Integration with the Barracuda Advanced Threat Protection

https://campus.barracuda.com/doc/73699152/

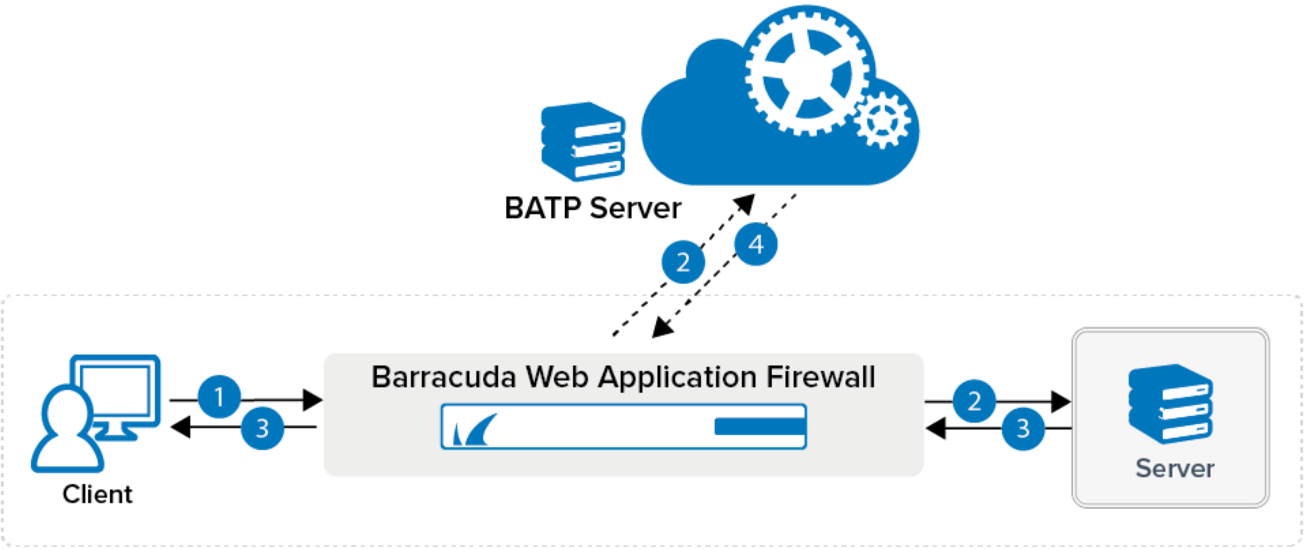
The Barracuda Advanced Threat Protection (BATP) is a cloud-based service that provides in-depth defense against ransomware, malware, and advanced cyber attacks. The Barracuda Web Application Firewall integrates with the Barracuda Advanced Threat Protection (BATP) to scan all files uploaded using POST method requests with encoding type multipart/form-data. BATP scans the files with multiple malware scanners that utilize different types of detection techniques to check for anomalies in the uploaded files and provides defense against zero day attacks. When a file is uploaded, the Barracuda Web Application Firewall processes the request and uploads the file to the server, while the BATP performs the scan and logs the details in the **BASIC > Web Firewall Logs** page. To view BATP logs in the **BASIC > Web Firewall Logs** page, use the **BATP Scan** keyword and filter the logs.

The BATP logs are also displayed in the **ADVANCED > System Logs** page with limited information such as file name, host, and URL.

The maximum size of the file that the BATP can scan is 10MB.

Barracuda Advanced Threat Protection (BATP) is a separate license that needs to be purchased from Barracuda Networks.

Scanning Process in the Barracuda Advanced Threat Protection



1. Client uploads a file as multipart/form-data in a request.

2. The Barracuda Web Application Firewall checks for the file extension/content-type and if the content-type matches the allowed policy, the file is sent to the server. If the content matches any of the MIME types listed below, the file is also sent to the BATP server.

- application/pdf
- application/msword
- application/vnd.ms-powerpoint
- application/vnd.ms-excel
- application/x-msaccess
- application/vnd.openxmlformats-officedocument.presentationml.presentation
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
- application/vnd.ms-cab-compressed
- application/vnd.microsoft.portable-executable
- application/vnd.openxmlformats-officedocument.wordprocessingml.document
- application/rtf

2. The server sends the response after processing the request.

> Barracuda Networks recommends quarantining all files until the BATP scan results are received.

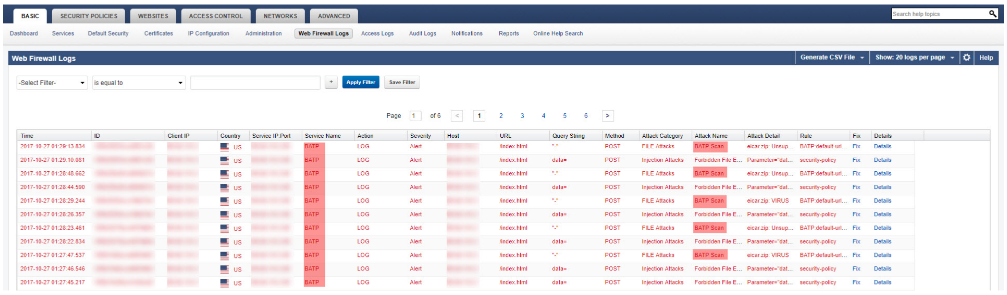
3. The Barracuda Web Application Firewall forwards the response to the client.

4. The BATP server analyzes the file content for any zero day attack or for the presence of other malwares.

   1. The Barracuda Web Application Firewall checks the BATP server for file scan completion.
   2. After the file scan is complete, the BATP server sends the response with details.
   3. The Barracuda Web Application Firewall processes the response and generates logs for the scanned file.

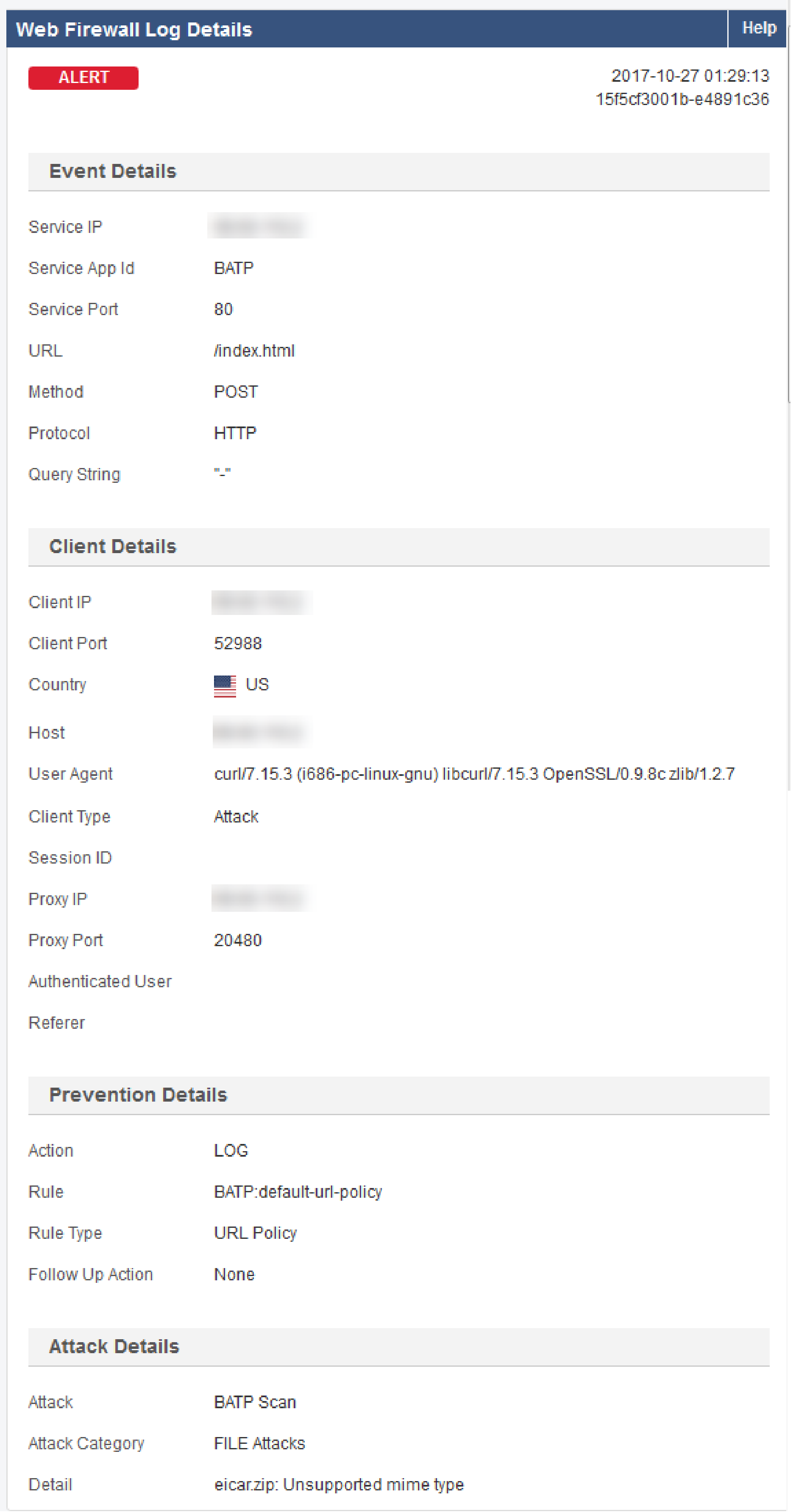
Logs generated by BATP

1. The status of the scanned files is logged in the **BASIC > Web Firewall Logs** page.



Time	ID	Client IP	Country	Service IP:Port	Service Name	Action	Severity	Host	URL	Query String	Method	Attack Category	Attack Name	Attack Detail	Rule	Fix	Details
2017-10-27 01:29:13.834	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	"-"	POST	FILE Attacks	BATP Scan	eicar.zip: Unsup...	BATP:default-url...	Fix	Details
2017-10-27 01:29:10.081	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	data=	POST	Injection Attacks	Forbidden File E...	Parameter="dat...	security-policy	Fix	Details
2017-10-27 01:28:48.662	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	"-"	POST	FILE Attacks	BATP Scan	eicar.zip: Unsup...	BATP:default-url...	Fix	Details
2017-10-27 01:28:44.590	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	data=	POST	Injection Attacks	Forbidden File E...	Parameter="dat...	security-policy	Fix	Details
2017-10-27 01:28:29.244	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	"-"	POST	FILE Attacks	BATP Scan	eicar.zip: VIRUS	BATP:default-url...	Fix	Details
2017-10-27 01:28:26.357	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	data=	POST	Injection Attacks	Forbidden File E...	Parameter="dat...	security-policy	Fix	Details
2017-10-27 01:28:23.461	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	"-"	POST	FILE Attacks	BATP Scan	eicar.zip: Unsup...	BATP:default-url...	Fix	Details
2017-10-27 01:28:22.834	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	data=	POST	Injection Attacks	Forbidden File E...	Parameter="dat...	security-policy	Fix	Details
2017-10-27 01:27:47.537	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	"-"	POST	FILE Attacks	BATP Scan	eicar.zip: VIRUS	BATP:default-url...	Fix	Details
2017-10-27 01:27:46.546	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	data=	POST	Injection Attacks	Forbidden File E...	Parameter="dat...	security-policy	Fix	Details
2017-10-27 01:27:45.217	[redacted]	[redacted]	US	[redacted]	BATP	LOG	Alert	[redacted]	/index.html	data=	POST	Injection Attacks	Forbidden File E...	Parameter="dat...	security-policy	Fix	Details

2. Click the **Details** link to view the **Web Firewall Log Details** page. The details of the scan are shown in the **Attack Details** section.



2017-10-27 01:29:13
15f5cf3001b-e4891c36

Event Details

Service IP	[redacted]
Service App Id	BATP
Service Port	80
URL	/index.html
Method	POST
Protocol	HTTP
Query String	"-"

Client Details

Client IP	[redacted]
Client Port	52988
Country	US
Host	[redacted]
User Agent	curl/7.15.3 (i686-pc-linux-gnu) libcurl/7.15.3 OpenSSL/0.9.8c zlib/1.2.7
Client Type	Attack
Session ID	
Proxy IP	[redacted]
Proxy Port	20480
Authenticated User	
Referer	

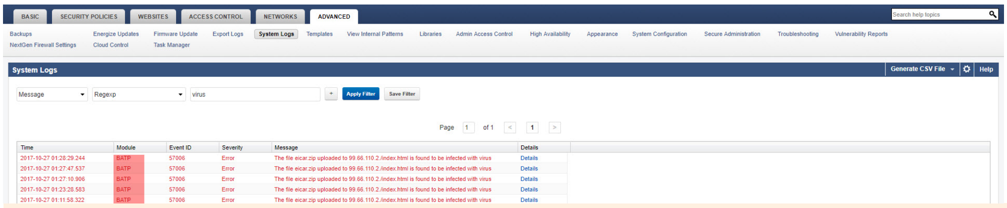
Prevention Details

Action	LOG
Rule	BATP:default-url-policy
Rule Type	URL Policy
Follow Up Action	None

Attack Details

Attack	BATP Scan
Attack Category	FILE Attacks
Detail	eicar.zip: Unsupported mime type

3. The BATP module also generates additional logging information which is available in the **ADVANCED > System Logs** page.
    1. To view the system logs under the **Module BATP**, select **Message** from the **-Select Filter-** dropdown, select **Regexp** from the **is equal to** dropdown and type **virus** in the text box beside the **is equal to** text box.
    2. Click the **Apply Filter** button to immediately view the generated system logs**.**
    3. Click on the **Save Filter** button to view the **System Logs** page at a later point in time. The **System Logs** page is as shown:

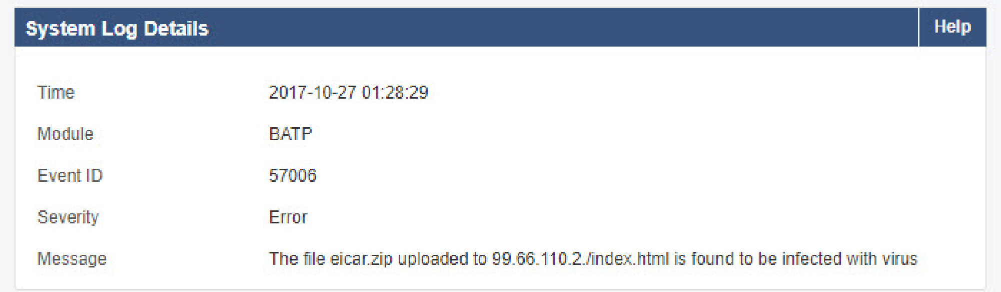


Message | Regexp | virus

Time	Module	Event ID	Severity	Message	Details
2017-10-27 01:28:29.244	BATP	57006	Error	The file eicar.zip uploaded to 99.66.110.2./index.html is found to be infected with virus	Details
2017-10-27 01:27:47.537	BATP	57006	Error	The file eicar.zip uploaded to 99.66.110.2./index.html is found to be infected with virus	Details
2017-10-27 01:27:10.906	BATP	57006	Error	The file eicar.zip uploaded to 99.66.110.2./index.html is found to be infected with virus	Details
2017-10-27 01:23:28.583	BATP	57006	Error	The file eicar.zip uploaded to 99.66.110.2./index.html is found to be infected with virus	Details
2017-10-27 01:11:58.322	BATP	57006	Error	The file eicar.zip uploaded to 99.66.110.2./index.html is found to be infected with virus	Details

> The **System Logs** image displays the **Module** name as **BATP.** However, the **Module** name under **System Logs** is displayed as **BATD** in the firmware version 9.1.

4. Click the **Details** link to view the **System Log Details** page. The **System Log Details** page is as shown:



Time	2017-10-27 01:28:29
Module	BATP
Event ID	57006
Severity	Error
Message	The file eicar.zip uploaded to 99.66.110.2./index.html is found to be infected with virus

After the logs are generated, the administrator can filter logs using the **BATP Scan** keyword. If any infected file is found, the administrator should take necessary action(s) to remove it from the server.

Figures