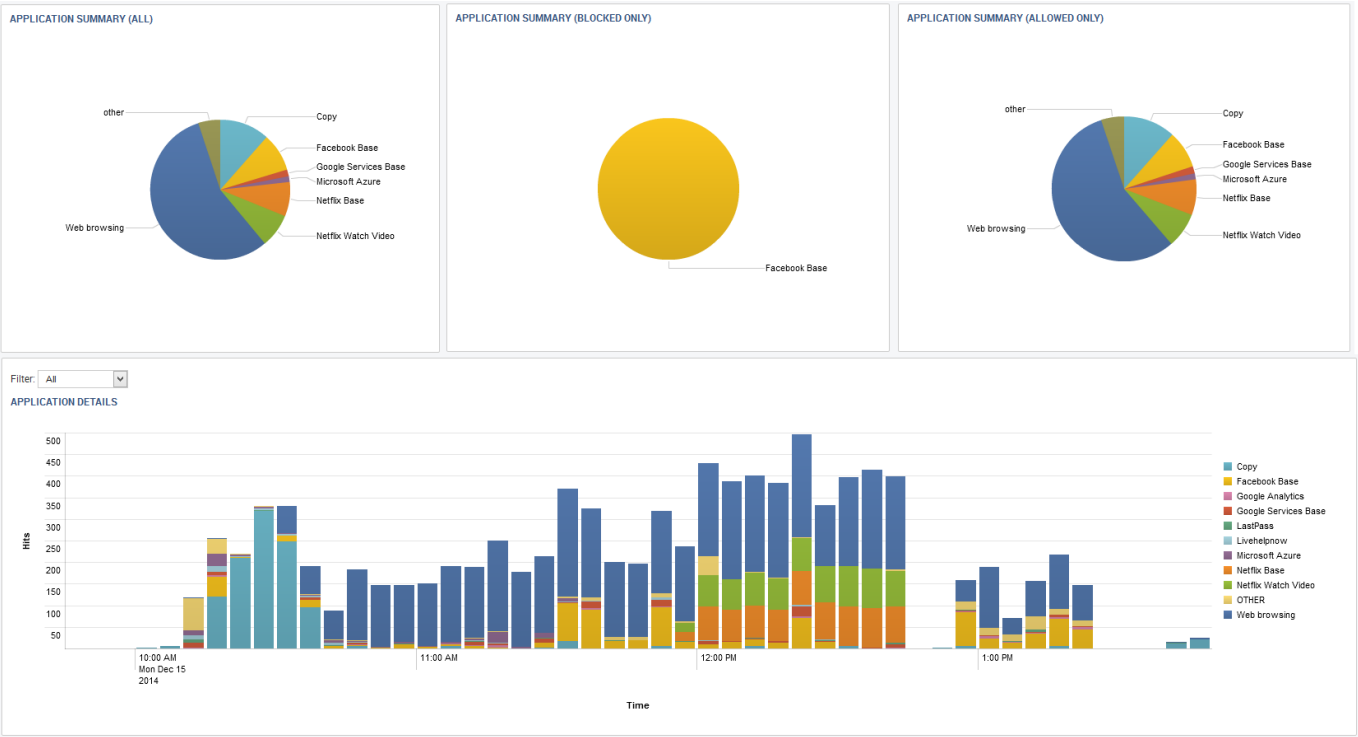
Splunk Integration

https://campus.barracuda.com/doc/96026552/

Splunk is a third-party platform for operational intelligence that allows you to monitor websites, application servers, and networks. The Barracuda CloudGen Firewall app shows the 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. Currently, the following Splunk versions are supported: 6.0, 6.1, 6.2, 7.x, 8.x, and 9.x.



Before You Begin

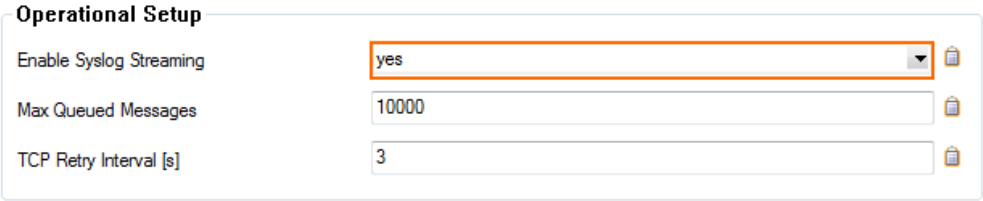
- Download the Barracuda CloudGen Firewall Splunk App from the Splunk Marketplace.
- Install the Barracuda CloudGen Firewall Splunk App on your Splunk Server. For more information, see http://docs.splunk.com/Documentation/PCI/2.1.1/Install/InstalltheAppManually.

Step 1. Configure Syslog Streaming on a Barracuda CloudGen Firewall

Configure and enable syslog streaming for every Barracuda CloudGen 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**.



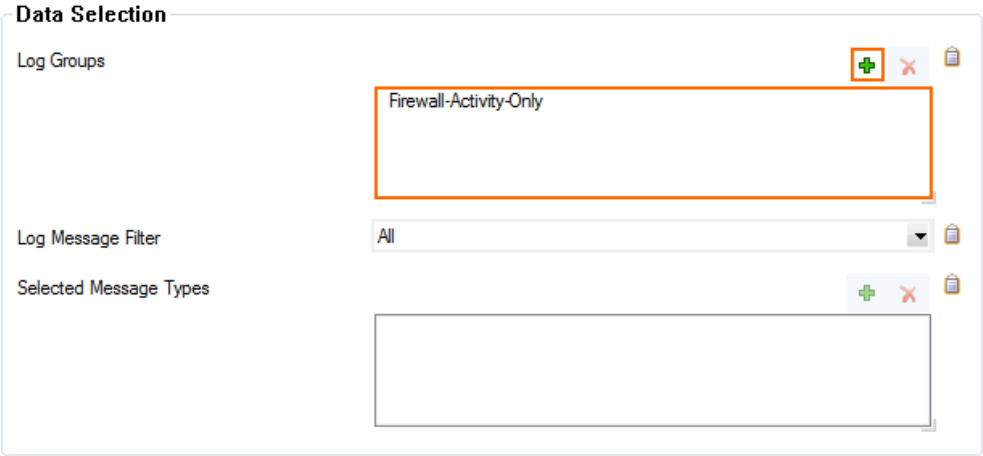
4. Click **Send Changes** and **Activate**.

Step 1.2. Configure Logdata Filters

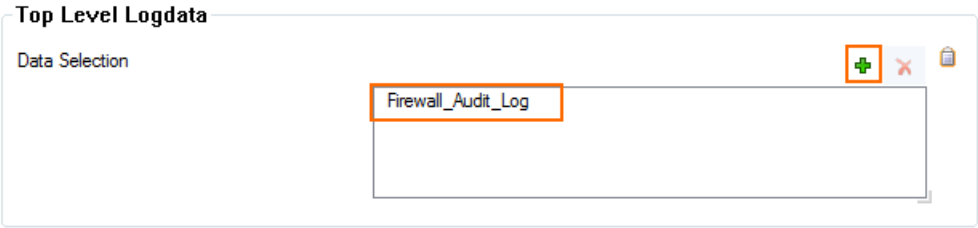
Define profiles specifying the log file types to be transferred/streamed.

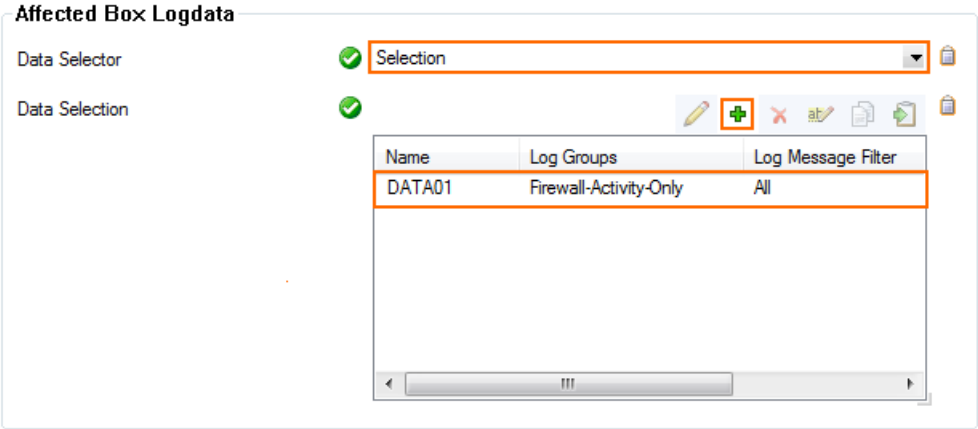
1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming.**
2. In the left menu, select **Logdata Filters**.
3. Click **Lock**.
4. Click the **+** icon to add a new filter.
5. Enter a **Name** and click **OK**. The **Filters** window opens.
6. Click **+** in the **Data Selection** table and select **Firewall_Audit_Log**.

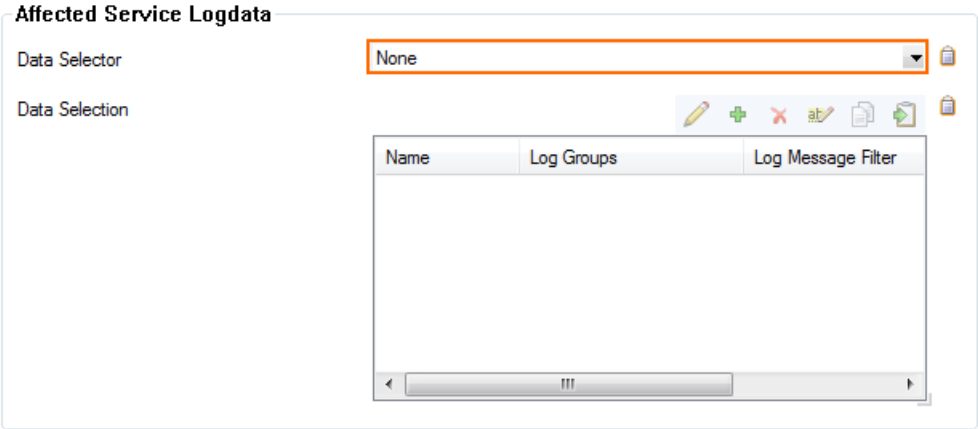
   Fatal_log and **Panic_log** data can also be streamed to the Splunk server, but are currently not processed by the Barracuda CloudGen Firewall F Series Splunk app.
7. In the **Affected Box Logdata** section select **Selection** from the **Data Selector** dropdown.
8. Click **+** to add a **Data Selection**. 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**.**



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







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

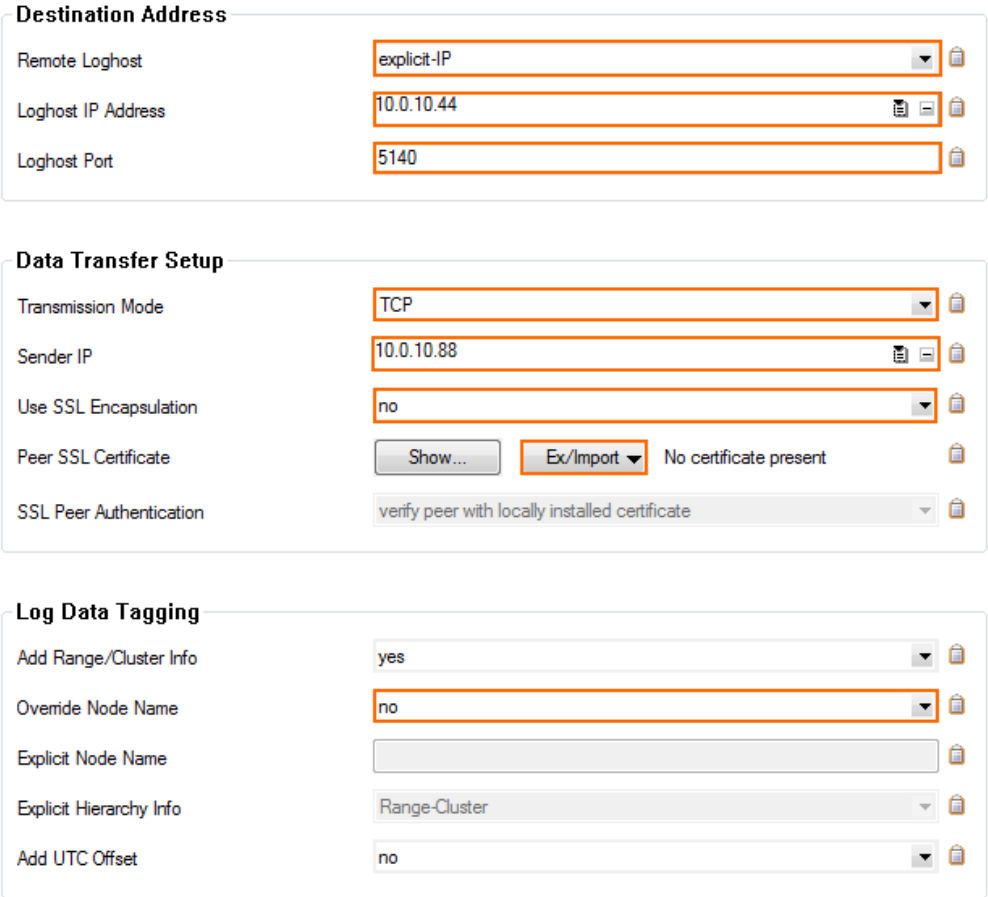
Step 1.3 Configure the Logstream Destinations

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 CloudGen 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 CloudGen Firewall or leave it blank for the CloudGen 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**.



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.

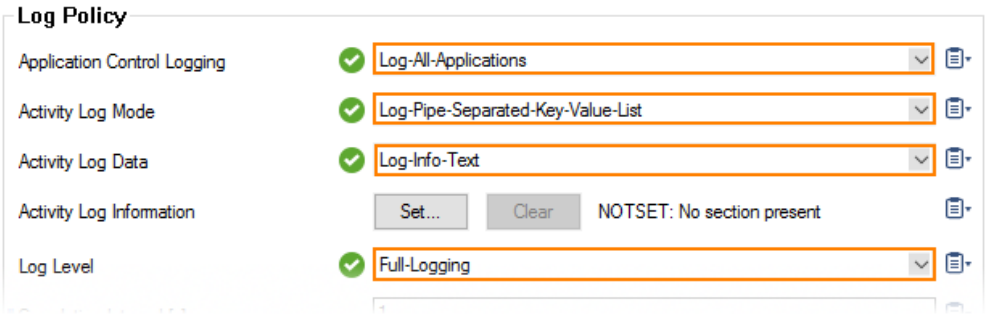
8. Click **OK.**
9. Click **Send Changes** and **Activate**.

Step 1.5 Configure Audit and Reporting

Configure the settings for log policies:

1. Go to ***your CloudGen Firewall*** **> Infrastructure Services > General Firewall Configuration**.
2. In the **Configuration Mode** section of the left menu, click **Switch to Advanced View**.
3. In the left menu, click **Audit and Reporting**.
4. Click **Lock**.
5. In the section **Statistics Policy**, set **Generate Dashboard Information** to **yes**.
6. In the section **Statistics Policy**, set **Generate Monitor Information** to **yes**.

7. In the **Log Policy** section, set **Application Control Logging** to **Log-All-Applications**.
8. In the **Log Policy** section, set **Activity Log Mode** to **Log-Pipe-Separated-Value-List**.
9. In the **Log Policy** section, set **Activity Log Data to Log-Info-Text**.
10. In the **Log Policy** section, set **Log Level** to **Full-Logging**.



11. Click **Send Changes**.
12. Click **Activate**.

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

Step 2. 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 CloudGen 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 CloudGen Firewall Splunk App

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

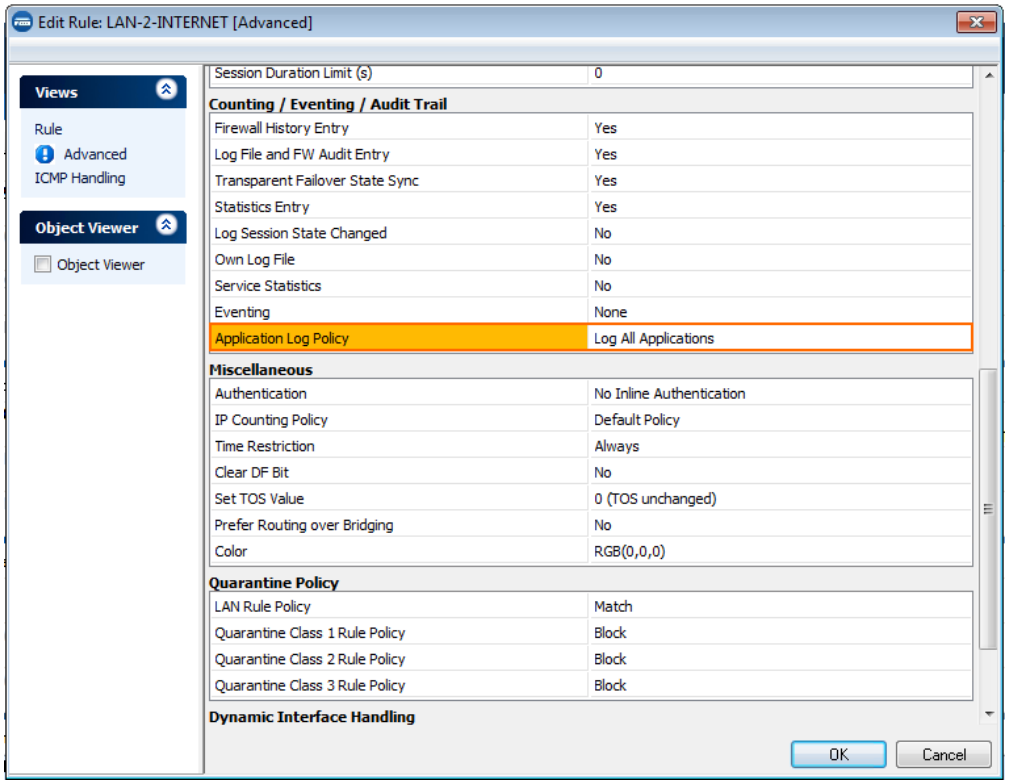
Certificate Troubleshooting

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:sslv3 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 the traffic you want to include in the data collected on the Splunk server. For more information, see [Advanced Access Rule Settings](#).

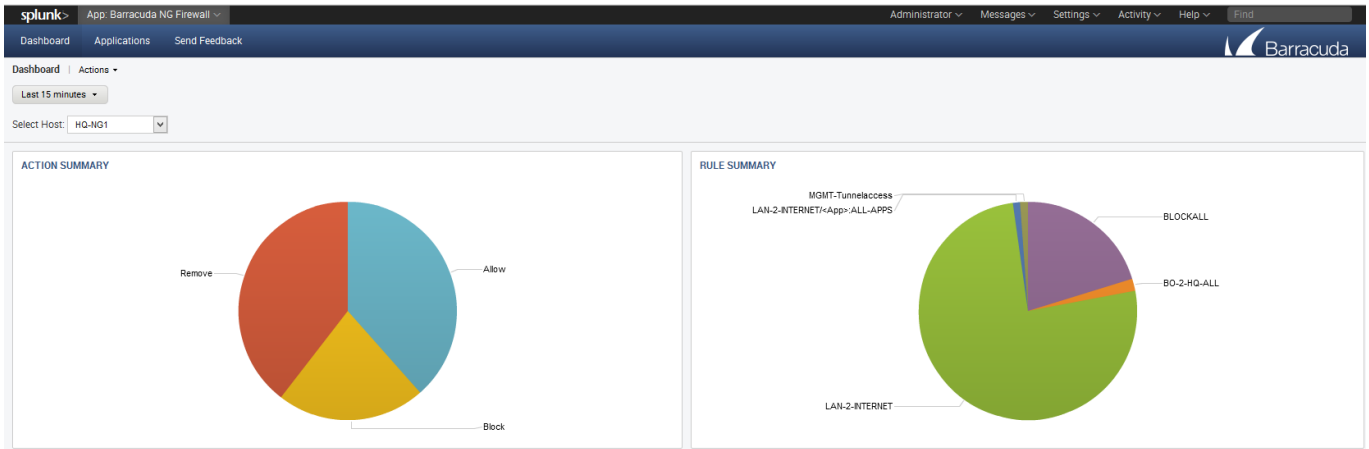


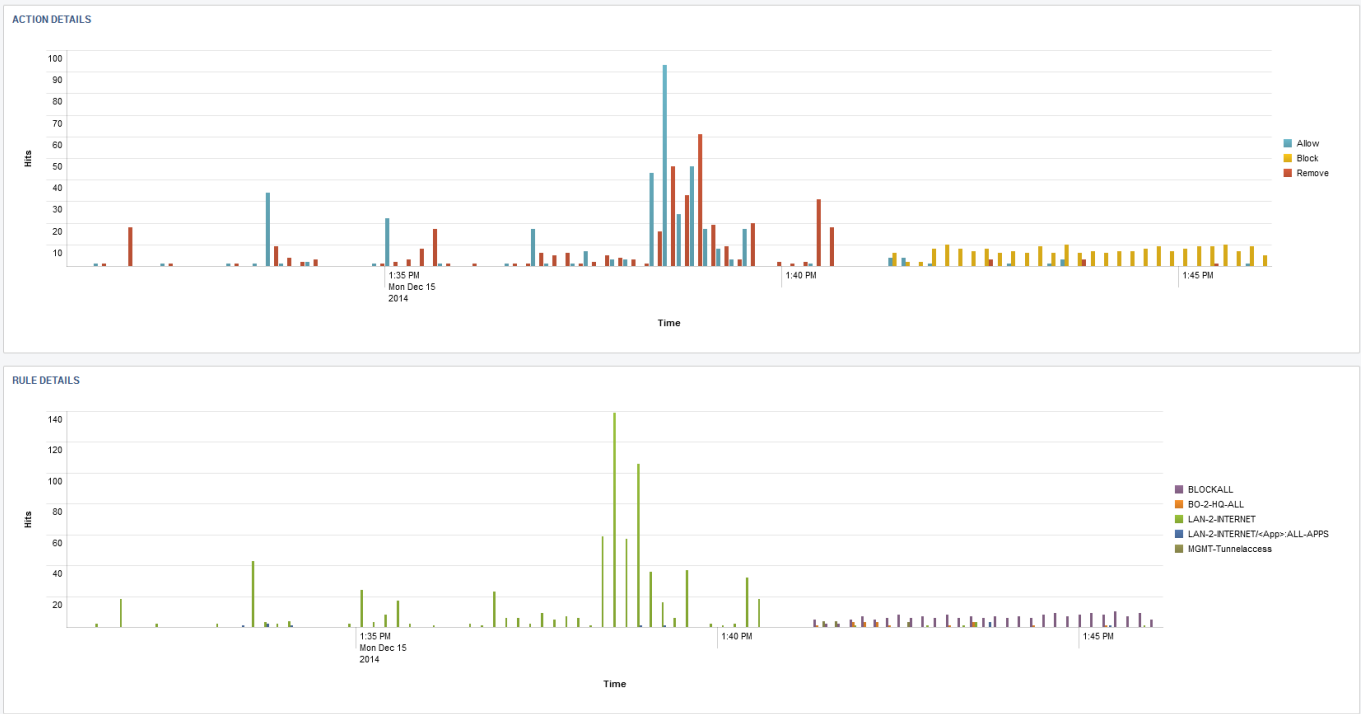
Step 5. The Barracuda CloudGen Firewall Splunk App

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

Barracuda CloudGen Firewall Dashboard

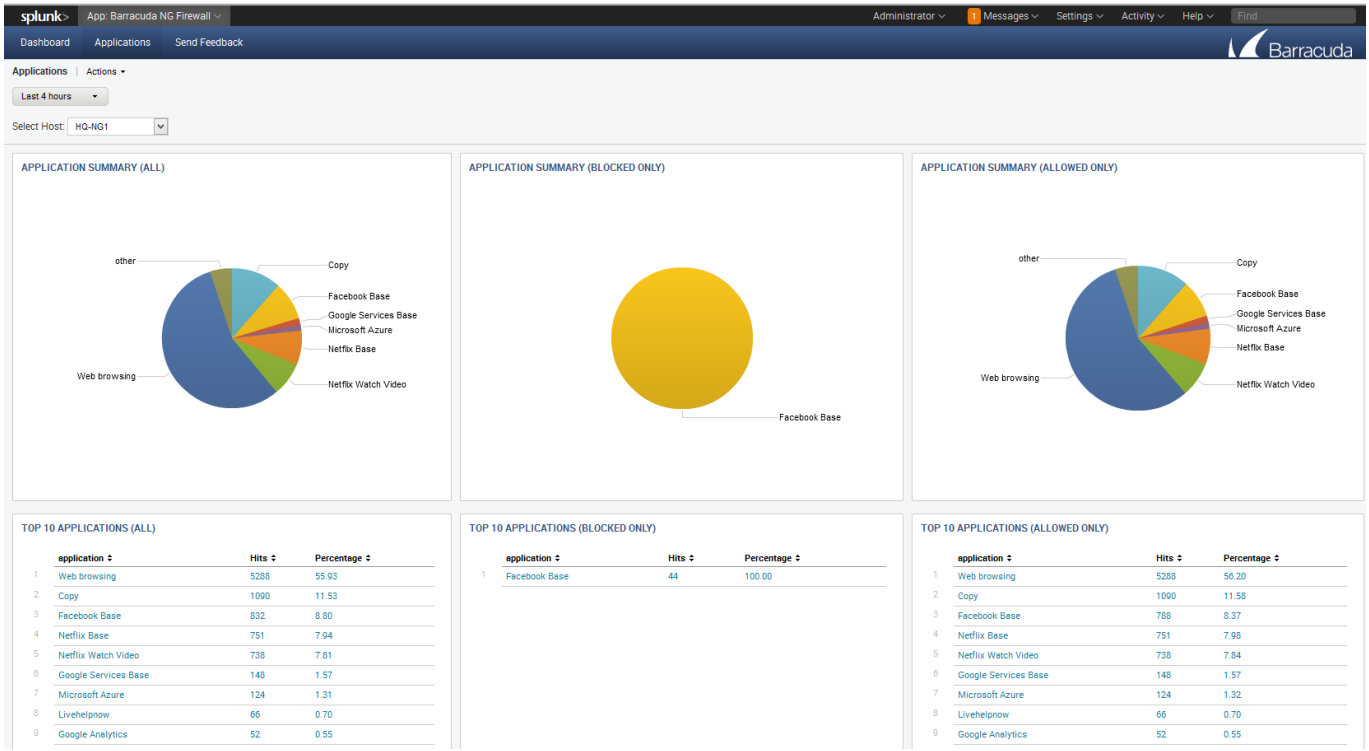
The app allows you to display connection information based on a fixed time period or in real time via Barracuda CloudGen Firewall host.

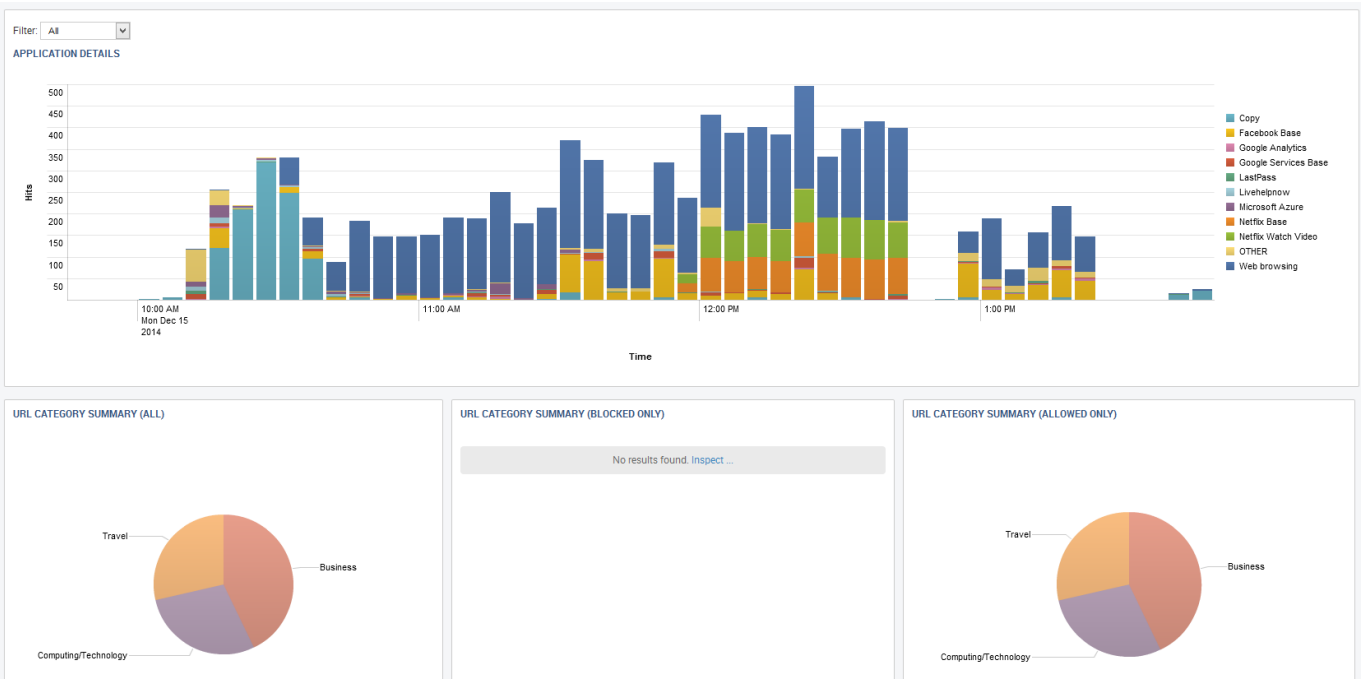




Barracuda CloudGen Firewall Applications

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




Filter: All
APPLICATION DETAILS
Hits
500
450
400
350
300
250
200
150
100
50
10:00 AM
Mon Dec 15
2014
11:00 AM
12:00 PM
1:00 PM
Time
Copy
Facebook Base
Google Analytics
Google Services Base
LastPass
Livehelpnow
Microsoft Azure
Netflix Base
Netflix Watch Video
OTHER
Web browsing
URL CATEGORY SUMMARY (ALL)
Travel
Business
Computing/Technology
URL CATEGORY SUMMARY (BLOCKED ONLY)
No results found. Inspect ...
URL CATEGORY SUMMARY (ALLOWED ONLY)
Travel
Business
Computing/Technology

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. statistics_policy_for_splunk_integration.png
8. audit_and_reporting_for_splunk_integration_v2.png
9. splunk_app_logging1.png
10. splunk_select1.png
11. splunk_dash1.png
12. splunk_dash2.png
13. splunk_app1.png
14. splunk_app2.png