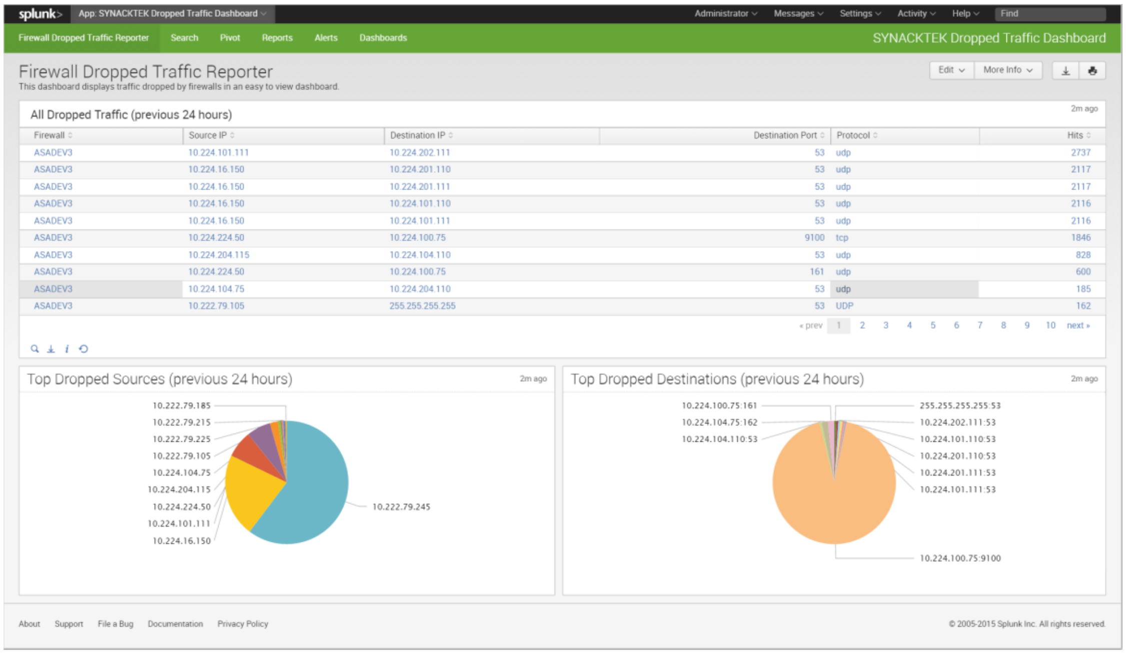
Firewall Dropped Traffic Reporter

Contents

Overview

This application uses fields defined in the Common Information Model to harvest and display details about network traffic dropped by firewalls. This is useful for base lining and monitoring the traffic required by applications running in protected networks (servers in a DMZ, critical systems within electronic security perimeters, etc.).


splunk>
App: SYNACKTEK Dropped Traffic Dashboard
Administrator
Messages
Settings
Activity
Help
Find
Firewall Dropped Traffic Reporter
Search
Pivot
Reports
Alerts
Dashboards
SYNACKTEK Dropped Traffic Dashboard
Edit
More Info

Firewall Dropped Traffic Reporter

This dashboard displays traffic dropped by firewalls in an easy to view dashboard.

All Dropped Traffic (previous 24 hours)

2m ago

Firewall	Source IP	Destination IP	Destination Port	Protocol	Hits
ASADEV3	10.224.101.111	10.224.202.111	53	udp	2737
ASADEV3	10.224.16.150	10.224.201.110	53	udp	2117
ASADEV3	10.224.16.150	10.224.201.111	53	udp	2117
ASADEV3	10.224.16.150	10.224.101.110	53	udp	2116
ASADEV3	10.224.16.150	10.224.101.111	53	udp	2116
ASADEV3	10.224.224.50	10.224.100.75	9100	tcp	1846
ASADEV3	10.224.204.115	10.224.104.110	53	udp	828
ASADEV3	10.224.224.50	10.224.100.75	161	udp	600
ASADEV3	10.224.104.75	10.224.204.110	53	udp	185
ASADEV3	10.222.79.105	255.255.255.255	53	UDP	162

If you have the Splunk Add-on for Cisco ASA installed, the dashboards in this application will display information about traffic dropped by Cisco ASA, Cisco PIX, and Cisco Firewall Service Module devices without any additional configuration.

Firewall Dropped Traffic Reporter

Prerequisites

The following pre-requisites are required:

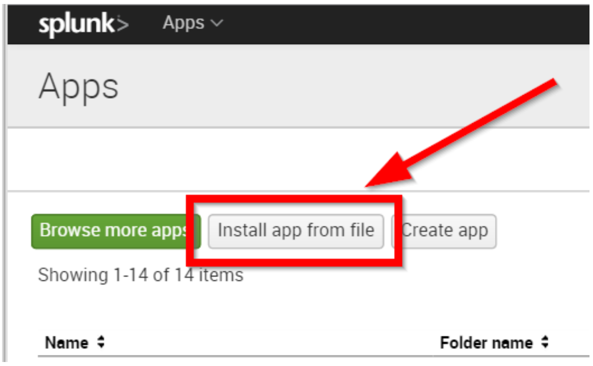
- Firewalls you wish to monitor using the dashboards in this application must be configured to send event data about dropped traffic to Splunk.

- Field extractions must exist for the following CIM defined fields: host, src_ip, dest_ip, dest_port, transport, and action.

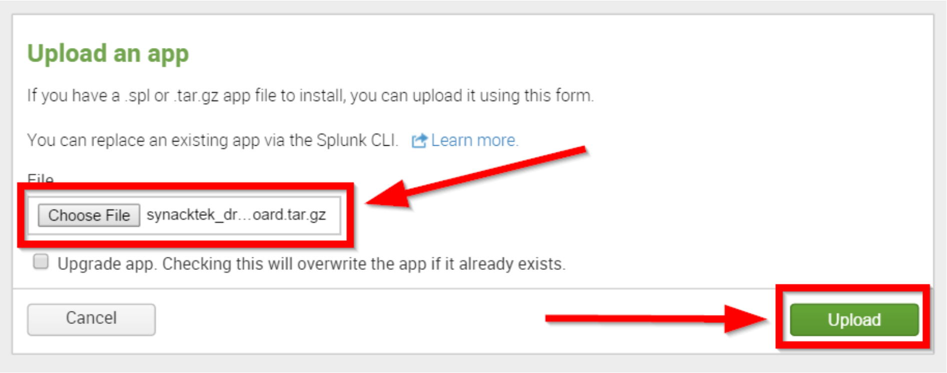
- Field extractions for Cisco ASA, PIX, and Firewall Service Module firewalls are available by installing the ***Splunk Add-on for Cisco ASA (https://apps.splunk.com/app/1620/)***. Extractions for devices from other manufacturers may be added to this application in future versions, or made available by other Splunk Add-ons or Technology Adapters.

Installation

To install this app, download the file compressed tar file for the most recent version from http://www.synacktek.com/dropped-traffic. Save this file on your system, then load it onto your Splunk server(s) by choosing **Apps / Manage Apps / Install app from file**.



Click the **Choose File** button, and find the installation archive file you downloaded from www.synacktek.com, then click the **Upload** button to install the app.


Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File: synacktek_dr...oard.tar.gz

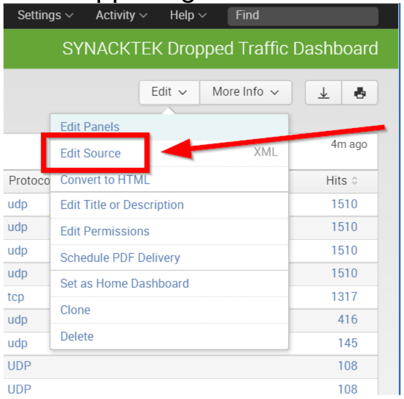
□ Upgrade app. Checking this will overwrite the app if it already exists.

Firewall Dropped Traffic Reporter

Configuration

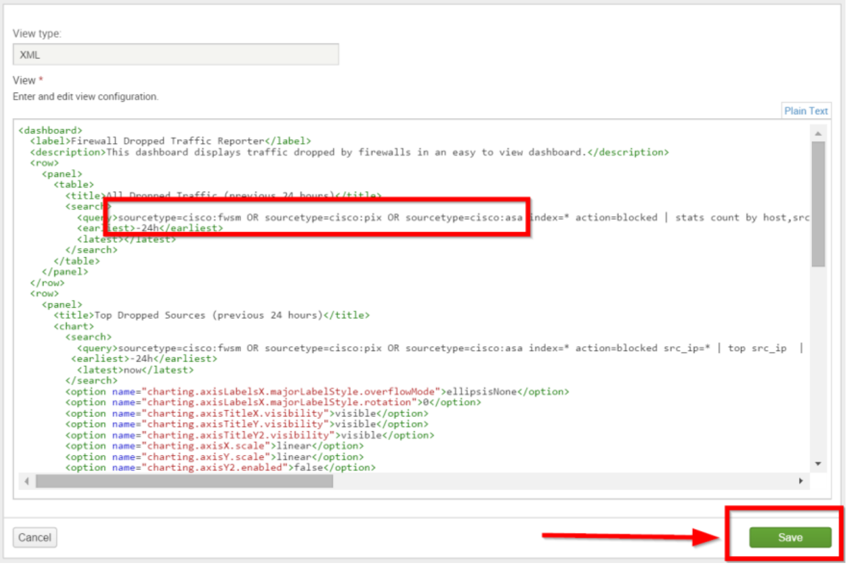
By default, the application dashboards are configured to look events that have ***action=blocked*** for the sourcetypes ***cisco:asa***, ***cisco:fwsm***, and ***cisco:pix.*** If you are using different sourcetype names for your data you will need to modify the dashboard to accommodate this.

To modify the sourcetypes used by the dashboard, open the ***SYNACKTEK Dropped Traffic Dashboard*** and select ***Edit Source*** from the ***Edit*** menu in the upper-right corner of the screen.



Protoco	Hits
udp	1510
udp	1510
udp	1510
udp	1510
tcp	1317
udp	416
udp	145
UDP	108
UDP	108

Once the source XML is open, find the ***<query>*** field and modify the list of sourcetypes being queried to match what you need for your environment. Click the ***Save*** button when your changes are complete.



```
<dashboard>
  <label>Firewall Dropped Traffic Reporter</label>
  <description>This dashboard displays traffic dropped by firewalls in an easy to view dashboard.</description>
  <row>
    <panel>
      <table>
        <title>All Dropped Traffic (previous 24 hours)</title>
        <search>
          <query>sourcetype=cisco:fwsm OR sourcetype=cisco:pix OR sourcetype=cisco:asa index=* action=blocked | stats count by host,src
          <earliest>-24h</earliest>
          <latest></latest>
        </search>
      </table>
    </panel>
  </row>
  <row>
    <panel>
      <title>Top Dropped Sources (previous 24 hours)</title>
      <chart>
        <search>
          <query>sourcetype=cisco:fwsm OR sourcetype=cisco:pix OR sourcetype=cisco:asa index=* action=blocked src_ip=* | top src_ip  |
         <earliest>-24h</earliest>
          <latest>now</latest>
        </search>
        <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>
        <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>
        <option name="charting.axisTitleX.visibility">visible</option>
        <option name="charting.axisTitleY.visibility">visible</option>
        <option name="charting.axisTitleY2.visibility">visible</option>
        <option name="charting.axisX.scale">linear</option>
        <option name="charting.axisY.scale">linear</option>
        <option name="charting.axisY2.enabled">false</option>
```

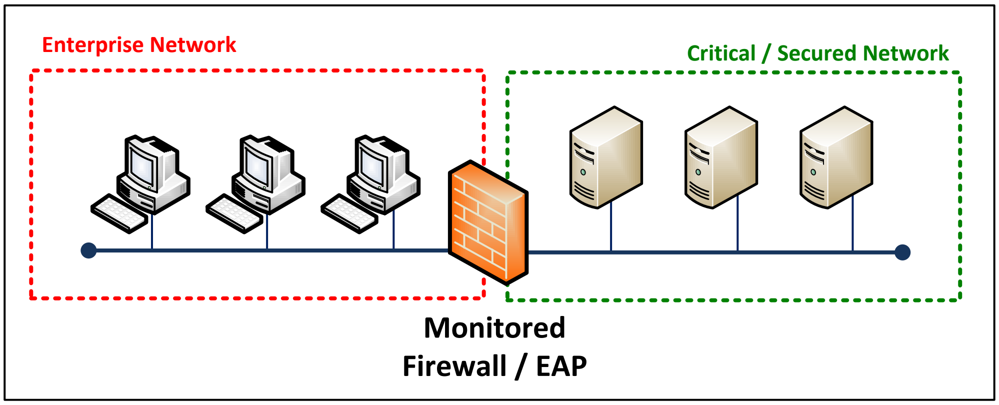
Note that you can make other changes to the search criteria by editing the XML source as well. If you want to exclude events from specific hosts, for example, you could add the text ***NOT host=<host_to_exclude>*** in the query field.

Firewall Dropped Traffic Reporter

Use Cases

The dashboards included in this application are designed for hardening and monitoring secure systems within your larger enterprise network; security zones where you can quantify the expected inbound and outbound traffic you should see traversing your security boundaries.

Events generated by security devices connected to the public Internet may generate a lot of noise and reduce the effectiveness of the dashboards; you may need to modify the dashboards to omit events from edge devices.



The following are some specific use cases this where this application can be best used:

System Hardening – When implementing a new system in a secured environment it can be difficult to identify all the traffic that needs to be white-listed in your security devices. More often than not, this becomes a trial-and-error process that requires security engineers to monitor traffic attempting to traverse a firewall, then either adding policies to permit the traffic or disabling the unneeded services which are generating the traffic. The dashboards provided in this application make it easy to find traffic being dropped by source, destination, or frequency so it can be addressed.

NERC CIP ESP Monitoring – ICS and Control Center networks used to support NERC CIP assets for electrical utilities require comprehensive monitoring to detect unexpected traffic. Luckily, the traffic footprints in these environments can be made very predictable. By capturing events from your electronic access points and displaying them in the dashboards provided by this app you can quickly detect unauthorized traffic and determine its source.

Misconfiguration / Malicious Traffic Detection – Once your secure systems and security policies are normalized, you should see very little unexpected traffic being dropped by your security devices. Spikes in dropped traffic are typically either an indication of a misconfigured device, or the result of malicious traffic trying to cross your security boundaries. These spikes are easy to identify using the dashboards provided in this app.

Firewall Dropped Traffic Reporter

To Do List

The following is a list of updates we plan to make available to users of this application in the future:

- Provide field extractions (or links to other technology adapters) for additional network security devices
- Addition of a configuration page that will eliminate the need to manually edit the XML source code for the dashboards

Provide Feedback

Please let us know if there is additional functionality you would like to see out of this app for Splunk. You can contact us by sending e-mail to info@synacktek.com, or visit us at www.synacktek.com. We welcome your feedback, and would love to help you get more of what you need from your Splunk data!