LOGPOINT

Integrations

DenyAll

*V*5.3.0 (latest)

CONTENTS

CHAPTER

ONE

DENY ALL WAF

Deny All WAF aggregates and normalizes Deny All WAF events and enables you to analyze Deny All WAF data through the *LP_Deny All Web Application Firewall* dashboard. The dashboard visualizes incident details for web attack source addresses, countries and other event details detected in your network. You can customize it to perform in-depth analysis by changing the data used in a search.

When Logpoint identifies threats, malware or malicious events with a potential risk, it triggers security alerts based on predetermined rules. The automated alert enables you to detect potential threats, malware or malicious events early and take corrective actions against them.

Deny All WAF enables you to collect and analyze Deny All WAF logs.

Supported Device/Source

- DenyAll Web Application Firewall v6.x

Deny All WAF components

1. **Compiled Normalizer**
    - LP_Deny All Web Application Firewall
2. **Alert Package**
    - LP_DenyAllWAF SQL Injection Attack

CHAPTER

TWO

INSTALLING DENY ALL WAF

Prerequisite

Logpoint v7.0.0 or later

To install Deny All WAF:

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 downloaded .pak file.
5. Click **Upload**.

After installing Deny All WAF, you can find it under *Settings >> System Settings >> Plugins*.

CHAPTER

THREE

UNINSTALLING DENY ALL WAF

You must remove the **Deny All WAF** configurations 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 DENY ALL WAF

4.1 Adding a Normalization Policy for Deny All WAF

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 Normalizers**, select *Deny All WAF*.
5. Click **Submit**.

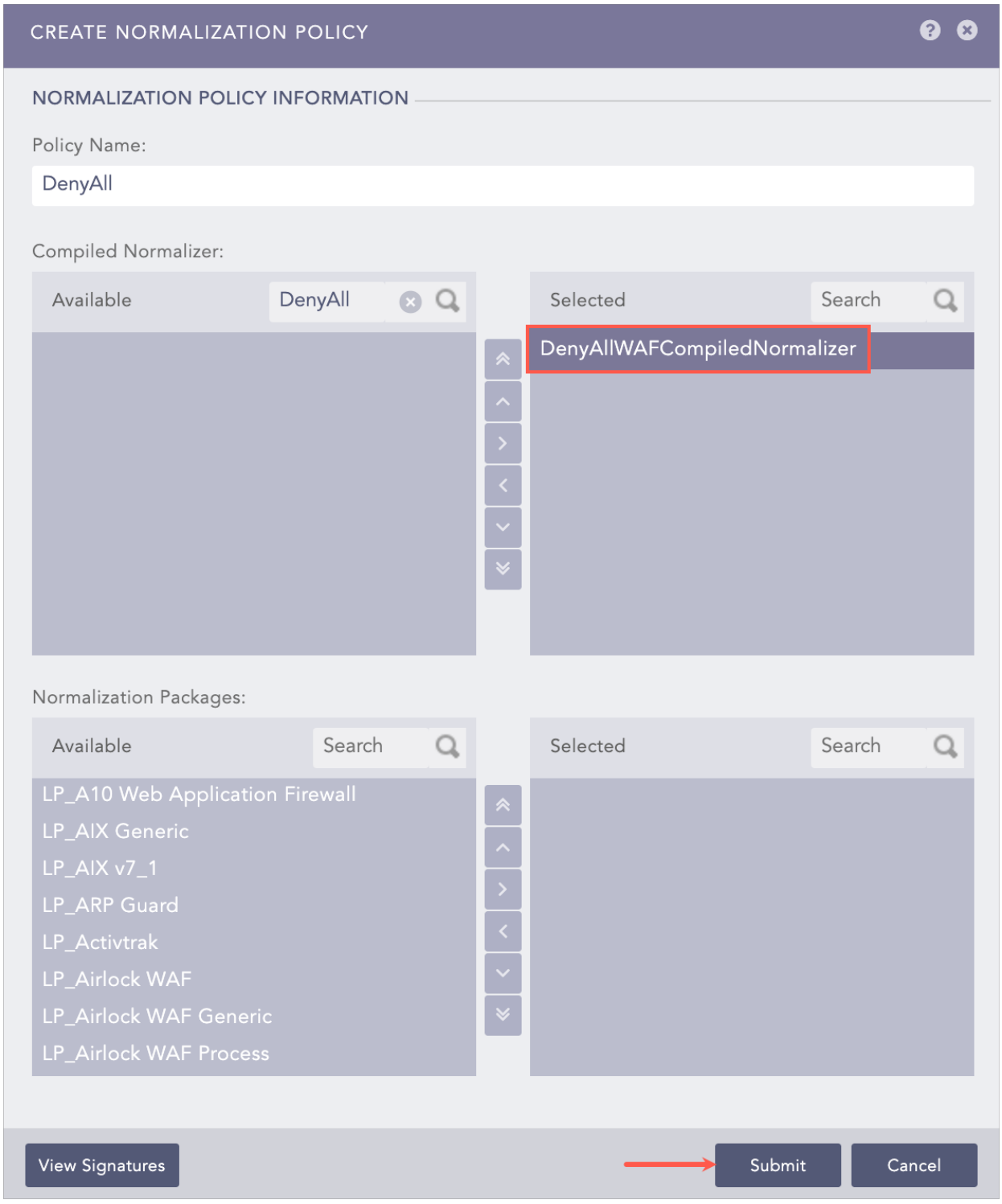

Fig. 1: Adding a Normalization Policy

4.2 Adding Deny All WAF 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 *Deny All WAF* 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 menu.

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 the 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**.

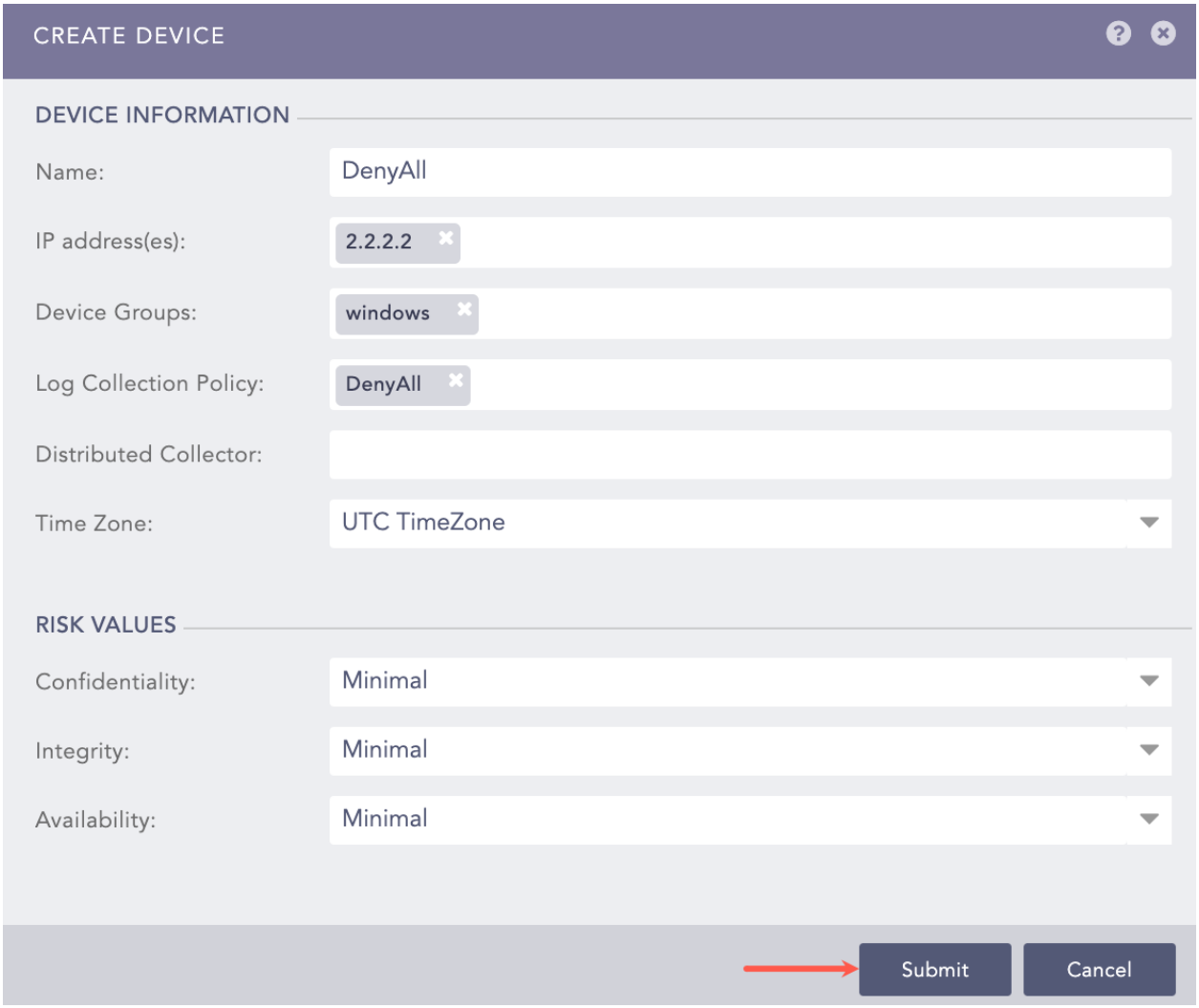

Fig. 2: Adding Deny All WAF as a Device

4.3 Configuring the Syslog Collector for Deny All WAF

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**.

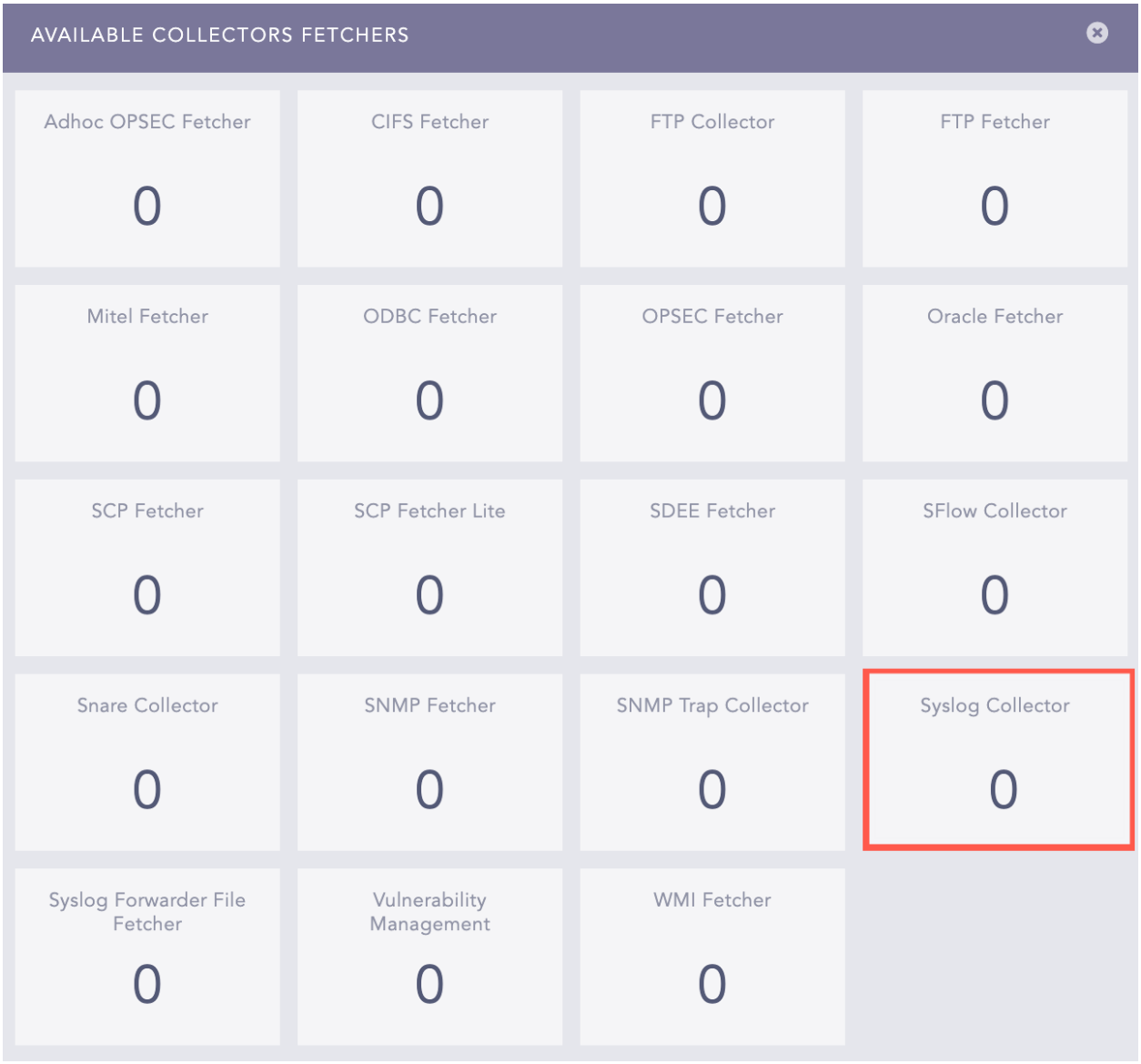

Fig. 3: Available Collectors Fetchers Panel

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**.

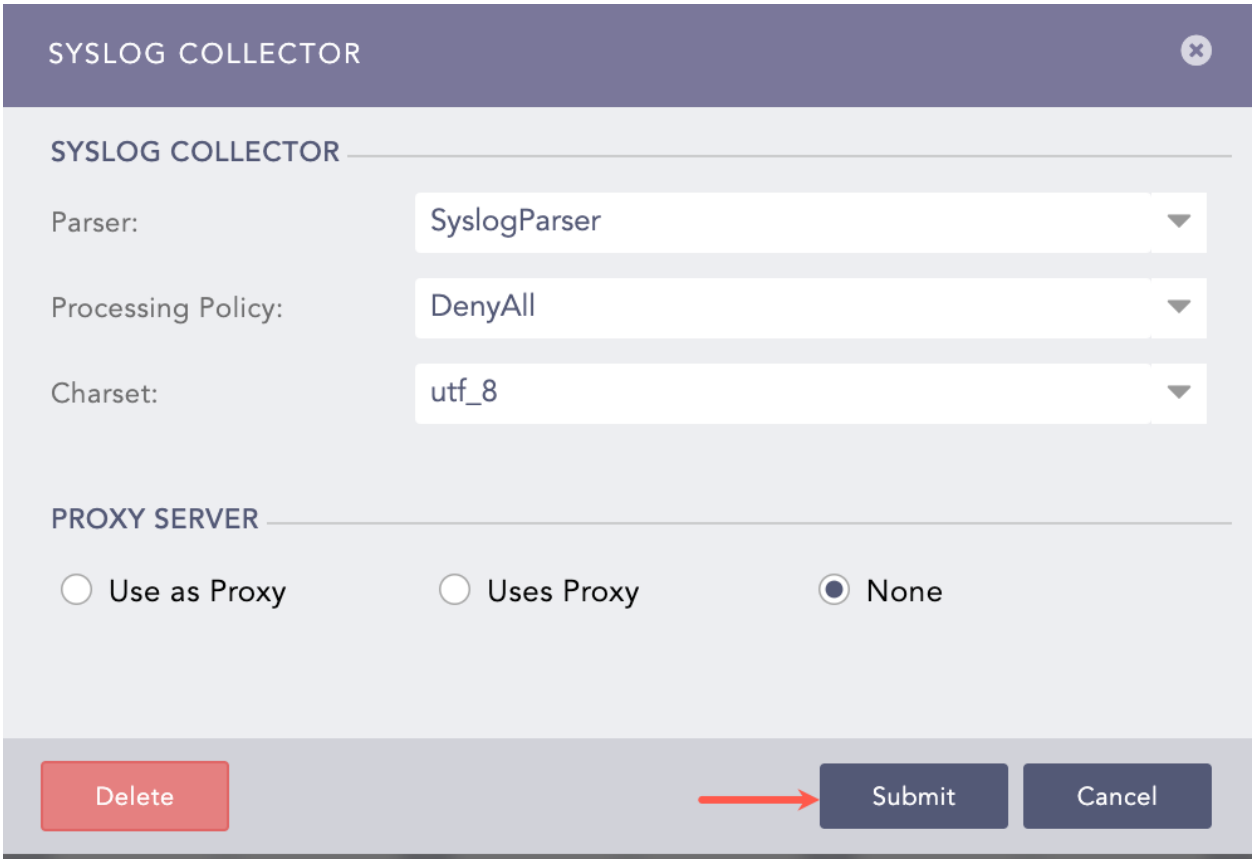

Fig. 4: Configuring Syslog Collector

CHAPTER

FIVE

DENY ALL WAF ANALYTICS

5.1 Deny All WAF Dashboard

5.1.1 LP_Deny All Web Application Firewall Dashboard

Widgets available in the dashboard *LP_Deny All Web Application Firewall* provide:

Widget Name	Description
Top 10 Source Address	Where a packet of data originated on a network so the firewall can determine whether the packet followed firewall rules.
Top 10 Firewall Rule	Entails the instructions used by the firewall to handle incoming, forwarding and outgoing traffic.
Firewall Request Rejection Reason	The source IP address's connection request refused for reasons being unknown hostname, path traversal or directory traversal.
Firewall Request Rejection - list	Entails all the rejected source addresses with reasons, uniform resource identifier (URI) and messages.
Top 10 Messages	The top 10 messages in network traffic inspected and authenticated before they are allowed to move to a more secure environment.
Top 10 Sources in SQL Injection Attack	The top ten compromised source IP addresses with an intent of SQL Injection Attack to manipulate backend database for accessing confidential information.
Top 10 Countries in SQL Injection Attack	The location of a source IP address with which the SQL Injection Attack originated.
SQL Injection Details	Entails sources IP address with SQL Injection, compromised url routes, threat type, country, log timestamp, action and function used for injection.

5.2 Adding the Deny All WAF 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**.

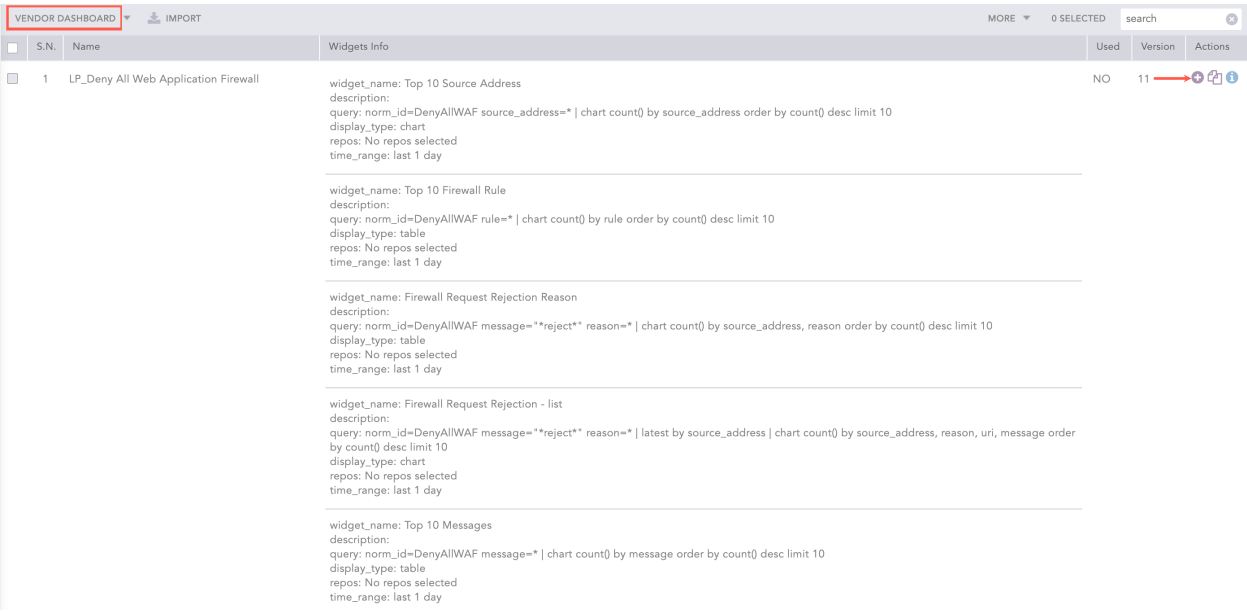

Fig. 1: Adding the Deny All WAF Dashboard

4. Click **Choose Repos**.

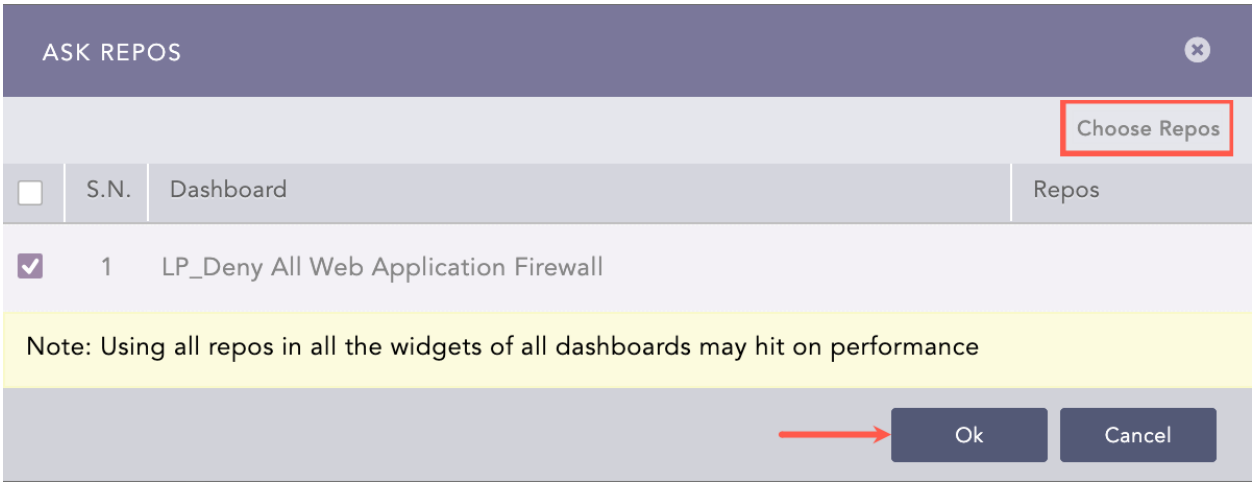

Fig. 2: Selecting Repos

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

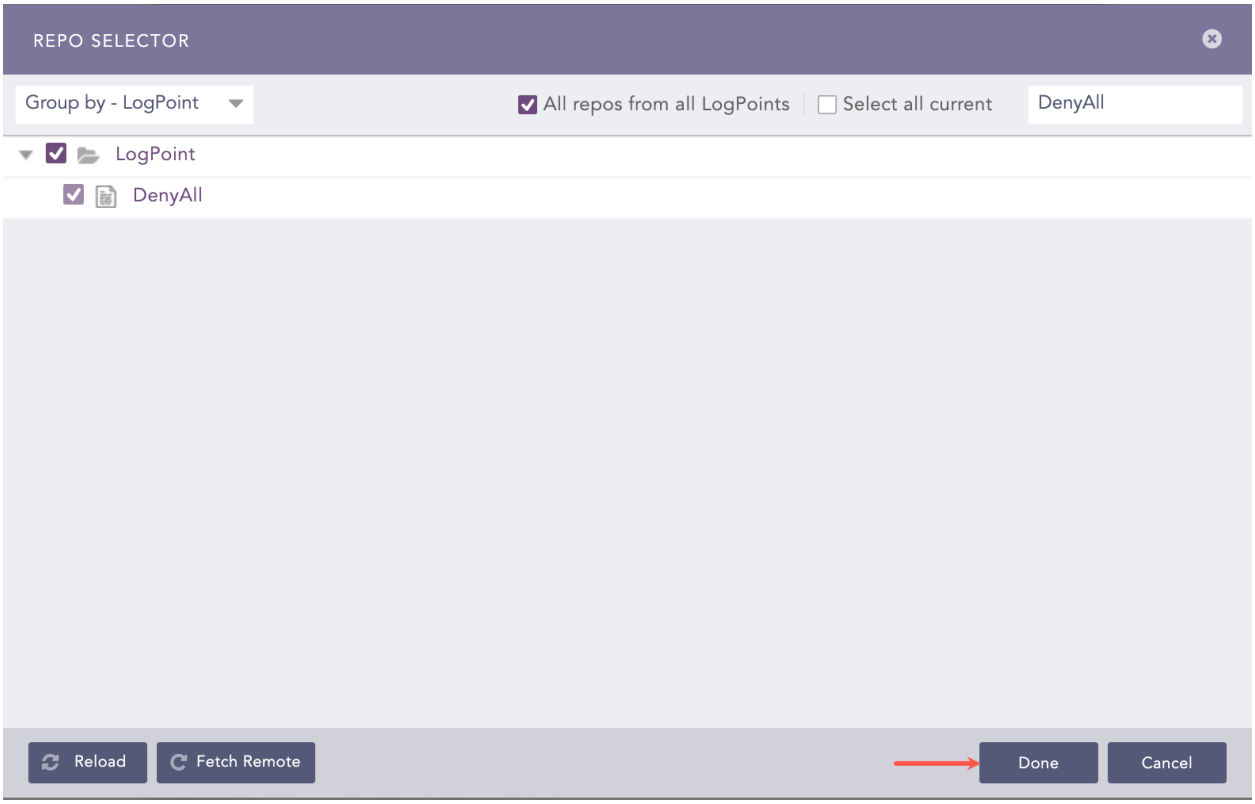

Fig. 3: Selecting Repos

6. Click **Ok**.

You can find the Deny All WAF dashboard under **Dashboards**.

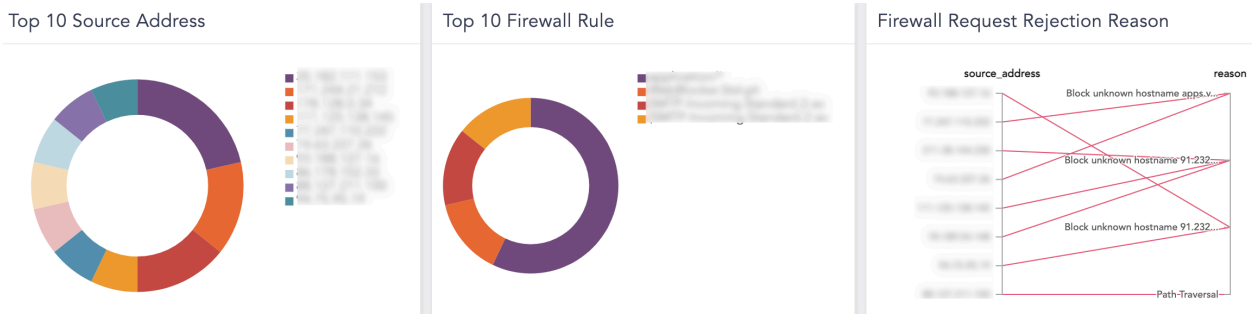

Fig. 4: Deny All WAF Dashboard

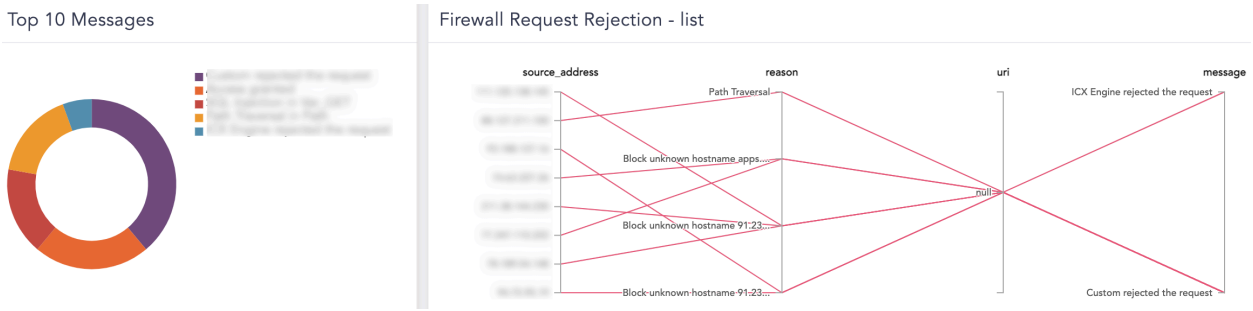

Fig. 5: Deny All WAF Dashboard

5.3 Deny All WAF Alert

5.3.1 DenyAllWAF SQL Injection Attack

- **Trigger condition:** A SQL injection attack is detected.
- **ATT&CK Category:** Initial Access
- **ATT&CK Tag:** Exploit Public-Facing Application
- **ATT&CK ID:** T1190
- **Minimum Log Source Requirement:** DenyAll WAF
- **Query:**

```
norm_id=DenyAllWAF label=SQL label=Injection
```

CHAPTER

SIX

EXPECTED LOG SAMPLES

6.1 Deny All WAF

Shellcode


```
"<5>1 2020-01-07T09:17:08.732356+01:00 Management - - - - {"logAlertUid":
↪"bb45b96adbb6a6216981645d5","@timestamp":"1578385028731","timestamp":
↪"1578385028731","_type_":"Controller_Business_Log_SecurityLog","request":{"body":"",
↪"cookies":[],"headers":[{"key":"Host","value":"admin.logpointnp.np"},{"key":"User-Agent",
↪"value":"check_ssl_cert/1.76.0"},{"key":"Connection","value":"close"}],"hostname":"admin.
↪logpoint.np","ipDst":"10.20.69.101","ipSrc":"10.2.1.31","method":"HEAD","path":"/",
↪"portDst":443,"protocol":"HTTP/1.1","query":"","requestUid":
↪"XhQ@hL3oLmW@9nUuvpOS@AAM0"},"context":{"tags":"","applianceName":
↪"Management","applianceUid":"fefaab9235ab42dbb5c4","backendHost":"10.100.1.1",
↪"backendPort":443,"reverseProxyName":"LOG123","reverseProxyUid":
↪"aaaaaad1cba28f9564840e0f774","tunnelName":"CD84-V-zyx","tunnelUid":
↪"661985yyyyyde9402cb00bc72af","workflowName":"WAF xxx-V-PORTACRM","workflowUid":
↪"xxxxx3b35b4c60a766801d0"},"events":[{"eventUid":"74c816c3e280a53df9c203ba05","tokens
↪":{"date":1578385028732003,"eventType":"security","engineUid":"custom","engineName":
↪"Custom","attackFamily":"No Attack Family","riskLevel":50,"riskLevelOWASP":0.0,"cwe":"-",
↪"severity":5,"resolveType":"No Resolve","part":"No Part","customMessage":"URL non
↪autorisee","reason":"Custom: URL non autorisee"}}]}"
```



```
"<5>1 2020-01-06T23:33:23.889229+01:00 Management - - - - {"logAlertUid":
↪"3820d6a0997f4444b5b6a3369b7053a3","@timestamp":"1578350003887","timestamp":
↪"1578350003887","_type_":"Controller_Business_Log_SecurityLog","request":{"body":"",
↪"cookies":[{"key":"PHPSESSID","value":"PHPSESSID=5g2r3dg3ka59f6vrvujb2mds53"}],
↪"headers":[{"key":"Accept-Encoding","value":"gzip,deflate"},{"key":"From","value":
↪"robot@seokicks.de"},{"key":"Connection","value":"Close"},{"key":"Referer","value":
↪"https://maps.vaucluse.fr/"},{"key":"Accept","value":"text/html,text/plain"},{"key":"Host",
↪"value":"maps.vaucluse.fr"},{"key":"User-Agent","value":"Mozilla/5.0 (compatible; SEOkicks;
↪ +https://www.seokicks.de/robot.html)"}],"hostname":"maps.vaucluse.fr","ipDst":"10.100.19.
↪46","ipSrc":"95.216.96.244","method":"GET","path":"/admin.php/auth/login/","portDst
↪":443,"protocol":"HTTP/1.1","query":"auth_url_return=%2Findex.php%2Fview%2F",
↪"requestUid":"XhO1s0rlt2PSIyBTRXMJ7AAAAAWs"},"context":{"tags":"","applianceName""
```