LOGPOINT

Integrations

Barracuda

V6.0.0

CONTENTS

CHAPTER

ONE

BARRACUDA

Barracuda normalizes Barracuda events and enables you to analyze Barracuda data. Logpoint aggregates and normalizes the Barracuda logs so you can analyze the information through *LP_Barracuda SV Firewall, LP_Barracuda Web Application Firewall*, and *LP_Barracuda Web Filter* dashboards. The dashboards provide visualization of attacks, URL details, content type, banned attachment and spam fingerprints detected in your network. You can customize it to perform in-depth analysis by changing the data used in a search.

Barracuda consists of the following components:

1. **Compiled Normalizers**

   Modularized Compiled Normalizer:

   Modularization separates a program's functionality into independent, interchangeable modules. Each module contains everything necessary to executes only one aspect of the program's functionality. With modularization it is easier to add and maintain smaller program components, understand the purpose of each module, and reuse and refactor them. The modularized compiled normalizer *BarracudaCompiledNormalizer* includes the modules like *BarracudaNGFirewallCompiledNormalizer*, *BarracudaEmailSGCompiledNormalizer* and *BarracudaEmailSecurityServiceCompiledNormalizer* that are capable of carrying out task(s) independently and work as basic constructs for the *BarracudaCompiledNormalizer*.

   Non-modularized Compiled Normalizer:

   Non-modularization means no modules are integrated into the program. The non-modularized Barracuda compiled normalizers like *BarracudaEmailSGCompiledNormalizer* and *BarracudaEmailSecurityServiceCompiledNormalizer* are independent and normalize specific logs such as *EmailSecurityGateway*, *EmailSecurityService* and *NextGenerationFirewall*.

   Following are the non-modularized compiled normalizers included in Barracuda:

- BarracudaNGFirewallCompiledNormalizer
- BarracudaCEFNormalizer
- BarracudaEmailSGCompiledNormalizer
- BarracudaWAFCompiledNormalizer
- BarracudaEmailSecurityServiceCompiledNormalizer
- BarracudaWSGCompiledNormalizer

2. **Normalization Packages**
   - LP_Barracuda Email Security Gateway
   - LP_Barracuda NG Firewall
   - LP_Barracuda Web Application Firewall
   - LP_Barracuda WAF CEF
   - LP_Barracuda Firewall
   - LP_Barracuda Web Filter
   - LP_Barracuda Load Balancer
   - LP_Barracuda ADC 540Vx Loadbalancer
   - LP_Barracuda Cloud Email Filter
3. **Label Packages**
   - LP_Barracuda NG Firewall
   - LP_Barracuda Web Filter
4. **Search Template**
   - LP_BarracudaWAF

CHAPTER

TWO

INSTALLING BARRACUDA

Prerequisite

Logpoint v6.7.4 or later

Supported Devices

- Barracuda System and Firewall
- Barracuda Web Application Firewall CEF
- Barracuda NG Firewall (Model F600) - version 5.4.3-182
- Barracuda Firewall
- Barracuda Web Filter
- Barracuda Spam And Virus Firewall
- Barracuda WAF

To install Barracuda:

1. Download the .pak file from the Help Center.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

After installing Barracuda, you can find it under *Settings >> System >> Plugins*.

CHAPTER

THREE

UNINSTALLING BARRACUDA

You must remove **Barracuda** configuration to delete it.

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** icon from **Actions**.
3. Click **Yes**.

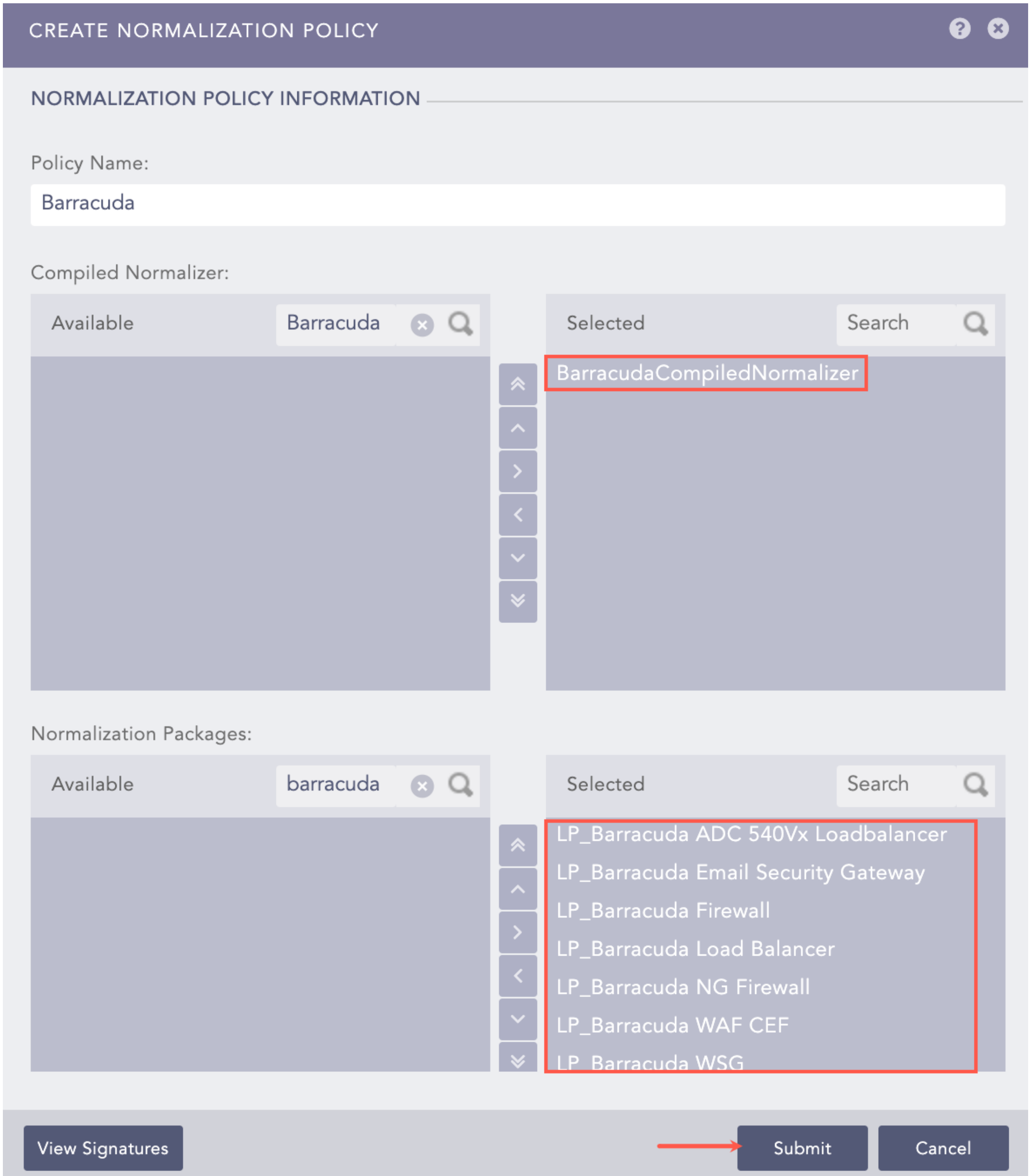
CHAPTER

FOUR

CONFIGURING BARRACUDA

4.1 Adding a Normalization Policy for Barracuda

1. Go to *Settings >> Configuration* from the navigation bar and click **Normalization Policies**.
2. At the top left, click **Add**.
3. Enter a **Policy Name**.
4. In **Compiled Normalizer**, select **BarracudaCompiledNormalizer**.
5. In **Normalization Packages**, select the required normalization package(s).
6. Click **Submit**.



Policy Name: Barracuda

Compiled Normalizer:

- Available (search: Barracuda)
- Selected: BarracudaCompiledNormalizer

Normalization Packages:

- Available (search: barracuda)
- Selected:
  - LP_Barracuda ADC 540Vx Loadbalancer
  - LP_Barracuda Email Security Gateway
  - LP_Barracuda Firewall
  - LP_Barracuda Load Balancer
  - LP_Barracuda NG Firewall
  - LP_Barracuda WAF CEF
  - LP_Barracuda WSG

Fig. 1: Adding a Normalization Policy

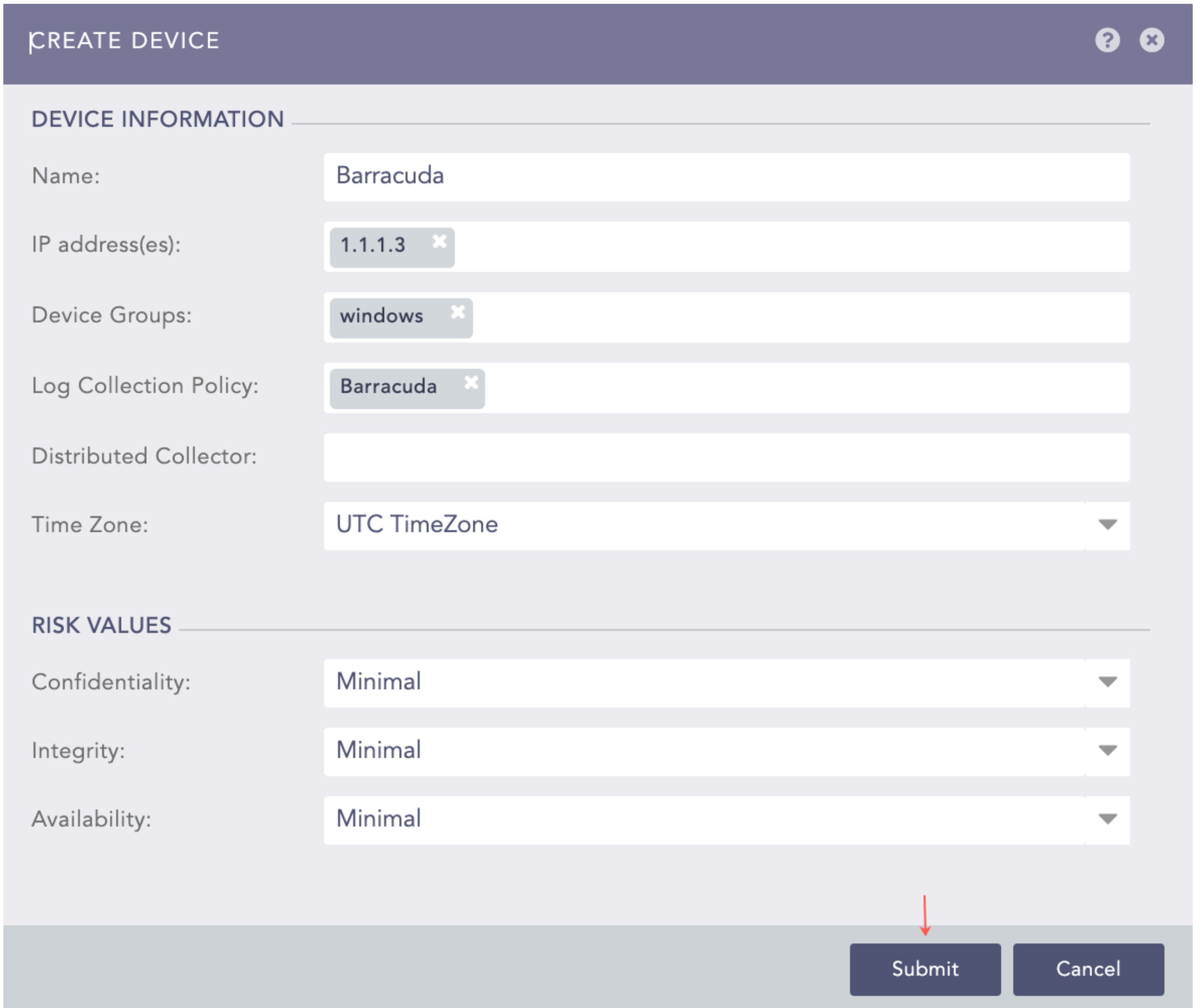
4.2 Adding Barracuda as a Device in Logpoint

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.

2. At the top left, click **Add**.
3. Enter a device **Name**.
4. Enter the **IP address(es)** of the *Barracuda* server.
5. Select the **Device Groups**.
6. Select an appropriate **Log Collection Policy** for the logs.
7. Select a collector or a forwarder from the **Distributed Collector** drop-down.

Note: It is optional to select the **Device Groups**, the **Log Collection Policy** and the **Distributed Collector**.

8. Select a **Time Zone**. The timezone of the device must be same as its log source.
9. Configure the **Risk Values** for **Confidentiality**, **Integrity** and **Availability** used to calculate the risk levels of the alerts generated from the device.
10. Click **Submit**.


CREATE DEVICE

DEVICE INFORMATION

Name: Barracuda

IP address(es): 1.1.1.3

Device Groups: windows

Log Collection Policy: Barracuda

Distributed Collector:

Time Zone: UTC TimeZone

RISK VALUES

Confidentiality: Minimal

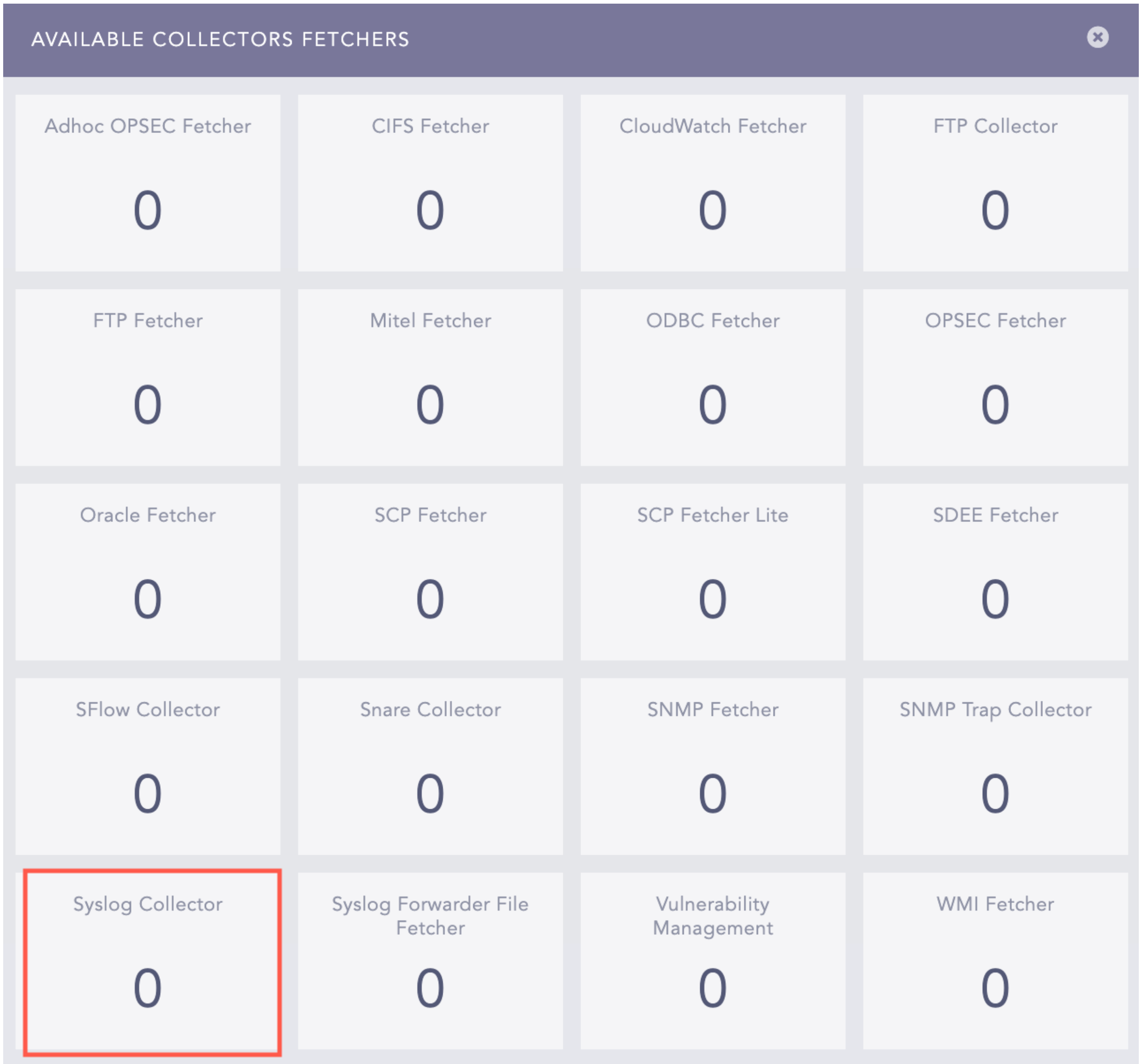
Integrity: Minimal

Availability: Minimal

Fig. 2: Adding Barracuda as a Device

4.3 Configuring the Syslog Collector for Barracuda

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.
2. Search for the previously added device.
3. Click the **Add** icon from **Actions**.
4. Click **Syslog Collector** on **AVAILABLE COLLECTORS FETCHERS**.

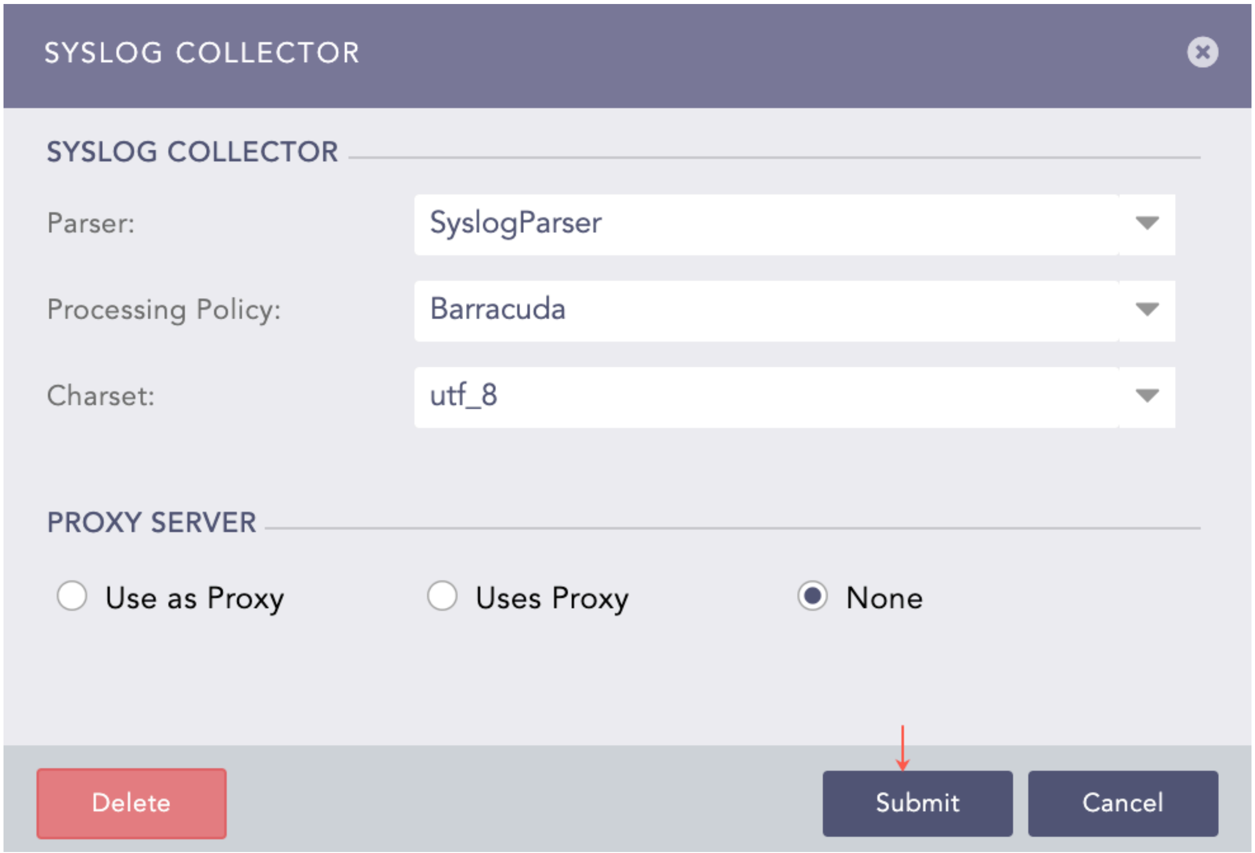


AVAILABLE COLLECTORS FETCHERS

Adhoc OPSEC Fetcher 0	CIFS Fetcher 0	CloudWatch Fetcher 0	FTP Collector 0
FTP Fetcher 0	Mitel Fetcher 0	ODBC Fetcher 0	OPSEC Fetcher 0
Oracle Fetcher 0	SCP Fetcher 0	SCP Fetcher Lite 0	SDEE Fetcher 0
SFlow Collector 0	Snare Collector 0	SNMP Fetcher 0	SNMP Trap Collector 0
Syslog Collector 0	Syslog Forwarder File Fetcher 0	Vulnerability Management 0	WMI Fetcher 0

Fig. 3: Available Collectors Fetchers Panel

5. Select **Syslog Parser** as **Parser**.
6. Select a **Processing Policy** that uses the previously created *normalization policy*.
7. Select the **Charset**.
8. In **Proxy Server**, select **None**
9. Click **Submit**.



SYSLOG COLLECTOR

Parser: SyslogParser

Processing Policy: Barracuda

Charset: utf_8

PROXY SERVER

○ Use as Proxy ○ Uses Proxy ● None

Fig. 4: Configuring Syslog Collector

CHAPTER

FIVE

BARRACUDA ANALYTICS

5.1 Barracuda Dashboards

5.1.1 LP_Barracuda Web Application Firewall

This dashboard consists of the following widgets:

Widget Name	Description
Attack Count	The count of attacks such as DDOS attacks, forceful browsing, protocol violations, limits violation and other to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage.
Attack Timetrend	A time span observation providing a dynamic view of attacks in the hope of forecasting future attacks.
Top 10 Attack Events	The top ten attack events that have or might lead to unauthorized data access, processing, corruption, alteration, transfer or disclosure of data.
Top Distinct Attacks by Source Locations	The sources of top distinct attacks and their destinations based on source country, action and destination address.
Total Attackers	The distinct count of total attackers based on source address.
Top Actions Taken on Traffic	The top actions taken on traffic by a firewall to block attack traffic while allowing valid traffic through the firewall with no impact on the quality of experience of the valid traffic.

Continued on next page

Table 1 – continued from previous page

Widget Name	Description
Top 10 Errors from Client	The top ten client-side error codes such as Invalid Request (status code 400), Authentication Failed (401), Not Found (status code 404), Method Not Allowed (status code 405) and Invalid Post Data (status code 415) that occurred on a client-server system, such as a web application. Client-side errors caused by problems with the client's web browser or device, rather than the server.
Top 10 Protocols	The top ten protocols applied by a firewall to establish a secure communication between different devices for the exchange of data.
Injection Attack Details	Details of an injection attack such as blind SQL injection or SSI injection. An attacker injects code into a program or query, or injects malware onto a computer to execute remote commands that can read or modify a database, or change data on a web site.
DOS Attack Details	Details of DOS attack such as buffer overflows or flood attacks, where an attacker use a false IP address to flood the targeted host or network with illegitimate service requests.
Top 10 Users in Attack Events	The top ten remote or local users involved during an attack.
Attack Details	Details of the attack including source address, source country, attack type, destination address, destination country, request method, URL, rule type and actions.

5.1.2 LP_Barracuda SV Firewall

This dashboard consists of the following widgets:

Widget Name	Description
Top 10 Action	The top ten actions taken to inspect incoming and outgoing traffic using a set of security rules to identify and block threats.
Top 10 Mail Destinations Domain	The top ten destination addresses domains where emails were sent, for a firewall to allow or block the destination IP address.

Continued on next page

Table 2 – continued from previous page

Widget Name	Description
Top 10 Source Address	The top ten source addresses of a device or user that sent data across the network. It allows an administrator to specify which source addresses are allowed or denied access to the network or choose to block all traffic from a particular source address.
Top 10 Mail Sender	The top ten email senders whose behavior on the server is monitored. Problem senders are blocklisted based on their IP address and domain name.
Top 10 Mail Receiver	The top ten email receivers can help administrators decide what kind of filters to apply to incoming emails in addition to removing spam.
User Login - List	The user logins activity list by login timestamp, username and actions.
Time trend of Action	A dynamic view of actions that can help forecast future threats.
Top 10 Destination Address	The top ten destination addresses of servers where you want to grant access to a service.
Message Category - RECV and SCAN services	The data on RECV services indicating a message was handled by the MTA and processing stopped and SCAN service indicating the message was scanned and processing may have stopped or it may have been sent to outbound processing for delivery.
Message Category - SEND services	The data on SEND services, such as delivered message, rejected message, deferred message and expired message indicating the status of outbound delivery. It is the only message that may appear multiple times for a given message ID.
Top 15 Event Category by Reason Code	The top fifteen Barracuda event categories by reason code, such as Virus, Banned Attachment or RBL Match to identify an error condition.
Top 10 Hosts in Barracuda Blocklist Category	The top ten hosts linked to junk emails in the block list category.
Top 10 Senders in Barracuda Blocklist Category	The top ten senders in the block list category from which you would not receive emails.
Top 10 Receivers in Barracuda Blocklist Category	The top ten receivers in the block list category who would not receive incoming mails.

Continued on next page

Table 2 – continued from previous page

Widget Name	Description
Top 10 Hosts in Virus Category	Top ten hosts categorized as *Virus* of Barracuda RECV and SCAN services.
Top 10 Senders in Virus Category	Top ten senders categorized as *Virus* of Barracuda RECV and SCAN services.
Top 10 Receivers in Virus Category	Top ten receivers categorized as *Virus* of Barracuda RECV and SCAN services.
Top 10 Receivers in Banned Attachment Category	The top ten receivers in the *Band Attachment* category of Barracuda RECV and SCAN services based on filename patterns you specify, common text attachment file types and attachment MIME types.
Top 10 Senders in Banned Attachment Category	Top ten senders in the *Band Attachment* category of Barracuda RECV and SCAN services.
Top 10 hosts in Banned Attachment Category	Top ten hosts in the *Band Attachment* category of Barracuda RECV and SCAN services.
Top 10 host in Spam Fingerprint Found Category	The top ten hosts in the *Spam Fingerprint Found* category of Barracuda RECV and SCAN services through which hackers create a network map that helps them identify vulnerabilities for a successful attack.
Top 10 Sender in Spam Fingerprint Found Category	Top ten senders in the *Spam Fingerprint Found* category of Barracuda RECV and SCAN services.
Top 10 receiver in Spam Fingerprint Found Category	Top ten receivers in the *Spam Fingerprint Found* category of Barracuda RECV and SCAN services.

5.1.3 LP_Barracuda Web Filter

This dashboard consists of the following widgets:

Widget	Description
Barracuda Web Filter Details - List	A list of Barracuda Web Filters activities based on timestamp, source address, destination address, URL, action, reason, content type (HTML or jpeg), data size, matched part and category.
Top 10 Source Address	The top ten source addresses to prevent malicious traffic.

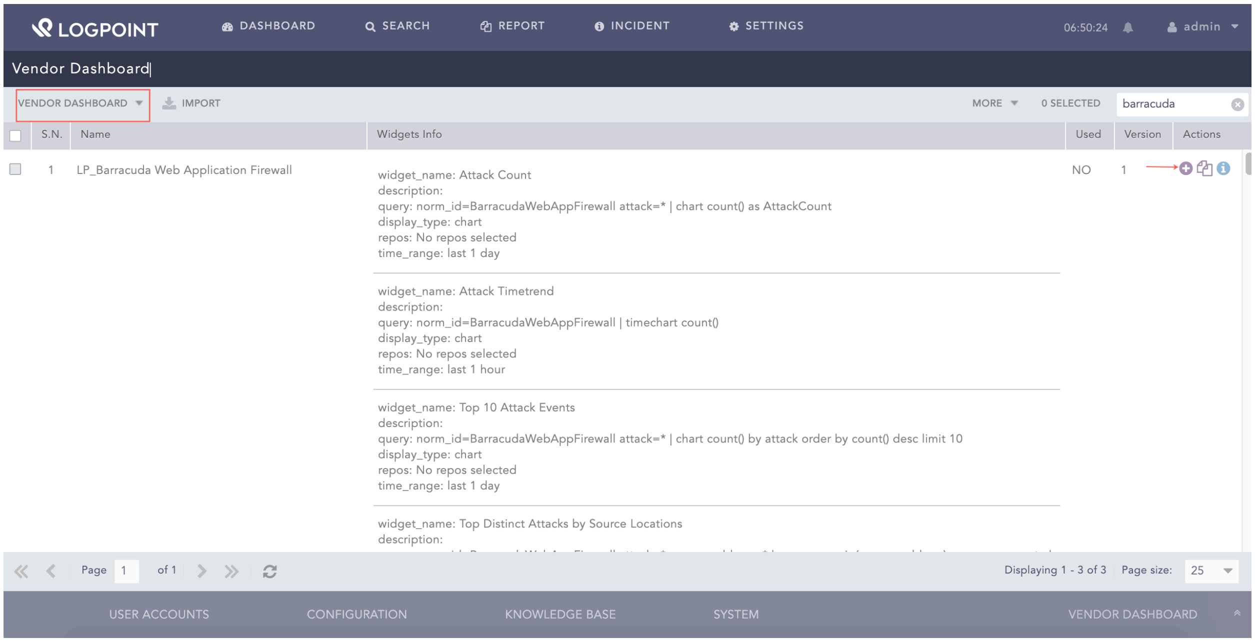
Continued on next page

Table 3 – continued from previous page

Widget	Description
Top 10 Destination Address	The top ten destination addresses to prevent certain data from flowing into a destination.
Top 10 Action with Reason	The top ten actions performed by Barracuda Web Filter, along with the reasons for the actions taken. For example, a device scanned as a threat is detected.
URL Details - List	A list of the frequently visited URLs based on action, reason, matched part and category.
Top Content Type - List	A list of the top website contents filtered by Barracuda Web Filters.
Top Matched Part - List	A list of the top regular expressions, domain names or keywords that matched to a URL.
Top Matched Category - List	A list of the top built-in or customized web content categories that matched with your regular expressions, domain names or keywords.

5.1.4 Adding the Barracuda Dashboard

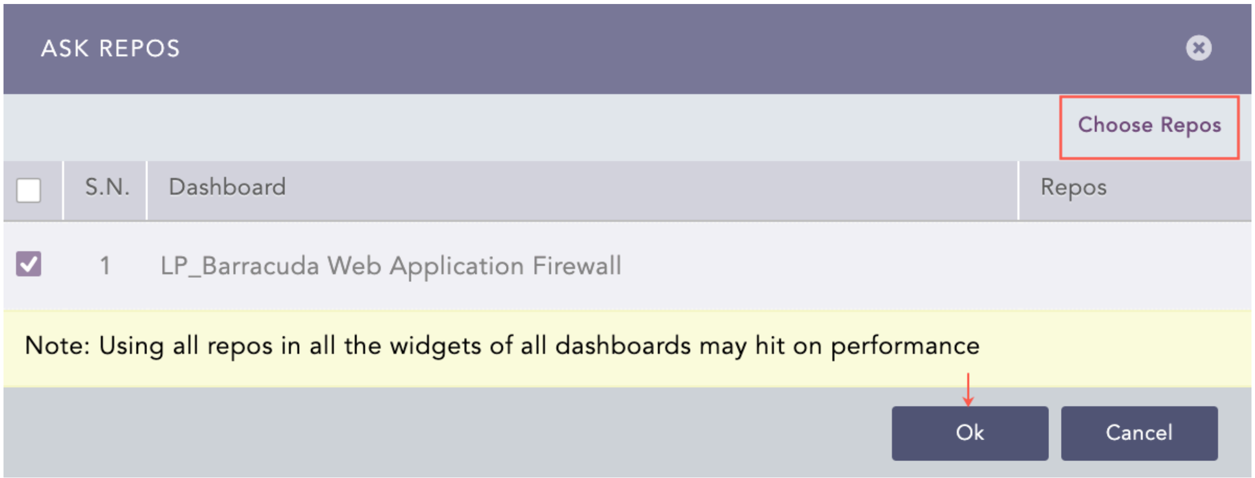
1. Go to *Settings >> Knowledge Base* from the navigation bar and click **Dashboard**.
2. Select **VENDOR DASHBOARD** from the drop-down.
3. Click the **Use** icon from **Actions**.



S.N.	Name	Widgets Info	Used	Version	Actions
1	LP_Barracuda Web Application Firewall	widget_name: Attack Count description: query: norm_id=BarracudaWebAppFirewall attack=* | chart count() as AttackCount display_type: chart repos: No repos selected time_range: last 1 day widget_name: Attack Timetrend description: query: norm_id=BarracudaWebAppFirewall | timechart count() display_type: chart repos: No repos selected time_range: last 1 hour widget_name: Top 10 Attack Events description: query: norm_id=BarracudaWebAppFirewall attack=* | chart count() by attack order by count() desc limit 10 display_type: chart repos: No repos selected time_range: last 1 day widget_name: Top Distinct Attacks by Source Locations description:	NO	1	⊕

Fig. 1: Adding the Barracuda Dashboard

4. Click **Choose Repos**.

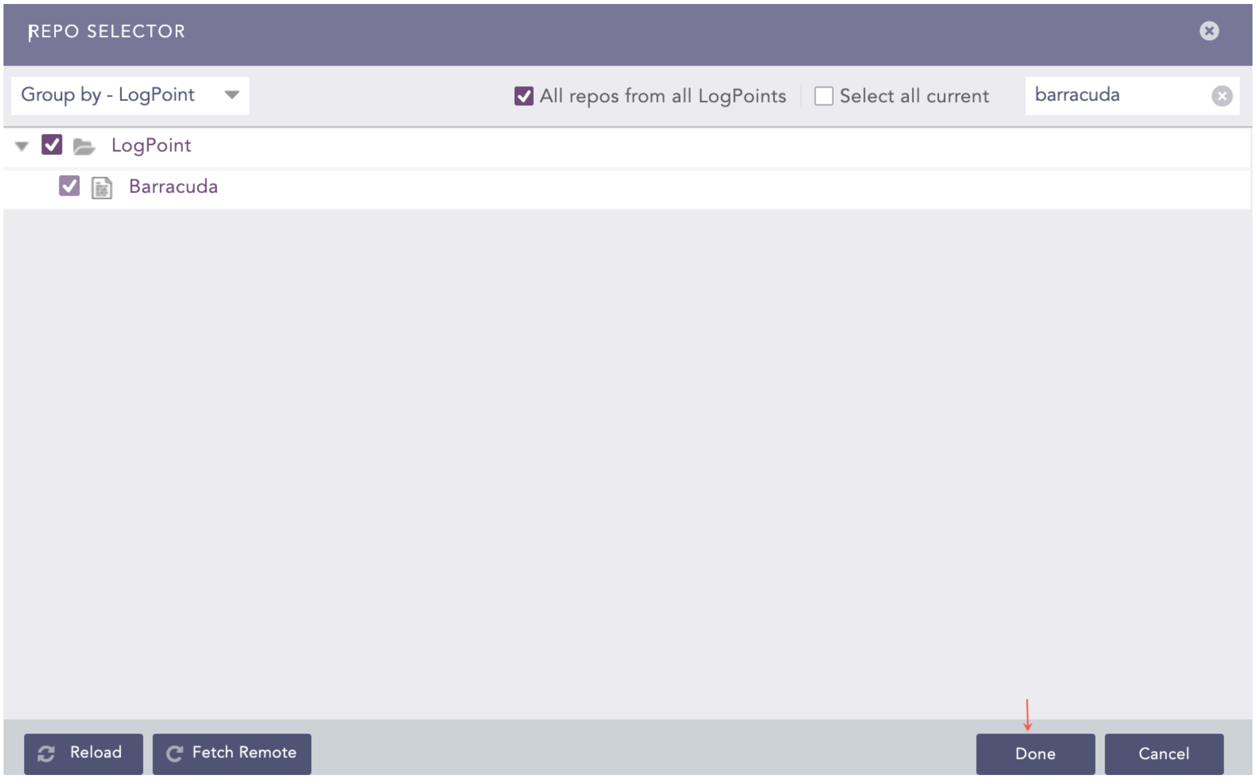


☐	S.N.	Dashboard	Repos
☑	1	LP_Barracuda Web Application Firewall	

Note: Using all repos in all the widgets of all dashboards may hit on performance

Fig. 2: Selecting Repos

5. Select the repo and click **Done**.



☑ All repos from all LogPoints ☐ Select all current

barracuda

- ☑ LogPoint
  - ☑ Barracuda

Fig. 3: Selecting Repos

6. Click **Ok**.

You can find the Barracuda dashboards under *Dashboard*.

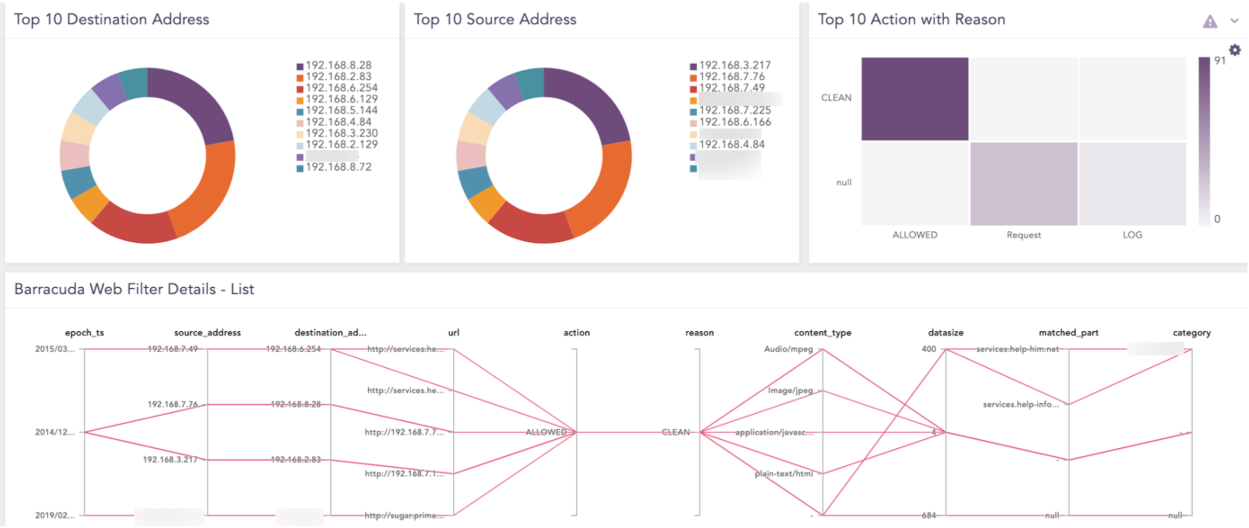


Fig. 4: Barracuda Dashboard

5.2 Barracuda Labels

Labels available in *LP_Barracuda NG Firewall* are:

Labels	Description
Allow	Events with the *Allow* or *LocalAllow* action.
Deny	Events with the *Deny* or *LocalDeny* action.
Drop	Events with the *Drop* and *LocalDrop* action.
Detect	Events with the *Detect* or *LocalDetect* action.
ARP	Events with the *ARP* action.
Normal, Operation	Events with the *Normal Operation* message.
Balance, Session, Idle, Timeout	Events with the *Balanced Session Idle Timeout* message.
Block, Rule	Events with the *Block by Rule* message.
Connection, Rese, Source	Events with the *Connection Reset by Source* message.
Session, Idle, Timeout	Events with the *Session Idle Timeout* message.
Connection, Reset	Events with the *Connection Reset by Destination* message.
Acknowledge, Timeout	Events with the *Last ACK Timeout* message.
TCP,Packet, Not, Active, Session	Events with the *TCP Packet Belongs to no Active Session* message.

Continued on next page

Table 4 – continued from previous page

Labels	Description
ARP, Duplicate, MAC	Events with the *ARP reply duplicate and MAC differs* message.
ICMP, Packet, Ignore	Events with the *ICMP Packet is Ignored* message.
Connection, Timeout	Events with the *Connect Timeout* message.
Timeout	Events with the *Unreachable Timeout* message.
Block, Broadcast	Events with the *Block Broadcast* message.
Timeout	Events with the *Halfside Close Timeout* message.
Application, Control	Events with the *Application Control* message.
Detect, Not, Allow, Port	Events with the *Unallowed Port Protcol Detected* message.
Reverse, Routing, Interface, Mismatch	Events with the *Reverse Routing Interface Mismatch* message.
Accept, Timeout	Events with the *Accept Timeout* message.
TCP, Header, Invalid	Events with the *TCP Header has an Invalid SEQ Number* message.
IPS, Warning	Events with the *IPS Warning* message.
Drop, Not, Allow, Port, Detect	Events with the *Drop due to Unallowed Port Protocol* message.
MAC, Address, Change	Events with the *MAC Address Change* message.
Local, Socket, Not, Present	Events with the *No Local Socket Present* message.
Policy, Block, URL, Category	Events with the *URL Category Blocked by Policy* message.
Block, Not, Rule, Match	Events with the *Block no Rule Match* message.
Not, Active, Session, ICMP, Packet	Events with the *ICMP Packet Belongs to no Active Session* message.
TCP, Header, Invalid	Events with the *TCP Header has an Invalid ACK Number* message.
Internal, SSL, Error	Events with the *Internal SSL Error* message.
Invalid, Synchronization, Establish, TCP, Session	Events with the *Invalid SYN for Established TCP Session* message.
Drop, TCP, RST	Events with the *Drop guessed TCP RST* message.
IPS, Drop, Log	Events with the *IPS Drop Log* message.
IPS, Alert	Events with the *IPS Alert* message.
Block, Local, Loop	Events with the *Block Local Loop* message.
Terminate, Content	Events with the *Terminated due to content* message.
IP, Header, Incomplete	Events with the *IP Header is Incomplete* message.
Request, IPS, Policy, Terminate	Events with the *IPS Policy Requested Termination* message.
Duplicate, IP, Detect, Match	Events with the *Duplicate IP Detection Matched* message.

Continued on next page

Table 4 – continued from previous page

Labels	Description
TCP, Header, Incomplete	Events with the *TCP Header is Incomplete* message.
TCP, Header, Checksum, Invalid	Events with the *TCP Header Checksum is Invalid* message.
TF-Sync	Events with the *TF-Sync* message.
Block	Events with the *Block* or *LocalBlock* action.
Remove	Events with the *Remove* or *LocalRemove* action.
Fail	Events with the *Remove* or *LocalRemove* action.

Labels available in *LP_Barracuda Web Filter* are:

Labels	Description
Allow	Events with the *ALLOWED* action.
Block	Events with the *BLOCKED* action.
Detect	Events with the *DETECTED* action.
Clean	Events with the *CLEAN* reason.
Virus	Events with the *VIRUS* reason.
Skyware	Events with the *SPYWARE* reason.

CHAPTER

SIX

LOG SAMPLES

Expected Log Format Sample

Barracuda Cloud Email Filter

```
<6> 2021-10-27T04:41:43Z ip-100.internal ESS91785[1]: {"message_id":"1633444894-105481-
↪5298-10428-1","src_ip":"192.168.97.25","hdr_from":"\"Logpoint Publications\" \u003cno-
↪reply@Logpoin.com\u003e","account_id":"abc123","domain_id":"189043","ptr_record":"s1.
↪asa1.acem.com","attachments":null,"recipients":[{"action":"allowed","reason":"m","reason_
↪extra":"m","delivered":"delivered","delivery_detail":"logpoint-edu.mail.protection.outlook.
↪com:25:250 2.6.0 \u003c20211005141738.8382.232815220.swift@Logpointpublications.
↪activehosted.com\u003e [InternalId=14306536080363, Hostname=BL3P223MB0161.NAMP223.
↪PROD.OUTLOOK.COM] 116795 bytes in 0.273, 417.467 KB/sec Queued mail for delivery",
↪ "email":"lpedraza@logpoint.edu","taxonomy":"none"}],"hdr_to":"\"Leon Pedraza\"
↪\u003clpedraza@logpoint.edu\u003e","recipient_count":1,"dst_domain":"logpoint.edu",
↪ "size":97272,"subject":"Develop deep knowledge of faculty development","env_from":
↪ "bounce-529093-2847-29700-lpedraza=logpoint.edu@s1.csa1.acemsa3.com","timestamp":
↪"2021-10-05T14:41:40+0000","geoip":"USA","tls":true}
```

Expected Log Format Sample

Intrusion Prevention System (IPS)

```
<12>Jul 06 07:40:54 xxxxxxx 1/sssss/ssss/box_Firewall_threat: Warning host firewall: [Request]
↪Allow: IPS ALLIP(0) 1.1.1.1 -> 0.0.0.0:0 |[ID: 5000002 TCPIP Port or IP Address Scan]||2|Probing
```

Expected Log Format Sample

Web Firewall Logs

```
2014-04-11 10:50:30.411 +0530 wafbox1 WF ALER PRE_1_0_REQUEST xx.xx.x.xxx 34006 xx.xx.
↪xxx.x 80 global GLOBAL LOG NONE [POST /index.cgi] POST xx.xx.xxx.x /index.cgi HTTP
↪REQ-0+RES-0 "Mozilla/5.0 (X11; Linux i686; rv:12.0) Gecko/20100101 Firefox/12.0" xx.xx.xxx.x
↪34005 ABC http://xx.xx.xxx.x /index.cgi
```

Expected Log Format Sample

Access Logs

```
<134>2020-11-12 06:37:42.791 -0400 WAF1 TR 1.1.1.1 443 24.2.252.238 43662 "-" "-" GET TLSv1.
↪3 www.abc.com HTTP/1.1 200 1643 1968 0 592 1.1.1.1 443 591 "-" SERVER PROFILED
↪PROTECTED VALID /load/rave/ "-" https://www.abc.com _ga=GA1.2.757211401.1575902461;
↪hubspotutk=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx; __hssrc=1; _gcl_au=1.1.1890078026.1600961
↪263; nmstat=1600961274952; _fbp=fb.1.1600961263367.958342315; __hstc=211988107.
↪b036aa4d75c35f4baae31bd05bb6da9d.1575902465900.15759024659 "Mozilla/5.0 (X11; CrOS
↪x86_64 xxxxx.xx.x) AppleWebKit/537.36 (KHTML , like Gecko) Chrome/xx.x.xxxx.xx Safari/537.
↪36" 24.2.252.238 43662 "-" "-" "-" "-" xxxxxxxxxx-xxxxxxxx
```

Expected Log Format Sample

Audit Logs

```
2016-02-02 21:08:53.861 -0800 wafbox1 AUDIT User3 GUI 192.0.0.0 0 CONFIG 17 - SET web_
↪firewall_policy default url_protection_max_upload_files "5" "6" "[]"
```

Expected Log Format Sample

Network Firewall Logs

```
afbox1 2016-05-21 03:28:23.494 -0700 NF INFO TCP 192.0.0.0 52236 1.1.1.1 8000 DENY testacl
↪MGMT/LAN/WAN interface traffic:deny policy TCPFeb 3 15:09:02 wsf STM: LB 5 00141
↪LookupServerCtx = 0xab0bb6xx
```

Expected Log Format Sample

Barracuda System and Firewall

```
2010-02-03 01:49:09.077 -0800 logpointbox WF ALER SQL_INJECTION_IN_PARAM 1.1.1.7 361 1.
↪1.1.20 webapp1:deny_ban GLOBAL LOG NONE "[type=""sql-injection-medium"" pattern="
↪"sql-quote"" token=""' or "" Parameter=""address"" value=""hi' or 1=1--""]" POST 1.1.1.2/
↪xxx-bin/process.xxx HTTP REQ-0+RES-0 "Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-US; rv:1.8.
↪1.20) Gecko/20081217 Firefox/2.0.0.20" 1.1.1.7 39661 Bob http://1.1.1.2/xxx-bin/1.pl 11956
↪ATTACK_CATEGORY_INJECTION
```

Expected Log Format Sample

Barracuda Web Application Firewall CEF

```
<161>CEF:0|Barracuda|WAF|910|2002|GeoIP-Pool:WPA_Rep_Pool|1|cat=NF src=xxx.xxx.xx.xx
↪spt=57169 dst=xx.x.x.xx dpt=443 act=DENY dvchost=ABC proto=TCP rt=1531388610159
↪cs1=MGMT/LAN/WAN interface traffic:deny  cs1Label=Details
```

Expected Log Format Sample

Barracuda NG Firewall

```
<14>Jun 15 07:52:08 LOGPOINT 1/DEBUxxx/LOGPOINT2/box_Firewall_Activity: Info
↪LOGPOINT2 Allow: type=FWD|proto=TCP|srcIF=p2.1|srcIP=xxx.xx.xxx.
↪x|srcPort=49609|srcMAC=xx:xx:xx:xx:xx:xx|dstIP=xxx.xx.x.
↪xxx|dstPort=49155|dstService=|dstIF=p1|rule=INSIDELYNCAUDIOWAN|info=FF-
↪Sync|srcNAT=xxx.xx.xxx.x|dstNAT=xxx.xx.x.
↪xxx|duration=0|count=1|receivedBytes=0|sentBytes=0|receivedPackets=0|sentPackets=0|user=|protocol=|ap
```

(continues on next page)

(continued from previous page)

Expected Log Format Sample

Barracuda Firewall

```
<14>Oct 20 11:02:51 bru02 1/GroupIT/logpoint/box_Firewall: Info logpoint firewall: [Request]
↪Allow: type=FWD rule=Exchangeclients (00:00:00:00:00:44)TCP 1.1.1.1:50531 (port1) -> 1.1.1.
↪2:8034-vanxxxxxx-mgmt port3.10
```

Expected Log Format Sample

Barracuda Web Filter

```
<164>http_scan[15983]: 1418826306 1 1.1.1.1 1.1.1.2 application/javascript 1.1.1.3 http://1.1.1.4/
↪lp/logpoint.com/warn.xx.10918xxxxxx/lp.ab.0328.0397/lp.cd.0329.0424? &tag=0&time=&
↪eventid=&callback=PushStreamManager_0_onmessage_1418826313069&_=1418826313069
↪584 BYF ALLOWED CLEAN 2 1 0 5 3 (-) 1 - 0 - 0 - - [ldap0:pp.op] http://www.abc.com/push/
```

Expected Log Format Sample

Barracuda Spam And Virus Firewall

```
<23>scan[2716]: mail2.abc.com[192.xxx.x.xx] 1425999233-06bc853d9ab85d40001-9xRH8n
↪1425999233 1425999273 SCAN - xxx@uvw.yz ppp@qrs.com 0.002 0 0 - SZ:135913 SUBJ:ppo
↪nrm-ul la acest aviz cat mai repede posibil
```

Expected Log Format Sample

Barracuda Email Security Service

```
1140 <6> 2022-05-09T14:41:23Z ip-1.1.1.1.us-east-2.compute.internal ESSxxxxx[1]: {"message_id
↪":"1633444868-102973-5408-2198-1","src_ip":"1.1.1.1","hdr_from":"\"ABC\" \u003logpoint.
↪com\u003e","account_id":"ess91785","domain_id":"189043","ptr_record":"target.com",
↪"attachments":null,"recipients":[{"action":"allowed","reason":"","reason_extra":"",
↪"delivered":"delivered","delivery_detail":"mail.protection.outlook.com:25:250 2.6.0
↪\u003xxxxxxxx6-065d-4026-bce7-xxxxxxxxx@at.xt.local\u003e [InternalId=14328010914404,
↪Hostname=PROD.OUTLOOK.COM] 13108 bytes in 0.050, 251.395 KB/sec Queued mail for
↪delivery","email":"bi@see.edu","taxonomy":"none"}],"hdr_to":"\u003chrxxxx","size":2517,
↪"subject":"Scale Ranks #1 on CRN,Äôs 2021 Annual Report Card for Edge Computing
↪infrastructure","env_from":"bounce-xxx_text-xxxxx-xxxxxx-xxxxx-xxx@bounce.etmailservices.
↪com","timestamp":"2022-05-09T14:41:21+0000","geoip":"Nepal","tls":true}
```