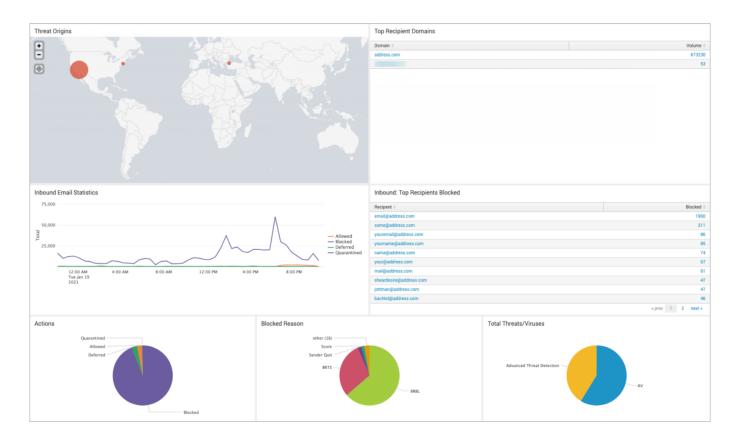


# **Splunk Integration**

#### https://campus.barracuda.com/doc/96023035/

Note that *Barracuda Email Security Service* and *Email Gateway Defense* are interchangeable in the Campus documentation and Splunk Marketplace user interface for the Barracuda Splunk app.

The Barracuda Splunk app collects data from Email Gateway Defense and utilizes Splunk to provide aggregated and individual visualizations. Administrators can view a number of different metrics, including but not limited to inbound and outbound mail, top sender/recipients, actions taken, and detected threats. Data is imported into Splunk via syslog streaming of the Message log. The Splunk dashboard can be exported to PDF format for easy distribution.



## Install the Email Gateway Defense Splunk App

- 1. Log into your Splunk interface.
- 2. In the left-hand navigation, click **Find more apps**.
- 3. Search for Barracuda. Once you find Barracuda Email Gateway Defense, click Install.
- 4. Log in with your Splunk.com credentials to download the app. If you do not have one, create



one for free here: <u>https://login.splunk.com/</u>.

Note that you sign into Splunk with your username, not your email address. Your username is configured when you created your Splunk account.

#### 5. Click Open app.

Alternatively, go to https://<your-splunk-instance>/en-US/app/BarracudaESS/ess.

### **Enable the Data Listener**

- 1. Go to **Settings > Data Inputs**.
- 2. Select TCP.
- 3. Click Enable.

### **Configure Certificates for Syslog and TLS**

The Barracuda Splunk app requires you to configure SSL encryption for communication between Barracuda Networks and Splunk.

- 1. Log into the Splunk server via SSH.
- Generate the certificate using the following command: sudo /opt/splunk/bin/splunk createssl server-cert -d /opt/splunk/etc/auth -n splunk -c splunk -p
  - For the PEM passphrase, enter password.
    - Hit **Enter** for all the other inputs.
- 3. Open the following file and add a section for SSL:
  - sudo vim /opt/splunk/etc/apps/BarracudaESS/default/inputs.conf
    [SSL]

serverCert=/opt/splunk/etc/auth/splunk.pem
password=password
requireClientCert=false
rootCA=/opt/splunk/etc/auth/cacert.pem

 Restart Splunk using the following command: sudo /opt/splunk/bin/splunk restart.

### Verify Splunk is Listening on the Proper Ports

Verify that the service is listening on the appropriate port using netstat or a similar utility.

[splunk-user@ip-172-30-22-95 default]\$ netstat -tln



Active	Active Internet connections (only servers)								
Proto	Recy	-Q Send-Q Local Ad	dress F	oreign Address	State				
tcp	0	0 0.0.0.0:8088	0.0.0.0:*	LISTEN					
tcp	0	0 0.0.0.0:8089	0.0.0.0:*	LISTEN					
tcp	0	0 127.0.0.1:25	0.0.0.0:*	LISTEN					
tcp	0	0 0.0.0.0:8191	0.0.0.0:*	LISTEN					
tcp	0	0 0.0.0.0:8000	0.0.0.0:*	LISTEN					
tcp	0	0 127.0.0.1:8065	0.0.0.0:*	* LISTEN					
tcp	0	0 0.0.0.0:9997	0.0.0.0:*	LISTEN					
tcp	0	0 0.0.0.0:111	0.0.0.0:*	LISTEN					
tcp	0	0 0.0.0.0:6515	0.0.0.0:*	LISTEN					
tcp	0	0 0.0.0.0:22	0.0.0.0:*	LISTEN					

#### **Certificate Troubleshooting**

Most syslog servers can be configured to check client certificates. Barracuda syslog clients currently use a self-signed client certificate. Thus, if the syslog server validates client certificates, syslog messages can be rejected. To avoid this error, turn off syslog client certificate validation for Email Gateway Defense or add the certificate to a trusted certificate configuration.

### **Configure Email Gateway Defense to Send Syslog to Splunk**

- 1. Log into Email Gateway Defense and navigate to the **Account Management** tab.
- 2. Enter the public IP address of your Splunk instance and port 6515.

Syslog Integration				
IP Address / Hostname	Port	Actions		
TCP+TLS is required to connect successfully. Non-TLS is not supported	6515	Test	Delete	Server Status: Port Reachable

For more information, see the Email Gateway Defense Syslog Integration.

### **Barracuda Splunk App**

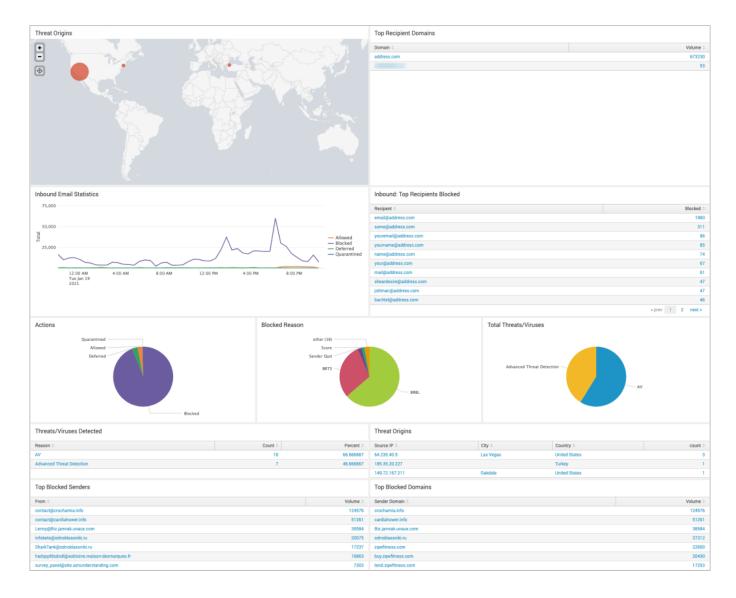
Log into Splunk, and click on the Barracuda app on the Splunk dashboard. Select the **Time Range** and **Domain** for the query.



splunk	> App: Ban	racuda ESS 🗸	,					
Search	Datasets	Reports	Alerts	Dashboards	Barracuda Em	nail Security Service		
Barracuda Email Security Service								
Time Rang	ge		Domai	n				
Last 24	hours		✓ All		• •	Hide Filters		

#### **Barracuda Splunk Dashboard**

The app allows you to display domain statistics information based on a relative period (i.e. last 30 days) or real-time window (i.e. 1 minute).





### **Examples of Additional Splunk Queries**

#### **Top PTR Records**

```
sourcetype=BarracudaESSJSON dst_domain=$destDomain$ ptr_record
| where isnotnull(account_id) and len(account_id) > 0
| foreach ptr_record [ eval ptr_record = if(isnull(ptr_record) OR
len(ptr_record)==0, "No PTR Record", ptr_record) ]
| top showperc=false limit=20 ptr_record
| rename "ptr_record" as "PTR Record", "count" as "Volume"
```

#### Popular Subjects

```
sourcetype=BarracudaESSJSON dst_domain=$destDomain$
| where isnotnull(account_id) and len(account_id) > 0
| top showperc=false limit=20 "subject"
| rename "subject" as "Subject", "count" as "Count"
```

# Email Gateway Defense



#### Figures

- 1. ess\_splunk1.png
- 2. netstat.png
- 3. splunk\_syslog1.png
- 4. essSplunkDash.png
- 5. ess\_splunk2.png

© Barracuda Networks Inc., 2025 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.