LOGZILLA DOCUMENTATION

Barracuda Networks

Rules, dashboards, and triggers for Barracuda Web Security Gateway with MITRE ATT&CK mapping

LogZilla App Store · Generated June 12, 2026 · logzilla.ai/docs/logzilla-appstore/barracuda

Overview

Barracuda Web Security Gateway is a web security appliance that provides advanced threat protection for organizations. The gateway functions as a web proxy server that inspects HTTP and HTTPS traffic, blocking malware, viruses, spyware, and malicious websites while enforcing web usage policies.

App Function

- Parse Barracuda Web Security Gateway syslog messages
- Extract metadata tags for filtering and analysis
- Categorize events by action (ALLOWED, BLOCKED, DETECTED)
- Provide dashboards for monitoring web traffic and threats
- Alert on blocked requests, virus detection, and spyware detection

Vendor Documentation

- Syslog and the Barracuda Web Security Gateway (https://campus.barracuda.com/product/websecuritygateway/doc/6160435/syslog-and-the-barracuda-web-security-gateway/)

Device Configuration

Configure the Barracuda Web Security Gateway to send syslog messages to LogZilla:

Log in to the Barracuda Web Security Gateway admin interface
Navigate to **Advanced** > **Syslog**
Enable syslog logging
Enter the LogZilla server IP address
Select the appropriate facility and severity levels
Save the configuration

Verification

Generate test traffic by browsing to a website, then verify events appear in LogZilla with the program name `http_scan` and `Vendor` tag set to `Barracuda`.

Incoming Log Format

Barracuda logs use a fixed-format with space-separated fields:

```
timestamp version srcip dstip content_type proxy_ip url bytes BYF action
reason ... match_domain category user referrer_url referrer_domain
referrer_category flag
```

Parsed Metadata Fields

Global Tags

Tag	Example	Description
`Vendor`	`Barracuda`	Vendor identifier for cross-vendor filtering
`Event Class`	`security`	Cross-vendor event classification

Standardized Tags

Tag	Example	Description
`SrcIP`	`192.168.1.100`	Source IP address
`DstIP`	`93.184.216.34`	Destination IP address
`Action`	`ALLOWED`	Action taken (ALLOWED, BLOCKED, DETECTED)
`User`	`jsmith@company.com`	User information

Barracuda-Specific Tags

Tag	Example	Description
`Barracuda Reason`	`CLEAN`	Reason for action (CLEAN, VIRUS, SPYWARE)

Tag	Example	Description
Barracuda Spyware	Eicar-Test-Signature	Spyware identifier if detected
Barracuda Policy Match	malware.com	Domain that matched a policy rule
Barracuda Category	adult,porn	Content category that matched
Barracuda Referrer Category	news	Category of the referrer URL

Log Examples

Clean Traffic Allowed

```
1158710819 1 11.22.33.44 55.66.77.88 image/gif 10.1.1.8
http://i.cnn.net/cnn/.element/img/1.3/video/tab.middle.on.gif 1744 BYF
ALLOWED CLEAN 2 0 0 0 0 - 0 - 0 - 0 cnn.net news ANON http://www.cnn.com
www.cnn.com news 1
```

Virus Blocked

```
1158710880 1 11.22.33.44 127.0.0.1 - 11.22.33.44
http://www.eicar.org/download/eicar.com.txt 0 BYF BLOCKED VIRUS
stream=>Eicar-Test-Signature FOUND 2 0 0 0 0 - 0 - 0 - 0 eicar.org
computing-technology ANON http://www.somedomain.com/index.html somedomain.com
news 0
```

MITRE ATT&CK Mapping

Event	MITRE Technique	Tactic
Virus detected	T1204 (User Execution)	Execution
Spyware detected	T1189 (Drive-by Compromise)	Initial Access

Triggers

Trigger	Description
`Barracuda: MITRE ATT&CK Threat Detected`	Any MITRE-mapped threat
`Barracuda: Virus Detected`	Virus detected in traffic
`Barracuda: Spyware Detected`	Spyware detected in traffic
`Barracuda: Adult Content`	Adult content category accessed
`Barracuda: Blocked Request`	Request blocked by the gateway