by default chooses the most secure by negotiating with the client.

Perfect Forward Secrecy

Another part of the SSL feature is Perfect Forward Secrecy where an SSL key is renegotiated for every SSL/TLS session to ensure that encrypted communication cannot later be decrypted if the private key has been compromised. If an attacker has a packet capture and a private key, they can listen to all traffic on the port. But with a cipher, data is unable to be read due to the constant regeneration of the public-private key pair. This is especially useful against Man-in-the-Middle attacks or general compliance and security situations. Cipher suits can be configured and customized.

Source: Miercom

Server Name Indication (SNI)

SNI extends the SSL/TLS protocol to solve the issue of hosting multiple domains on the same IP address. Each domain has a distinct SSL certificate, so the Real Server needs to select the proper certificate for each domain. This occurs with public cloud platforms where there is a limitation on automatic use of public IPs. To have an application and WAF using a single interface with one IP address is challenging when each application has its own individual certification. SNI binds different certificates for different domains to resolve this issue.

The virtual domain information is sent as part of the SSL/TLS negotiation between the client and server. Clients supporting the extension send the domain name when initializing a secure SSL session. The server looks at the domain name and sends the corresponding certificate to the client. SNI certificate binding is applicable to HTTPS only.

7.3.2 Action Policy

The Action Policy feature is a collection of settings that decide what action will be taken in the event of a violation. It consists of attack groups and their associated actions. The attack action specifies the WAF response for a particular type of web attack.

7.3.3 URL Policies

URL policies are automatically created for each service, and additional policies can be created for any part of the application. Such policies cover data theft prevention, brute force prevention, antivirus and rate control.

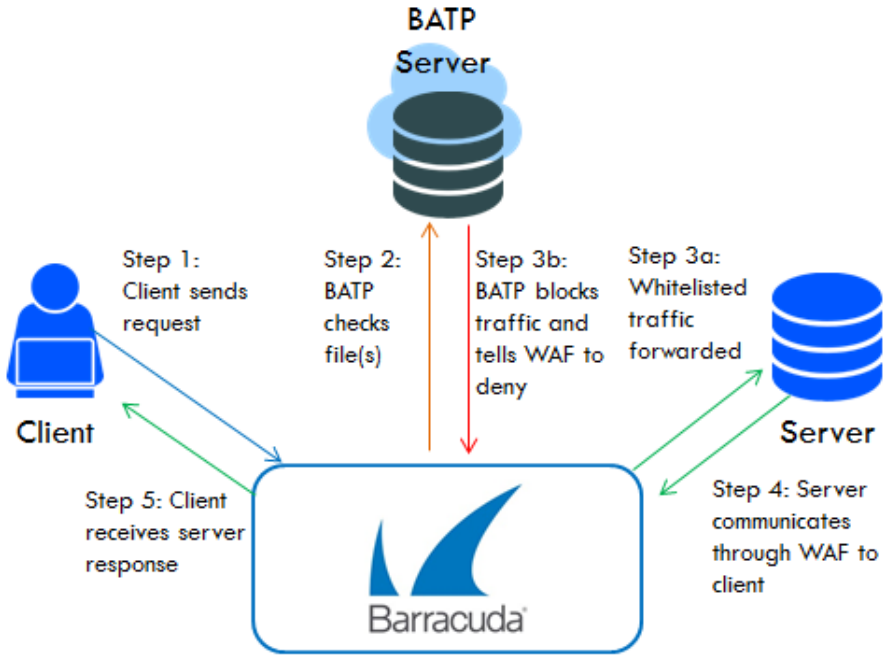
Antivirus

Virus scanning is performed on a per-URL basis for file uploads and downloads. File signatures are created and pushed through updates.

Source: Miercom

Barracuda Advanced Threat Protection (BATP)

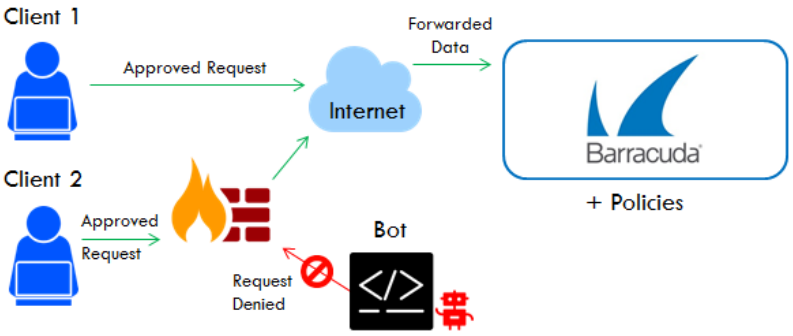
The Barracuda WAF integrates with BATP to provide a hardened defense against the toughest malware and advanced attacks. The cloud-based BATP service uses multiple techniques to scan files, checking for anomalies. All scans are logged in filterable firewall and system logs. Files are each checked for whitelisted content. If the policy allows, the application traffic is forwarded to the server. Otherwise, it is sent to the BATP server and recommended to be quarantined until the scan determines whether the file should be allowed or denied.



Source: Miercom

7.3.4 Bot Attack Protection

Web scraping remotely extracts data from websites using bots and stores the stolen information to a database. The Barracuda WAF determines if requests are coming from legitimate users or a non-browser client, like bots or fake search engines. Honey traps and bot detection triggers, such as inserted hidden links or JavaScript, are used to trick the bot script.



Source: Miercom

The first response should be normal, but the second response is a challenge that the bot is expected to correctly answer to gain access. If the Barracuda WAF does not receive the appropriate challenge response, the request is assumed to be coming from a bot and access is denied.

```
* Connection #0 to host web2.selahcloud.in left intact
<a hidden href="/-cusAgvGLL14biR4qVRCUW9Dsywa9KaYJMHSGITtjcs=.html">-cus
ext/javascript">var _0xcaad=["indexOf","; path=/","cookie","=","x-bni-ja
function indexOfString(_0x1ce0x3,_0x1ce0x4){return _0x1ce0x3[_0xcaad[0]]
lce0x6){var _0x1ce0x7=1558105393;var _0x1ce0x8=1185076615;var _0x1ce0x9=
xcaad[3]+_0x1ce0x9}function set_answer_cookie(){setCookie(_0xcaad[4])}fu
ng(err[_0xcaad[5]],_0xcaad[6])> -1)||(!(navigator[_0xcaad[7]] instanceof
ument[_0xcaad[9]]=set_answer_cookie_1()}</script></html>8
*   Trying 34.215.235.169...
* TCP_NODELAY set
* Connected to web2.selahcloud.in (34.215.235.169) port 80 (#0)
> GET /dvwa/setup.php HTTP/1.1
> Host: web2.selahcloud.in
> User-Agent: curl/7.54.0
> Accept: */*
>
```

The first response is normal, but the second response shown above includes hidden JavaScript. The bot will unknowingly request from that link as well. It opens a new page giving an error with an ID.

The administrator can use this ID in the WAF log to see the bot which triggered this error has been blocked.

7.3.5 Application DoS

DoS attacks via web applications consume all available resources and make the application unavailable to its users – denying them service. These attacks are typically accomplished using traffic flooding to the target application, or large loads of requests from many sources to prevent legitimate traffic from reaching the application server.

Like with web scraping, the Barracuda WAF looks for suspicious clients and validates incoming users. It can similarly insert hidden links or JavaScript to elicit a challenge response from the suspected attack source. The WAF includes a library of Captcha challenges (available through its response-validation security policies) which the requester is expected to answer correctly.

While Captcha images are stored in the WAF product itself, the HTML of the challenge page is customizable, if for instance a company logo is desired. A legitimate request requires the end user to submit the correct letters or numbers in the Captcha image. But a malicious script cannot pass this challenge and is successfully prevented from tampering with the network. The WAF assumes the non-validated incoming requests originate from a bot or web crawler.

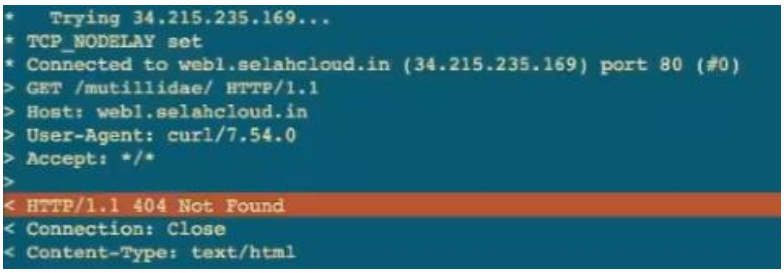
Administrators can configure a Distributed DoS (DDoS) policy to issue CAPTCHAs to all clients who access a URL space, or to clients with suspicious profiles.

7.3.6 Brute Force Prevention

A brute force attack technique explores unknown values, such as login credentials, by systematically trying vast amounts of key combinations to gain access to the targeted resource. The Barracuda WAF offers advanced security configurations for handling inbound traffic during these attacks. A count window allows a limited number of seconds for connections to be made. A maximum allowed access number limits incoming connections. Once either of the thresholds is reached, the Barracuda WAF presents the user with a CAPTCHA image to prove they are humans. If the challenge is not answered correctly, it is considered a brute force attack. Alternatively, a violated access policy may result in the user being locked out for a custom time period.

Source: Miercom

The URL of the target, such as a gated URL for logins, can be specified for protection. After the limit of responses is met, those requests over TCP are processed, but HTTP requests receive a 404 Error or a customized response. Action policies can be created and customized.



TCP connections are made, but application layer HTTP request receives a "404 Not Found" error response.

All brute force attacks are prevented, logged, incite a response and, if chosen, a follow-up action to block the IP altogether. The WAF identifies clients who violate brute force policies and pushes these updates to the network firewall, blocking connections for this IP address.

7.3.7 Profiles

During security efficacy testing, the security policies were used to enable or disable patterns, such as service level features like OS command injection. This configuration change is reflected on the overall service. But if the customer prefers to have a single URL exception while upholding an OS command injection policy, this can be whitelisted using a Profile.

What an administrator cannot do with a security policy, can be done with a Profile. There are many options available in a profile to configure parameters based on type or class.

An example is a form may have an input parameter (string) for the name and selection parameter (session choice) for choosing gender. Threats may come in the form of scripts during the form filling process that need to be detected by using pattern recognition assignments. The ever-changing use of applications can be difficult for an administrator to constantly update profiles manually. The Barracuda WAF offers a Start Learning feature for auto-profiling creation.

URL Profiling

A URL profile lists allowed fields, like HTTP methods, names and parameter types, query strings and length-based restrictions.

Parameter Profiling

A parameter profile defines the allowed format for each parameter, using either a negative or positive security model. It also includes length-based restrictions.

Adaptive Profiling Configuration

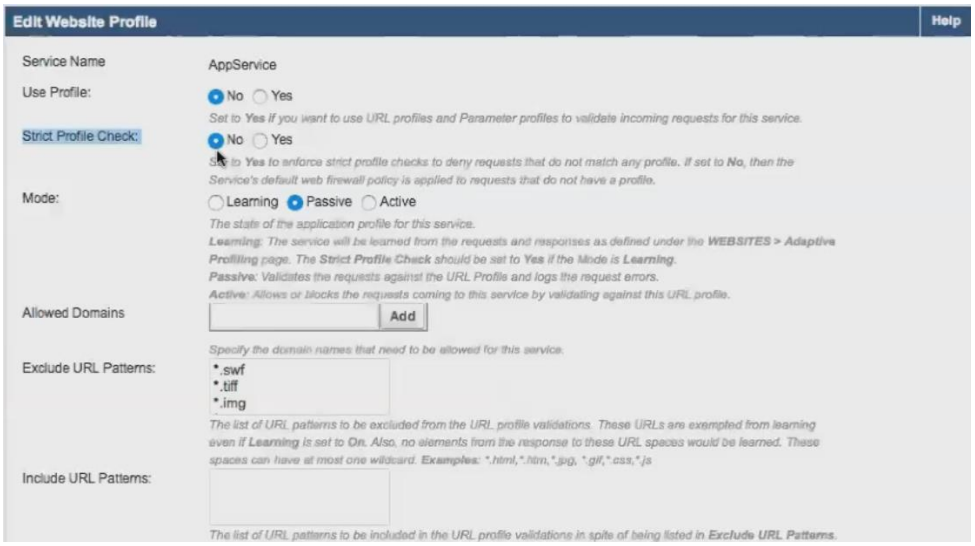
The service can be configured in Learning mode. URL profiles can be reviewed and locked, if opted. The adaptive profiling works by monitoring successful requests or responses. This feature is useful for users who want site traffic rules based on site structure.

Profile Modes

Profiles can be either actively or passively enabled. Active profiles validate requests, block and log request violations. These profiles directly use URL profile or parameter profile settings set by the administrator, or learned through adaptive profiling. Passive profiles only validate requests and log violations; no blocking is administered.

7.3.8 Positive and Negative Security Model of Configuration

Strict Profile Checks can be enabled or disabled, depending on whether the administrator prefers a positive or negative security model. Enabled Strict Profile Check validates requests and denies any that do not match the URL and parameter profiles. Without it, validated requests are checked using the global security policy.



By selecting "No" for the Strict Profile Check, all requests are screened using the global security policy.

Positive Security Model

This model ensures that the default network firewall does not allow any incoming traffic, except for what is required – or whitelisted. This is a strict form of security that tends to be overly complex to both configure and maintain. It opens the door for false positives, or legitimate requests that have been erroneously flagged as malicious and denied a connection.

Negative Security Model

This model blocks only specific patterns, but all other traffic is allowed to pass through the firewall. This type of security is not as complex as the positive model. However, any attacks that haven't been profiled will gain access to the network and may result in an attack.

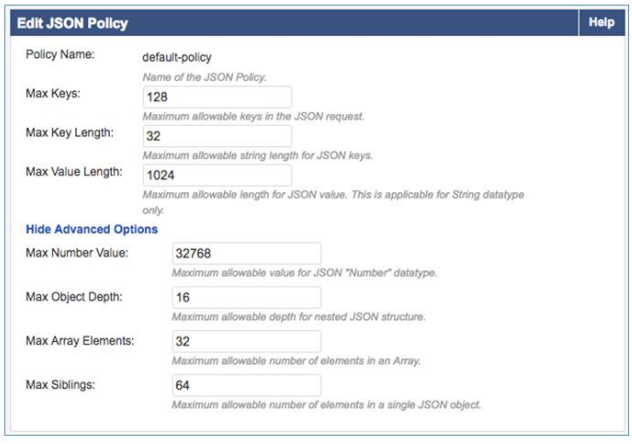
7.3.9 URL Encryption

The Barracuda WAF encrypts all URLs associated with the requested page without making changes to the application itself. Any encrypted URLs that have been tampered with are automatically blocked and logged.

7.3.10 API Security

Many applications, including mobile, exchange data using JSON (RFC 4627). This protocol is a lightweight data-interchange format but very vulnerable to attacks, such as improperly formatted data or embedded attacks. It is important for applications using JSON to validate inputs before processing. The Barracuda WAF offers JSON Security and XML Validation, for XML-based APIs. Both ensure attacks are not tunneled inside HTTP requests with JSON content.

The following protection is available through Barracuda WAF through JSON payload profiling.



Source: Barracuda

7.4 Application Delivery Features

7.4.1 Load Balancing

The Barracuda WAF can act as a standalone load balancer or work in conjunction with other load balancers. This feature is supported for all types of applications.

7.4.2 Caching

Caching stores commonly used information in local memory for quick retrieval. This reduces repeated requests for the same information. Such information includes web pages, graphics files and other objects. This can dramatically improve performance and reliability.

Caching requirements of an application can be offloaded to the Barracuda WAF to enable:

- Reduced latency when retrieving web content
- Reduced bandwidth and server load
- Automatic identification and replication of site content

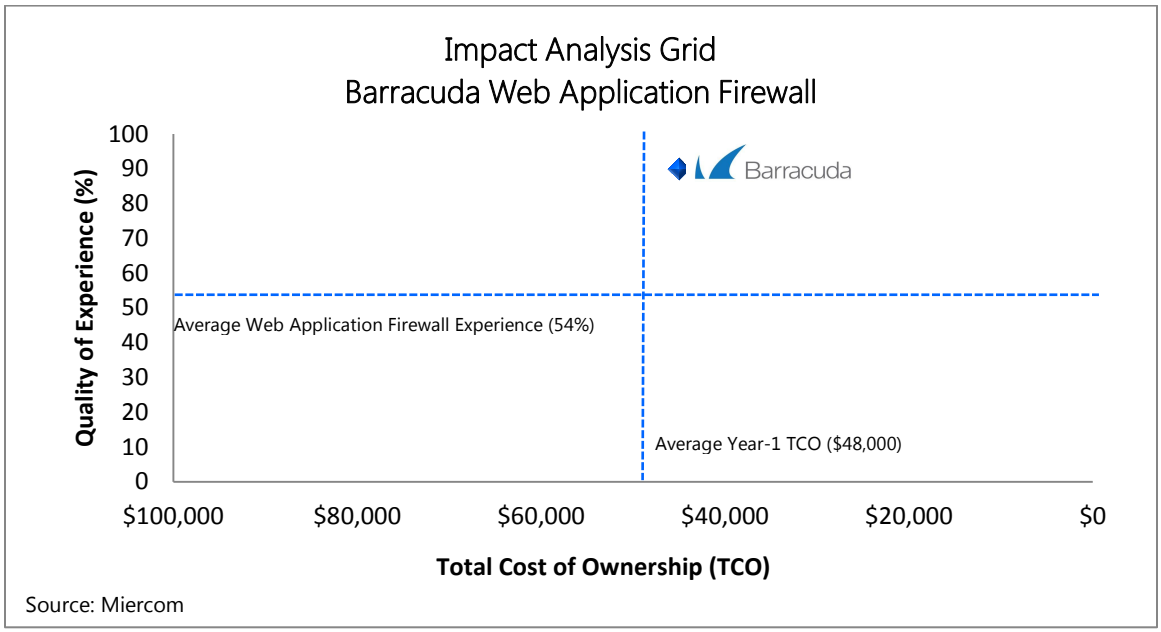
7.4.3 Compression

Compression improves response time for clients by reducing the quantity of transferred data. Web pages using HTML, JavaScript, Java and other text-based languages can be compressed to improve traffic management and reduce download time. The Barracuda WAF can apply compression for all, or specific, client requests that match Content Rules. Enabling compression as a service applies compression to all service requests.

8.0 Total Cost of Ownership

Miercom compares products using its Impact Analysis Grid. The Quality of Experience (QoE) is in percent, and weighed against the Total Cost of Ownership (TCO).

Real-world observations during customer deployment, IT installment and engineering development determined QoE. TCO was the average first-year cost of product and updates, based on several sources. Our proprietary formula calculated the weighted average to reflect the true product value. For example - an expensive product, with all benefits considered, has higher value than a low-cost, low-benefit competitor.



Source: Miercom

Many factors contribute to benefit the QoE (y-axis) of each product. Such factors include detection efficacy, ease of deployment, setup and use. Additionally, business practices and legal restriction play a role. While subjective, the numbers of hits and misses contribute to an unbiased rating.

The TCO (x-axis) is a range of costs, based on deductions from, or credits towards, the actual listed pricing. The following determine cost weight: training, maintenance, upgrades, support, licensing and legal restrictions.

The top-right quadrant is ideal, as it features low cost with high QoE. The next best quadrant depends on the customer needs - low cost or high efficiency? Depending on the size, cost may not be a concern. The bottom two quadrants are far from ideal. The worst is the bottom left; it has a high price for low QoE.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.