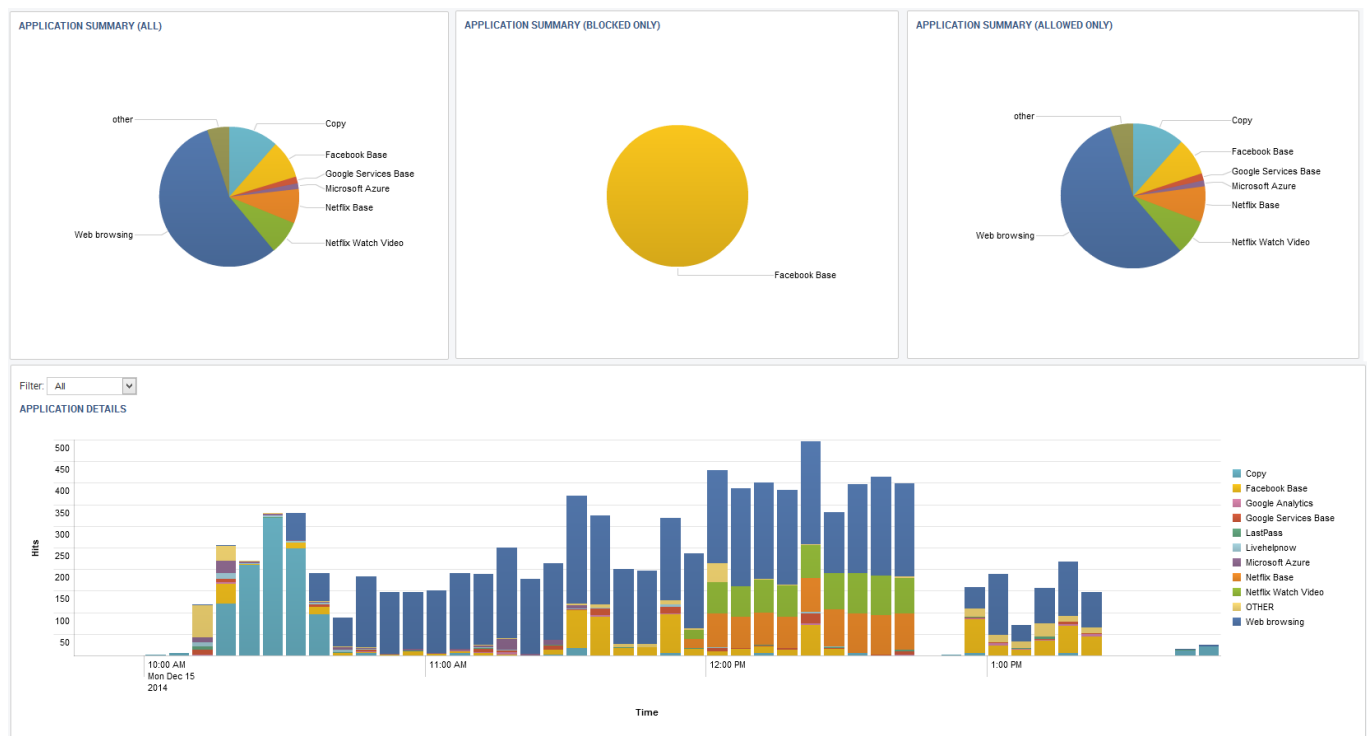


Splunk Integration

<https://campus.barracuda.com/doc/43846818/>

Splunk is a third-party platform for operational intelligence that allows you to monitor websites, applications servers, and networks. The Barracuda NG Firewall app shows information on matched access rules, detected applications, and applied URL filter policies on various fixed and real-time timelines. Data is imported into Splunk via syslog streaming of the Firewall activity log.



In this article

Before you Begin

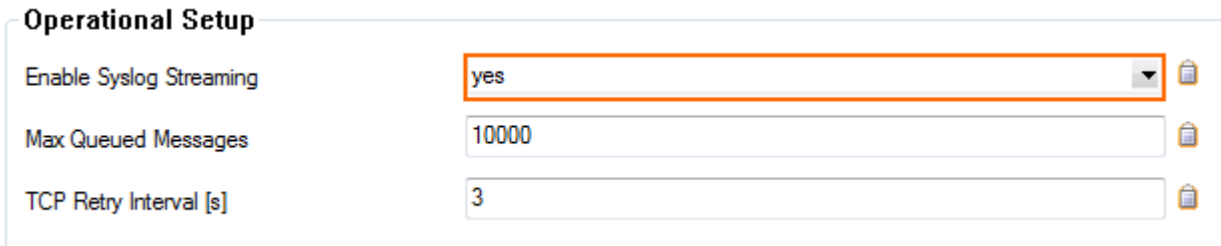
- Download the Barracuda NG Firewall Splunk App from the Splunk Marketplace.
- Install the Barracuda NG Firewall Splunk App on your Splunk Server. For more information, see <http://docs.splunk.com/Documentation/PCI/2.1.1/Install/InstalltheAppManually>.

Step 1. Configure Syslog Streaming on Barracuda NG Firewalls

Configure and enable syslog streaming for every Barracuda NG Firewall you want to include in the Splunk App.

Step 1.1. Enable Syslog Streaming

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.
3. Set **Enable the Syslog service** to **yes**.



Operational Setup	
Enable Syslog Streaming	yes
Max Queued Messages	10000
TCP Retry Interval [s]	3

4. Click **Send Changes** and **Activate**.

Step 1.2. Configure Logdata Filters

Define profiles specifying the log file types to be transferred / streamed.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Filters**.
3. Click **Lock**.
4. Click the + icon to add a new filter.
5. Enter a **Name** and click **OK**. The **Filters** window opens.
6. Click + in the **Data Selection** table and select **Firewall_Audit_Log**.
Fatal_log and **Panic_log** data can also be streamed to the Splunk server, but are currently not processed by the Barracuda NG Firewall Splunk app.
7. In the **Affected Box Logdata** section select **Selection** from the **Data Selector** dropdown.
8. Click + to add a **Data Selection**. The **Data Selection** window opens.
9. Enter a **Name** and click **OK**.
10. In the **Log Groups** table, click + and select **Firewall-Activity-Only** from the list.

Data Selection

Log Groups + - 📄

Firewall-Activity-Only

Log Message Filter ▼ 📄

Selected Message Types + - 📄

11. Click **OK**.
12. In the **Affected Service Logdata** section, select **None** from the **Data Selector** dropdown.
13. Click **OK**.

Top Level Logdata

Data Selection + ✕ 📄

Firewall_Audit_Log

Affected Box Logdata

Data Selector ✔ Selection 📄

Data Selection ✔ + ✕ 📄 📄 📄 📄

Name	Log Groups	Log Message Filter
DATA01	Firewall-Activity-Only	All

Affected Service Logdata

Data Selector None 📄

Data Selection + ✕ 📄 📄 📄 📄

Name	Log Groups	Log Message Filter

14. Click **Send Changes** and **Activate**.

Step 1.3. Configure the Logstream Destinations

Configure the data transfer settings for the Splunk server. You can optionally choose to send all syslog data via an SSL-encrypted connection.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logstream Destinations**.
3. Click **Lock**.
4. Click **+** in the **Destinations** table. The **Destinations** window opens.
5. Configure the Splunk server logstream destination:
 - **Remote Loghost** - Select **explicit-IP**
 - **Loghost IP Address** - Enter the IP address of the Splunk server.
 - **Loghost Port** - Enter **5140** for plaintext or **5141** for SSL-encrypted connections.

The Barracuda NG Firewall app can only process syslog data that is received on port 5140 (not encrypted) or 5141 for SSL-encrypted connections.
 - **Transmission Mode** - Select **TCP** or **UDP** (only for unencrypted connections).
 - **(optional) Sender IP** - Enter the management IP address of the Barracuda NG Firewall or leave blank for the NG Firewall to do a routing lookup to determine the Sender IP address.
 - **(optional) Use SSL Encapsulation** - Select **yes** to send the syslog stream over an SSL-encrypted connection.
 - **(optional) Peer SSL Certificate** - Import the SSL certificate configured on the Splunk server for this data import.

Configure the Splunk server to receive SSL-encrypted connections. For more information, see <http://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf>.
 - **Override Node Name** - Select **no**
6. Click **OK**.

Destination Address	
Remote Loghost	explicit-IP
Loghost IP Address	10.0.10.44
Loghost Port	5140

Data Transfer Setup	
Transmission Mode	TCP
Sender IP	10.0.10.88
Use SSL Encapsulation	no
Peer SSL Certificate	Show... Ex/Import No certificate present
SSL Peer Authentication	verify peer with locally installed certificate

Log Data Tagging	
Add Range/Cluster Info	yes
Override Node Name	no
Explicit Node Name	
Explicit Hierarchy Info	Range-Cluster
Add UTC Offset	no

7. Click **Send Changes** and **Activate**.

Step 1.4. Configure Logdata Streams

Create a logdata stream configuration combining the previously configured **Log Destinations** and **Log Filters**.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logdata Streams**.
3. Click **Lock**.
4. Click **+** in the **Streams** table.
5. Enter a **Name** and click **OK**. The **Streams** window opens.
6. In the **Log Destinations** table, click **+** and select the **Log Destination** created in Step 1.3.
7. In the **Log Filters** table, click **+** and select the **Log Filter** created in Step 1.2.

Stream Configuration

Active Stream

Log Destinations

Log Filters

8. Click **OK**.
9. Click **Send Changes** and **Activate**.

All firewall log data is now being streamed to the Splunk server.

Step 2. Data Data Input on Splunk

The Splunk server must be configured to receive the syslog data. Verify that you have a **Data input** entry for TCP or UDP port 5140 or TCP port 5141 (SSL) that listens for the incoming syslog streaming connections. You must use port 5140/5141 because the Barracuda NG Firewall Splunk app can only process data received on these ports. For more information, see <http://docs.splunk.com/Documentation/Splunk/6.2.0/Data/Monitornetworkports>.

Step 3. (optional) Enable SSL Encryption for Barracuda NG Firewall Splunk App

If you want to SSL encrypt connections with Splunk, you must modify the inputs.conf configuration file for the Barracuda NG Firewall Splunk App.

1. Copy your SSL certificates to `/opt/splunk-6.2/etc/auth/server.pem` and `/opt/splunk-6.2/etc/auth/box-cert.pem`.
2. Login to the Splunk server via SSH.
3. Edit `$SPLUNK_HOME/etc/apps/BarracudaNGFirewall/default/inputs.conf` and add a section for SSL:

```
[SSL]
serverCert = /opt/splunk-6.2/etc/auth/server.pem
password = password
```

```
requireClientCert = true  
rootCA = /opt/splunk-6.2/etc/box-cert.pem
```

4. Restart Splunk.

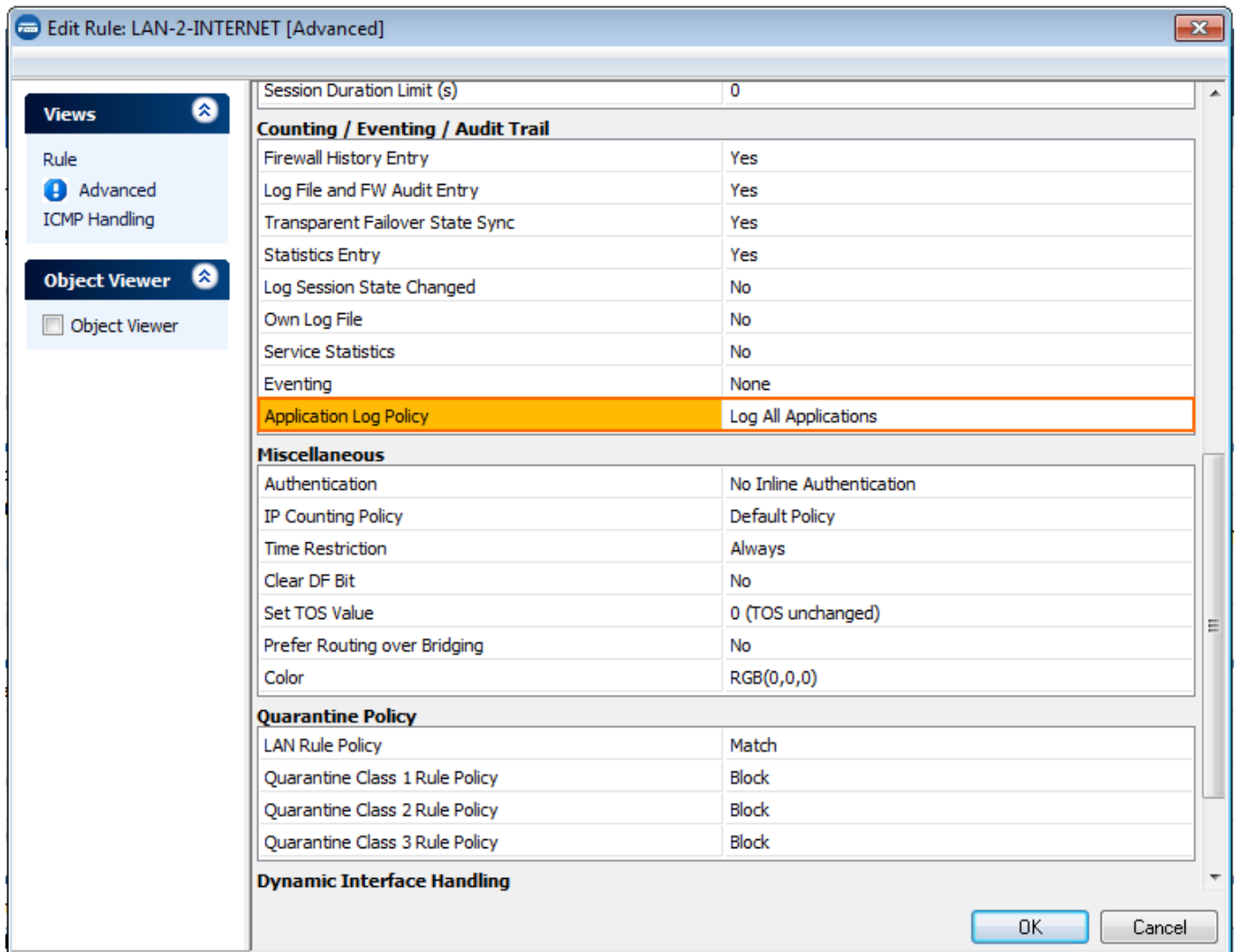
Certificate Troubleshooting

If you see log messages containing the string "alert bad certificate" in the **bsyslog** log file, the **rootCA** certificate is either missing or invalid. Set **requireClientCert** to **false** to disable the certificate check.

```
2014 12 16 09:43:34 Notice +01:00 Syslog connection established; fd='14',  
server='AF_INET(127.0.0.1:6224)', local='AF_INET(0.0.0.0:0)' 2014 12 16 09:43:34 Error  
+01:00 [18697:4146318224] SSL_connect:14094412: error:14094412:SSL  
outines:SSL3_READ_BYTES:ssl3 alert bad certificate
```

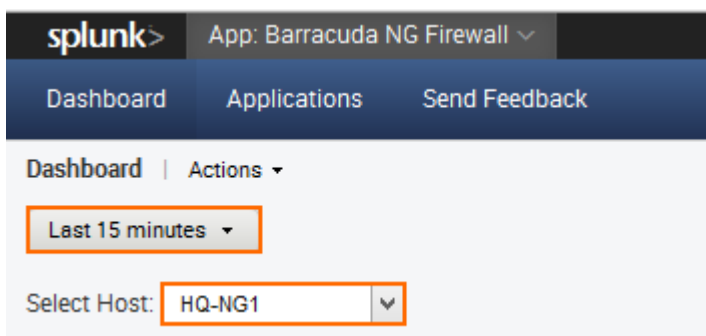
Step 4. Enable Application Logging in the Firewall

Application data is collected on a per-access rule basis. Set the **Application Log Policy** to **Log All Applications** in the **Advanced Firewall Rule Settings** for each access rule that matches traffic you want to include in the data collected on the Splunk server. For more information, see [Advanced Access Rule Settings](#).



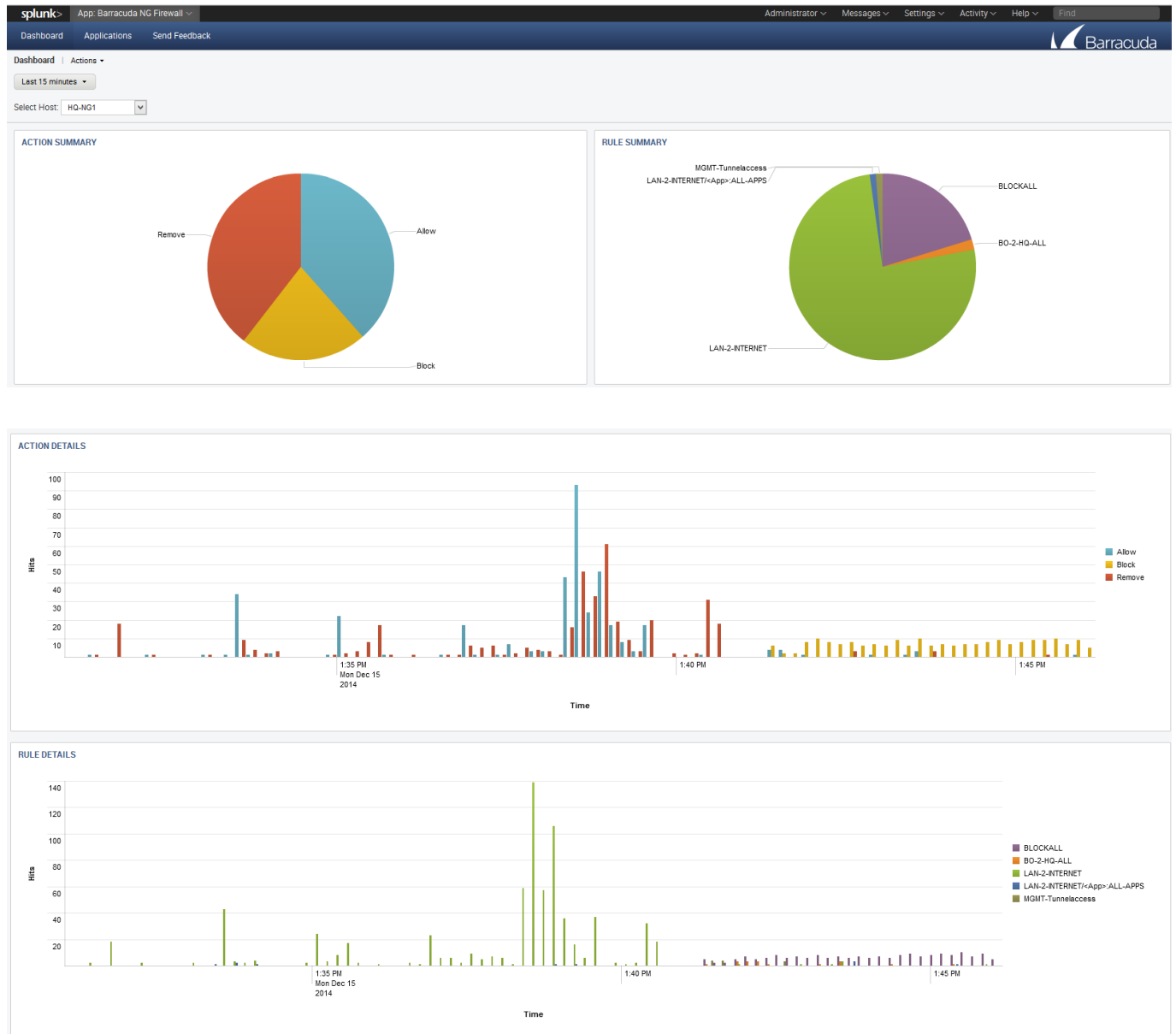
Step 5. The Barracuda NG Firewall Splunk App

Log into Splunk, and click on the Barracuda NG Firewall app on the Splunk dashboard. Select the Barracuda NG Firewall from the **Select Host** dropdown menu, and then select the **time span** for the query.



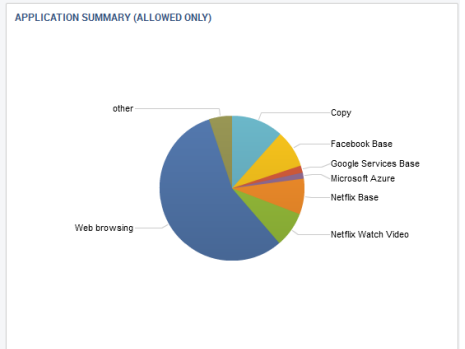
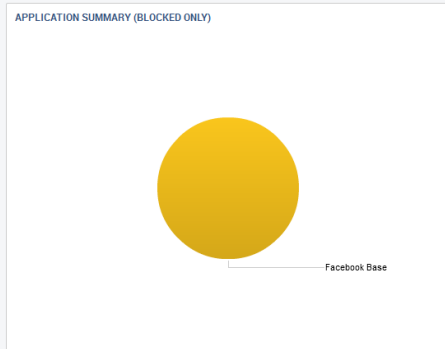
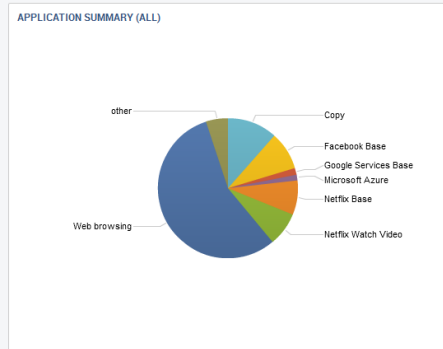
Barracuda NG Firewall Dashboard

The app allows you to display connection information based on a fixed time period or in real-time via Barracuda NG Firewall host.



Barracuda NG Firewall Applications

Click on the **Applications** tab of the Barracuda NG Firewall Splunk plugin to view Application Control 2.0 data, such as detected and blocked applications and websites blocked by URL Filter policies.



TOP 10 APPLICATIONS (ALL)

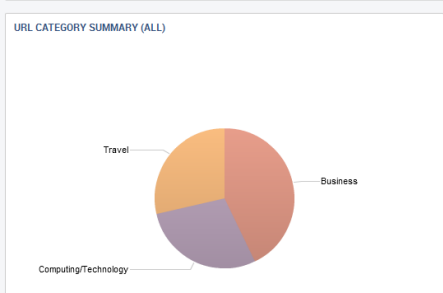
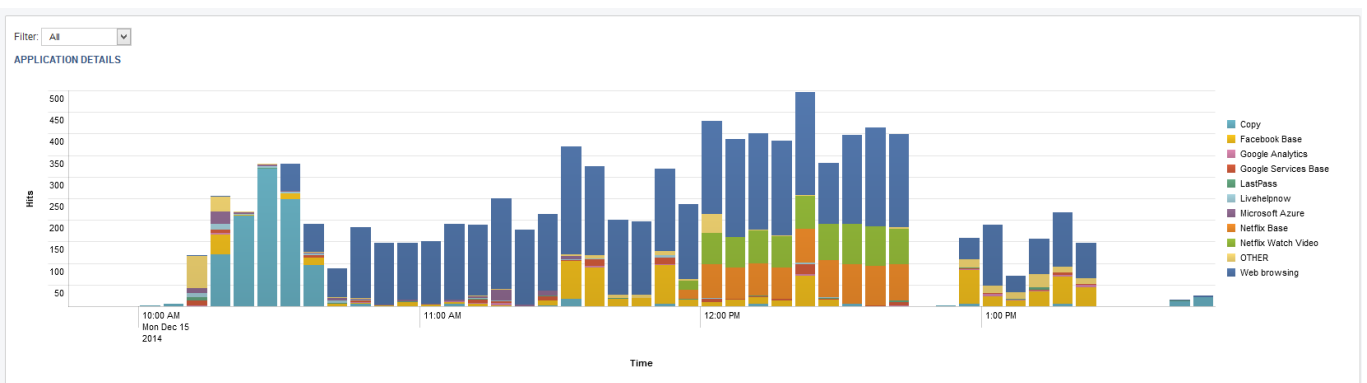
application	Hits	Percentage
1 Web browsing	5288	55.93
2 Copy	1090	11.53
3 Facebook Base	832	8.80
4 Netflix Base	751	7.94
5 Netflix Watch Video	738	7.81
6 Google Services Base	148	1.57
7 Microsoft Azure	124	1.31
8 Livehelpnow	66	0.70
9 Google Analytics	52	0.55

TOP 10 APPLICATIONS (BLOCKED ONLY)

application	Hits	Percentage
1 Facebook Base	44	100.00

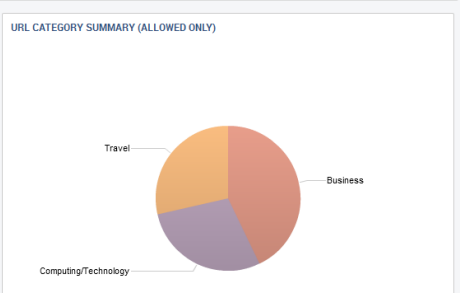
TOP 10 APPLICATIONS (ALLOWED ONLY)

application	Hits	Percentage
1 Web browsing	5288	50.20
2 Copy	1090	11.58
3 Facebook Base	788	8.37
4 Netflix Base	751	7.98
5 Netflix Watch Video	738	7.84
6 Google Services Base	148	1.57
7 Microsoft Azure	124	1.32
8 Livehelpnow	66	0.70
9 Google Analytics	52	0.55



URL CATEGORY SUMMARY (BLOCKED ONLY)

No results found. Inspect ...



Figures

1. splunk_top.png
2. splunk_syslog01.png
3. splunk_syslog01a.png
4. splunk_syslog02.png
5. splunk_syslog03.png
6. splunk_syslog04.png
7. splunk_app_logging1.png
8. splunk_select1.png
9. splunk_dash1.png
10. splunk_dash2.png
11. splunk_app1.png
12. splunk_app2.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.