



SECURITY
EAGLES

SPLUNK

Part 5

Introduction To Splunk

splunk >

Table of contents

Module 8: Creating Visualizations and Interactive Dashboards

- Understanding Chart Types and Visualizations 2
- Constructing a Static Dashboard (Fixed Content) 7
- Implementing a Shared Global Time Range Picker 13
- Creating Dynamic Forms with Token Management 19
- Improving Performance with Base Searches (Statistical Data) 24
- Base Searches for Time-Based Visualizations (Timecharts) 28
- Configuring Basic Drilldown Functionality 30
- Implementing Logic in Drilldowns 37
- Customizing Dashboard Navigation and Layout 41
- Next-Gen Dashboards An Exploration of Dashboard Studio 44

Understanding Chart Types and Visualizations

Visualizations are key to turning raw data into actionable insights. They help security analysts spot patterns and anomalies that might be missed in plain tables. Splunk makes this easy with built-in charts and the ability to add custom visualizations.

1. Built-in Splunk Visualizations

Splunk offers several ready-to-use charts like:

- **Line Chart**
- **Area Chart**
- **Bar Chart**
- **Pie Chart**
- **Single Value**
- **Maps**

These charts expect structured data: usually a **grouping field** (e.g., `http_user_agent`) and a **statistical measure** (e.g., `count`).



2. Extending Splunk Visualizations

Want more options? Splunkbase Apps let you add advanced charts like:

- **Timeline**
- **Punchcard**
- **Sankey**
- **Parallel Coordinates**

This flexibility ensures you can tailor visualizations for any security use case.

3. Preparing Data for Visualizations

The foundation of any chart is a search that outputs structured data. Example SPL:
`index=botsv2 sourcetype=stream:http* | stats count by http_user_agent`
 This creates a **Statistics table** listing each **http_user_agent** and its event count.



The screenshot shows the Splunk search interface with the query `index=botsv2 sourcetype=stream:http* | stats count by http_user_agent`. The results are displayed in a table with 40 rows, showing various user agents and their corresponding event counts.

http_user_agent	count
Microsoft BITS/7.5	1396
Microsoft-CryptoAPI/6.1	254
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	1032
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	192
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Microsoft Outlook 16.0.8229; ms-office; MSOffice 16)	222
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 1.1.4322; .NET4.0C)	30
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2)	78
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	48
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)	1888
Mozilla/4.0 (compatible;)	272
Mozilla/5.0 (MSIE 10.0; Windows NT 6.1; Trident/5.0)	2764

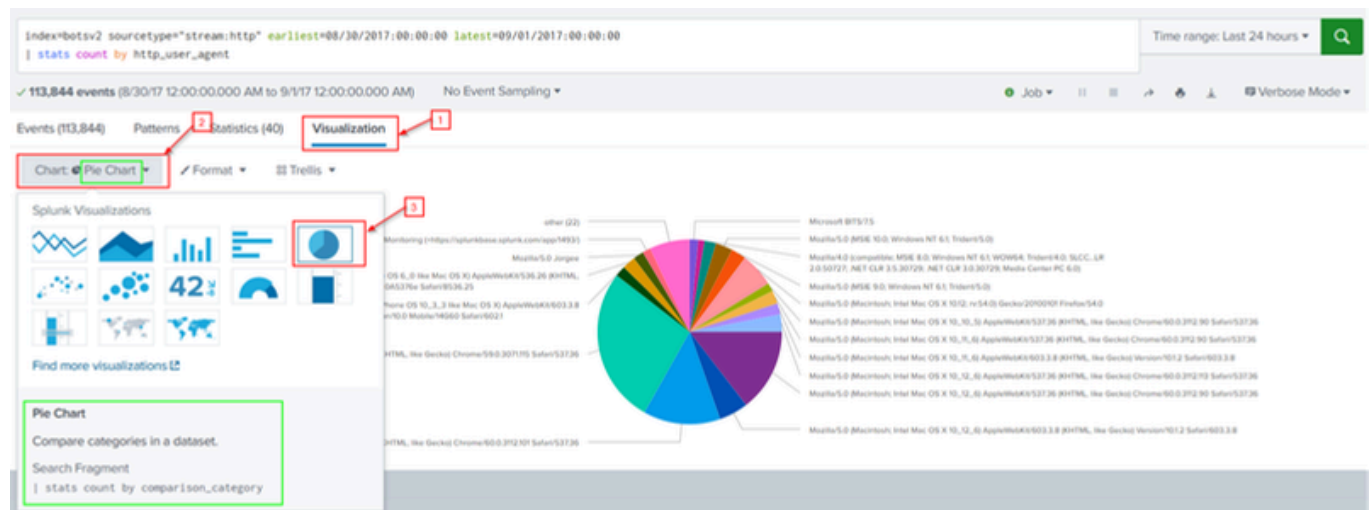
4. Detailed Visualizations and Formatting

A. Pie Charts - Compare Categories

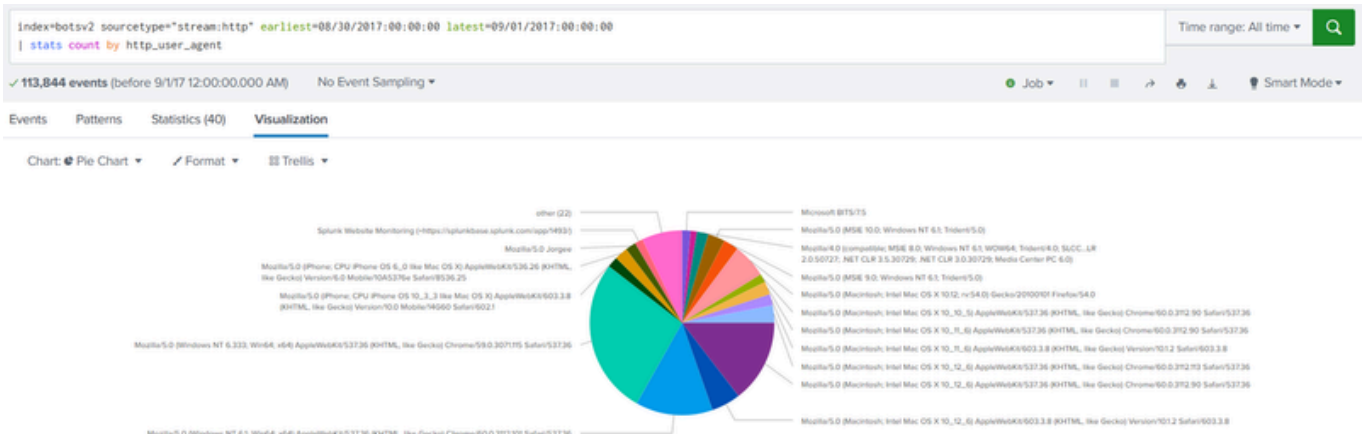
Pie charts show the proportion of each category in your dataset.

Steps:

- Go to **Visualization tab** → Select **Pie Chart**.



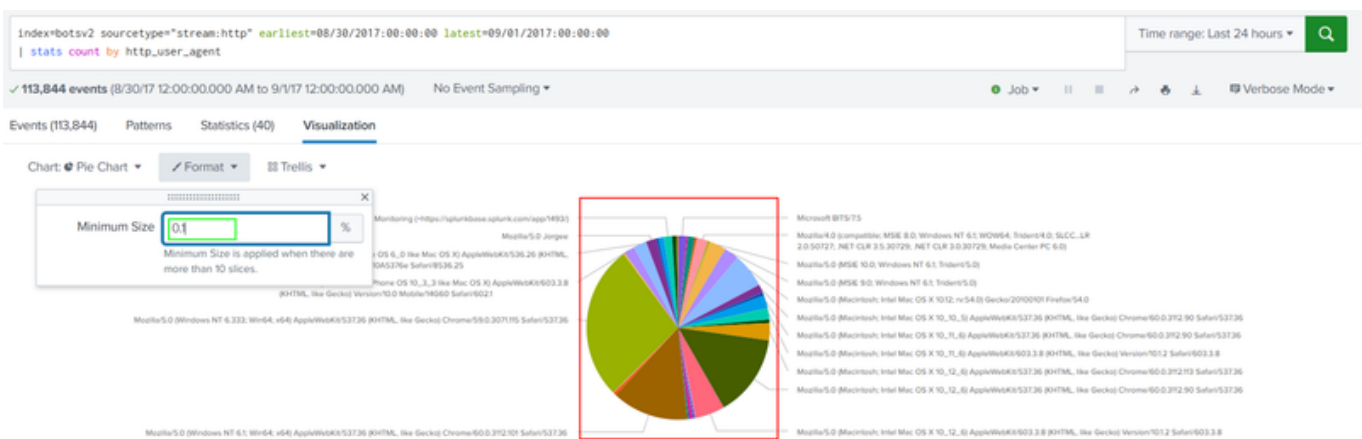
- Instantly see your data as a proportional chart.



Formatting Tip:

Use **Minimum Size** to group small slices into “Other” for clarity.

- Default: 1% → Groups tiny segments.
- Adjusted: 0.1% → Shows more detail for top contributors.

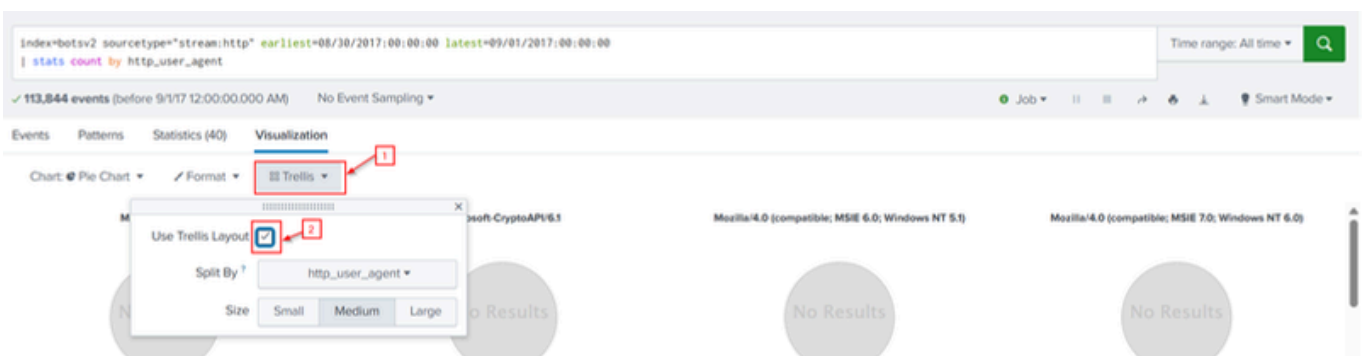


B. Trellis Layout - Multi-Panel Views

Trellis splits one chart into multiple panels for easy comparison.

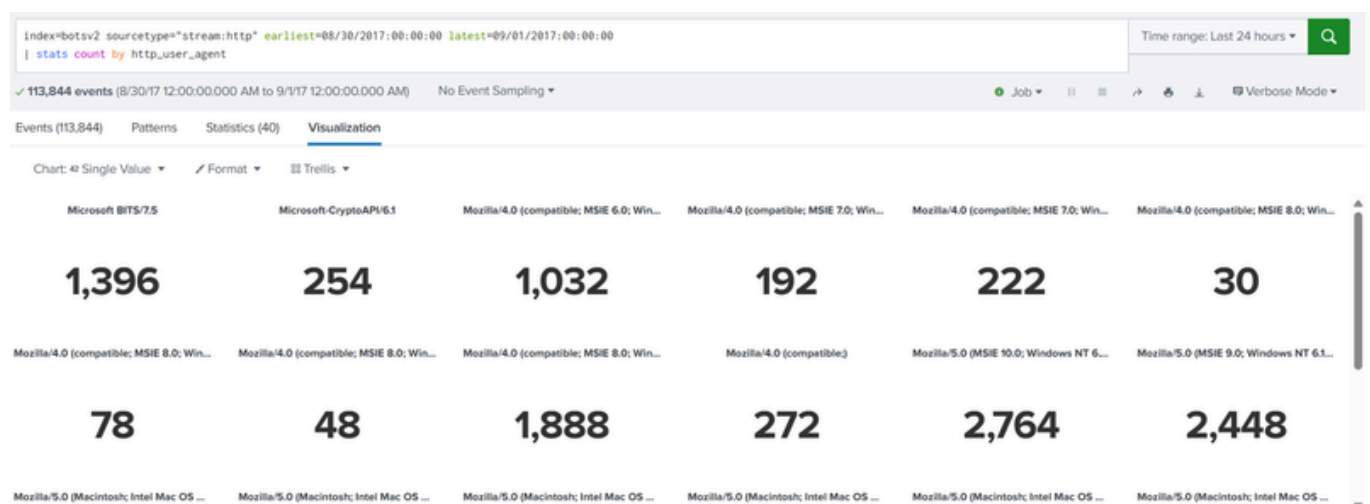
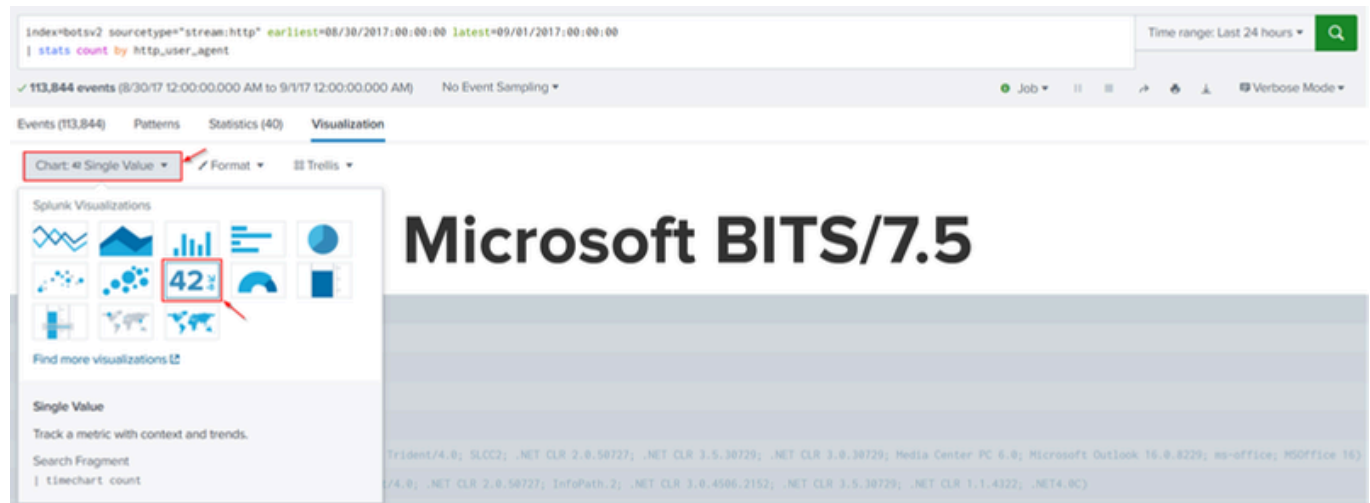
Steps:

- Enable **Trellis Layout**.
- Choose **Split By** field (e.g., `http_user_agent`).
- Adjust panel size.

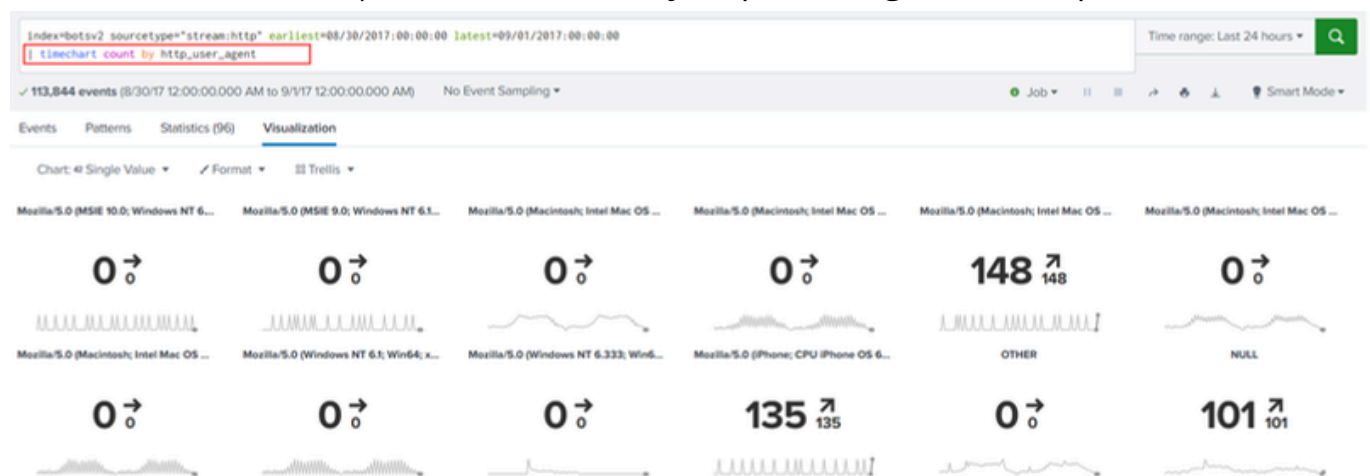


Examples:

- **Single Value Panels:** Show raw counts per user agent.



- **Timecharts:** Use `| timechart count by http_user_agent` to compare trends.



C. Maps – Geographical Analysis

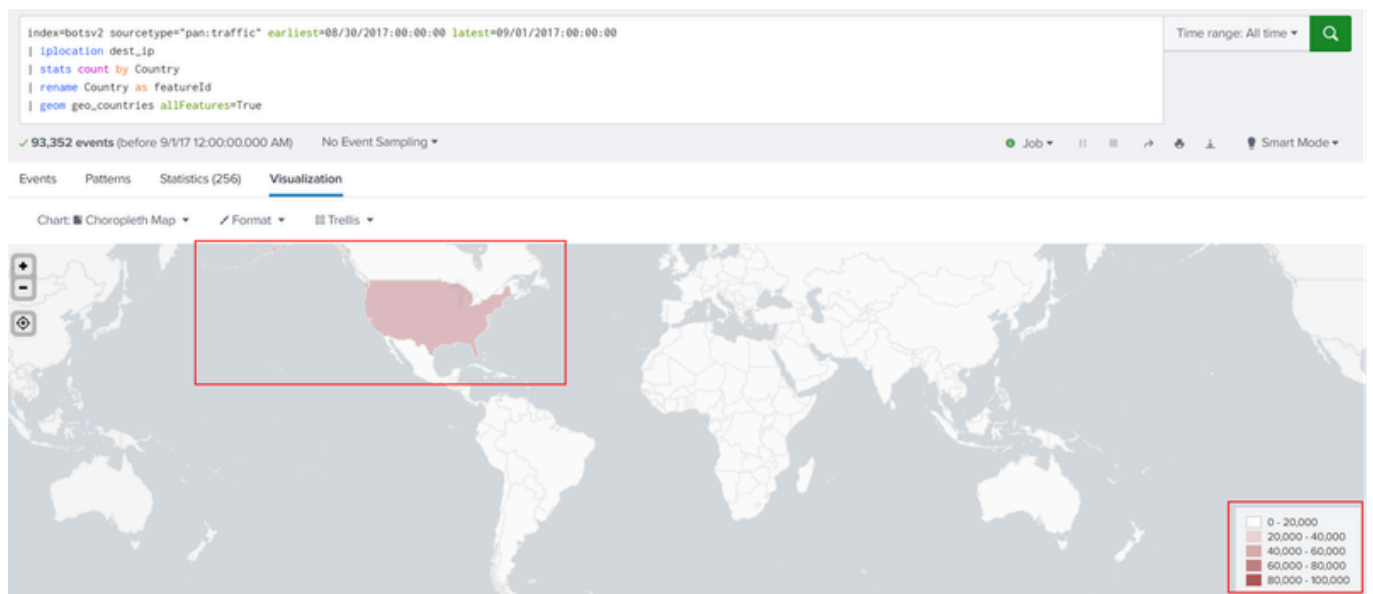
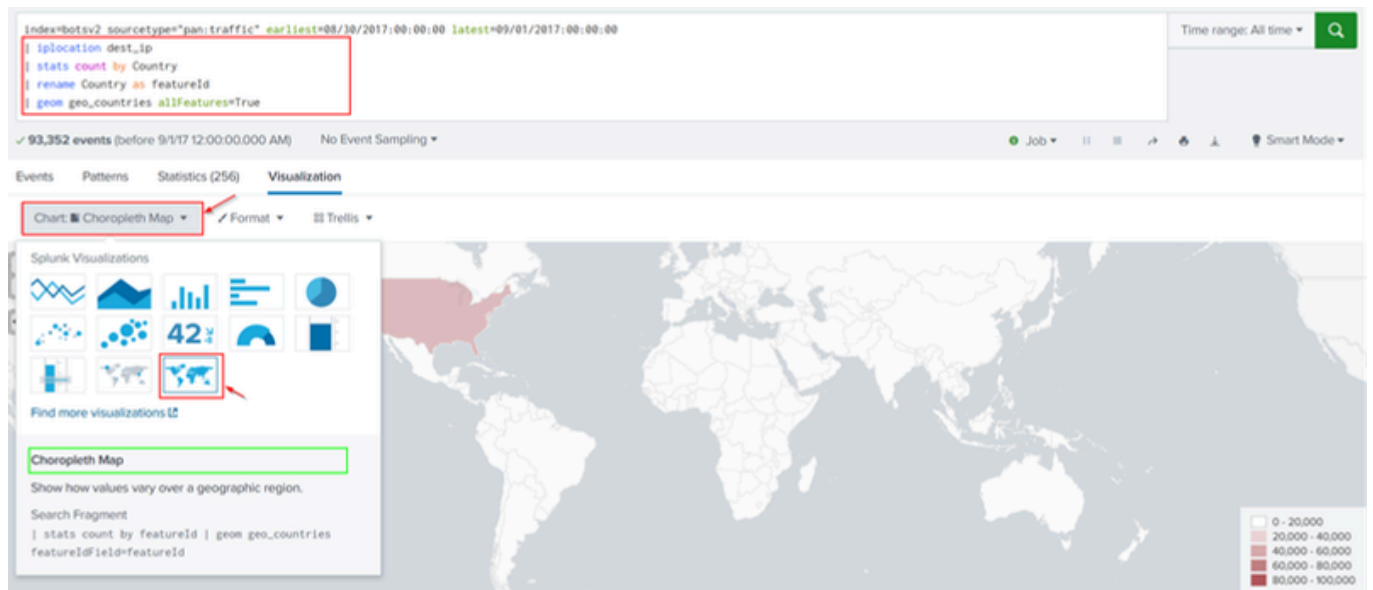
Maps visualize events by location (e.g., IP addresses).

SPL Chain:

```
| iplocation dest_ip  
| stats count by Country  
| rename Country as featureId  
| geom geo_countries allFeatures=True featureField=featureId
```

Visualization:

Select **Choropleth Map** to shade countries based on event count.



Constructing a Static Dashboard (Fixed Content)

A well-designed dashboard gives security teams a quick, actionable view of firewall traffic. Here's how to create a static, multi-panel dashboard in Splunk to monitor connections by IP, port, and network interface.

Step 1: Initialize the Dashboard with Core Traffic Panels

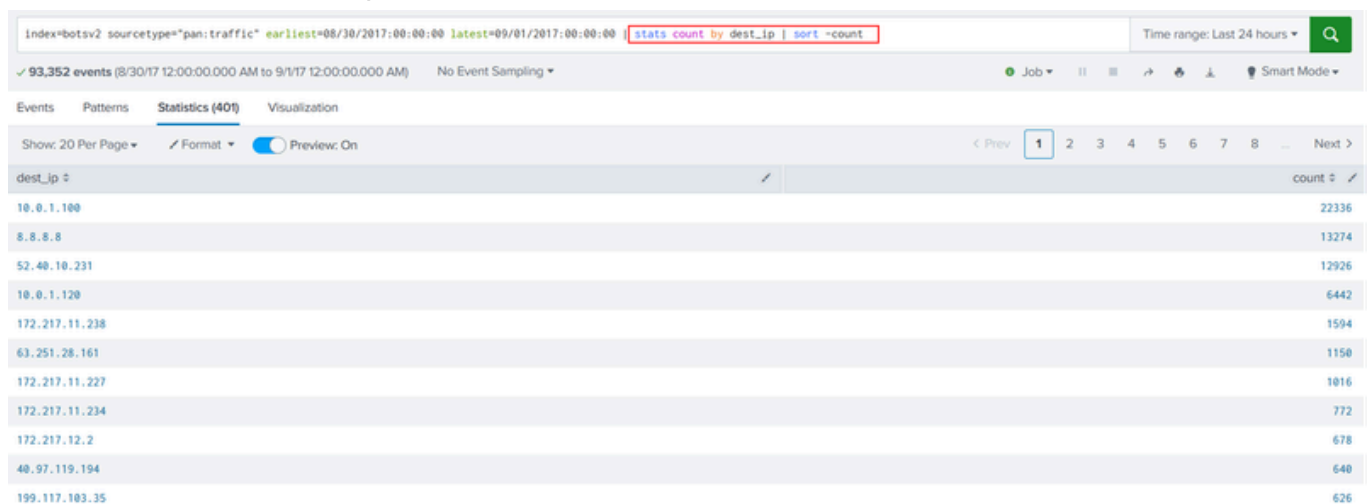
Start by identifying the top destination IPs.

SPL Example:

```
index=botsv2 sourcetype=pan:traffic | stats count by dest_ip | sort -count
```

Actions:

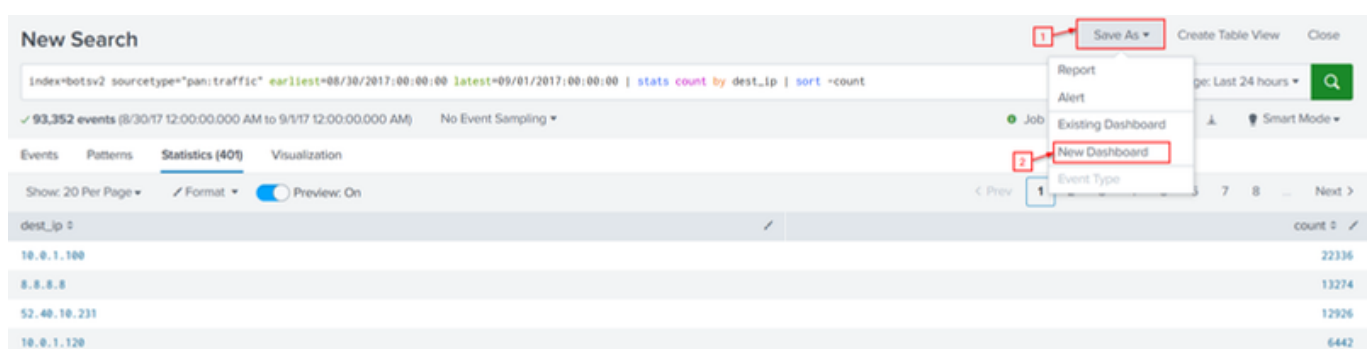
1. Run the search in Splunk.



The screenshot shows the Splunk search interface with the search bar containing the query: `index=botsv2 sourcetype=pan:traffic earliest=08/30/2017:00:00:00 latest=09/01/2017:00:00:00 stats count by dest_ip | sort -count`. The search results are displayed in a table with the following data:

dest_ip	count
10.0.1.100	22336
8.8.8.8	13274
52.40.10.231	12926
10.0.1.120	6442
172.217.11.238	1594
63.251.28.161	1150
172.217.11.227	1016
172.217.11.234	772
172.217.12.2	678
40.97.119.194	640
199.117.103.35	626

2. Click **Save As** → **New Dashboard**.



The screenshot shows the 'New Search' panel in Splunk. The search bar contains the same query as the previous screenshot. The 'Save As' menu is open, and the 'New Dashboard' option is highlighted. The search results table is also visible in the background.

3. Set:

- **Dashboard Title:** Firewall
- **Permissions:** Shared in App
- **Dashboard Type:** Classic Dashboards

4. Click **Save to Dashboard**.

Save Panel to New Dashboard

Dashboard Title

Firewall

firewall

Edit ID

Description

Optional

Permissions

Shared in App

Dashboard type

?

Classic Dashboards

The traditional Splunk dashboard builder

Dashboard Studio

A new builder to create visually-rich, customizable dashboards

Panel Title

Optional

Cancel

Save to Dashboard

5. View Dashboard

Your Dashboard Panel Has Been Created

The panel has been created and added to firewall. You may now view the dashboard.

View Dashboard

Firewall		☆	Edit	Export	...
dest_ip	count				
10.0.1.100	22336				
8.8.8.8	13274				
52.40.10.231	12926				
10.0.1.120	6442				
172.217.11.238	1594				
63.251.28.161	1150				
172.217.11.227	1016				
172.217.11.234	772				
172.217.12.2	678				
40.97.119.194	640				
199.117.103.35	626				
172.217.11.226	472				

Step 2: Refine Panel Titles and Theme

Make the dashboard visually consistent:

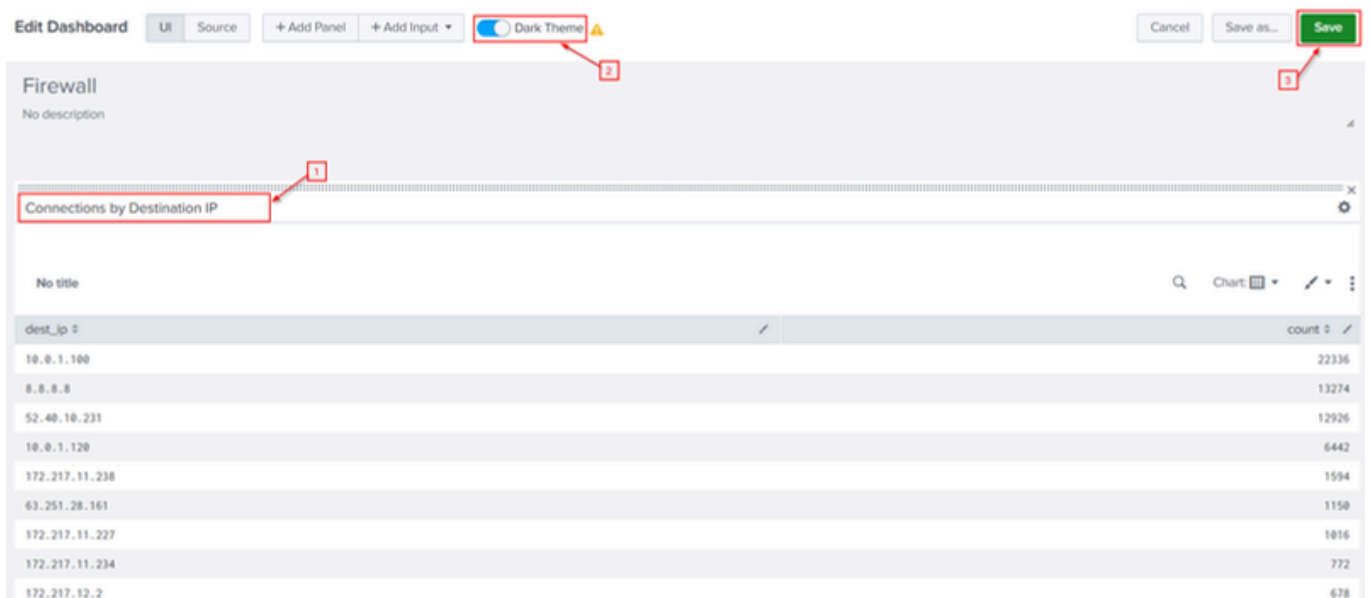
- Click **Edit** on the dashboard.



The screenshot shows a dashboard titled "Firewall" with a table of destination IP addresses and their connection counts. The "Edit" button in the top right corner is highlighted with a red box and an arrow.

dest_ip	count
10.0.1.100	22336
8.8.8.8	13274
52.40.10.231	12926
10.0.1.120	6442
172.217.11.238	1594
63.251.28.161	1150
172.217.11.227	1016
172.217.11.234	772
172.217.12.2	678
40.97.119.194	640
199.117.103.35	626
172.217.11.226	472

- Update panel title to **Connections by Destination IP**.
- (Optional) Enable **Dark Theme** for a security-focused look.
- Click **Save**, then **Refresh**.



The screenshot shows the dashboard editor interface. The "Dark Theme" toggle is highlighted with a red box and a red arrow labeled "2". The "Save" button is highlighted with a red box and a red arrow labeled "3". The panel title "Connections by Destination IP" is highlighted with a red box and a red arrow labeled "1".

Connections by Destination IP

dest_ip	count
10.0.1.100	22336
8.8.8.8	13274
52.40.10.231	12926
10.0.1.120	6442
172.217.11.238	1594
63.251.28.161	1150
172.217.11.227	1016
172.217.11.234	772
172.217.12.2	678

- Then click **Refresh**.

Page refresh required

You have changed the dashboard theme. To see this change, you must refresh the page. Would you like to refresh the page now?

Not Now

Refresh

Creating Visualizations and Interactive Dashboards

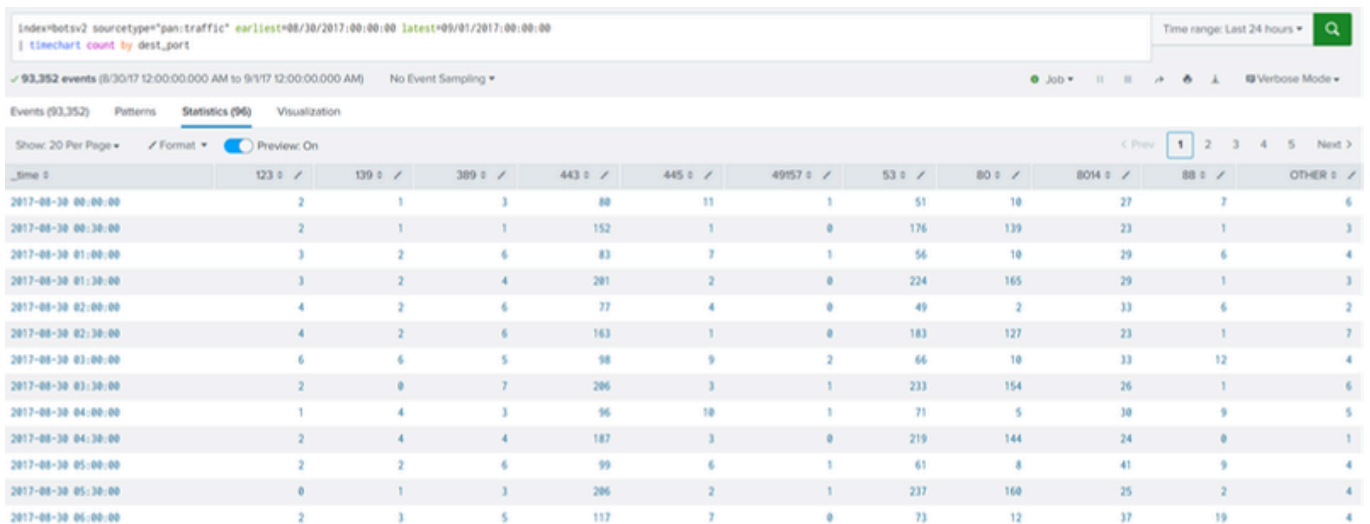
Firewall		☆	Edit	Export ▾	...
Connections by Destination IP					
dest_ip	count				
10.0.1.100	22336				
8.8.8.8	13274				
52.40.10.231	12926				
10.0.1.120	6442				
172.217.11.238	1594				
63.251.28.161	1150				
172.217.11.227	1016				
172.217.11.234	772				
172.217.12.2	678				
40.97.119.194	640				
199.117.103.35	626				
172.217.11.226	472				
172.217.11.225	468				
216.58.217.34	468				
199.117.103.33	466				

Step 3: Add a Time-Based Traffic Trend

To track traffic over time, add a timechart panel for destination ports.

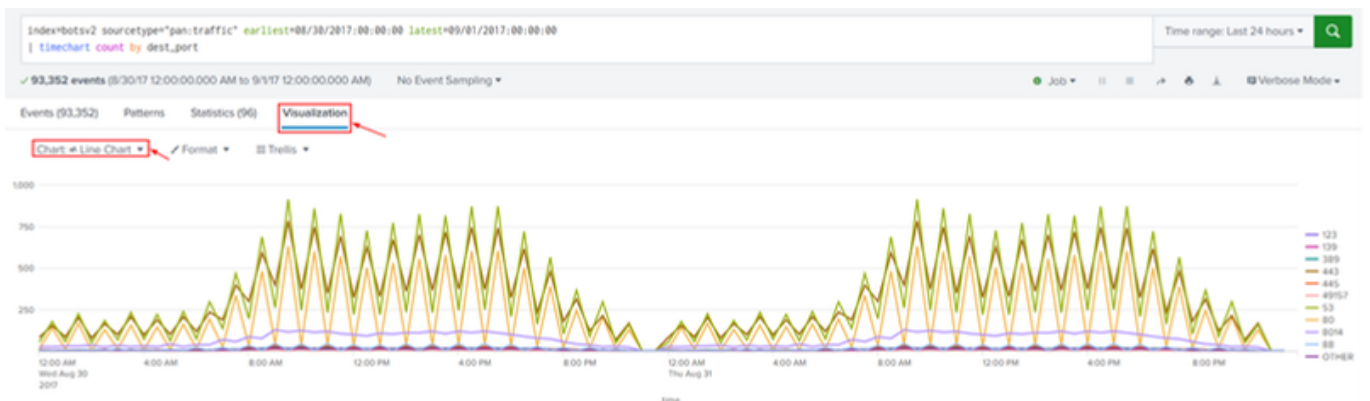
SPL Example:

```
index=botsv2 sourcetype=pan:traffic | timechart count by dest_port
```

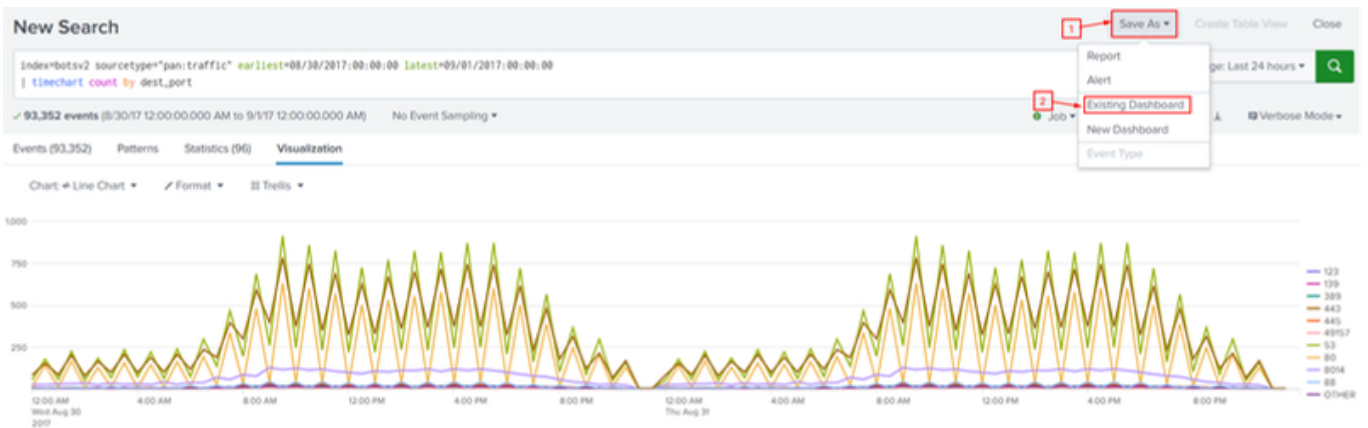


Actions:

- Switch to **Visualization** tab → **Line Chart**.



- Save to **Existing Dashboard** (Firewall).



Save Panel to Existing Dashboard

Select an Existing Dashboard

Firewall

Owner: admin

Shared in App

Panel Title

Optional

Visualization Type

Line Chart

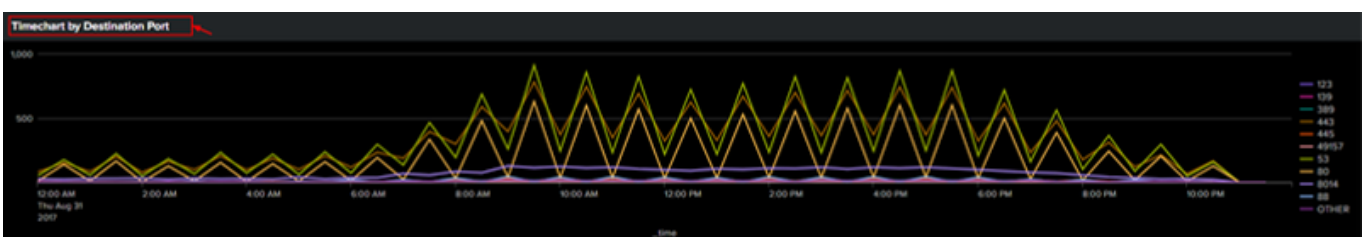
Statistics Table

> Advanced Panel Settings

Cancel

Save to Dashboard

- Click **Edit**.
- Set panel title: **Timechart by Destination Port**.
- **Save Dashboard**.



Step 4: Add Network Interface Analysis

Add a panel to show traffic by interface pairs.

SPL Example:

```
index=botsv2 sourcetype=pan:traffic | stats count by src_interface dest_interface | sort -count
```

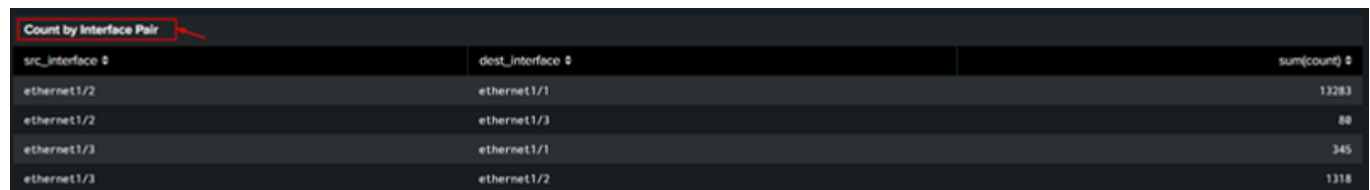


The screenshot shows the Splunk search interface with the query `index=botsv2 sourcetype=pan:traffic | stats count by src_interface dest_interface | sort -count` entered in the search bar. The results are displayed in a table with columns `src_interface`, `dest_interface`, and `count`. The table shows four rows of data:

src_interface	dest_interface	count
ethernet1/3	ethernet1/1	15938
ethernet1/3	ethernet1/2	2882
tunnel.2	ethernet1/1	198
ethernet1/2	ethernet1/3	48

Actions:

- Save as **Existing Dashboard (Firewall)**.
- Click **Edit**.
- Panel title: **Count by Interface Pair**.
- **Save Dashboard**.



The screenshot shows a dashboard panel titled "Count by Interface Pair". The panel displays a table with columns `src_interface`, `dest_interface`, and `sum(count)`. The table shows four rows of data:

src_interface	dest_interface	sum(count)
ethernet1/2	ethernet1/1	13283
ethernet1/2	ethernet1/3	88
ethernet1/3	ethernet1/1	345
ethernet1/3	ethernet1/2	1318

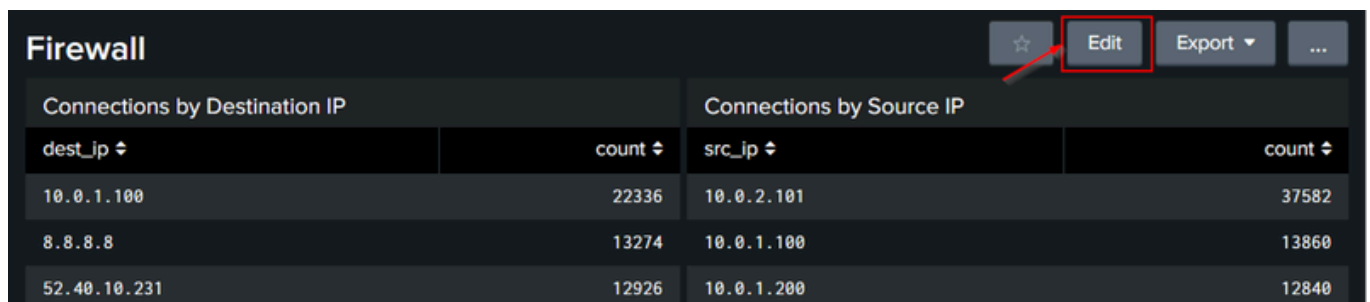
Implementing a Shared Global Time Range Picker

Static dashboards are useful, but interactive dashboards make analysis faster and more flexible. Adding a Shared Time Range Picker lets users adjust the time frame for all panels at once perfect for security investigations.

Step 1: Link Panels to the Shared Time Picker

Your panels currently use fixed time ranges or their own time pickers. To make them dynamic:

1. Click **Edit** on a panel (e.g., Connections by Source IP).



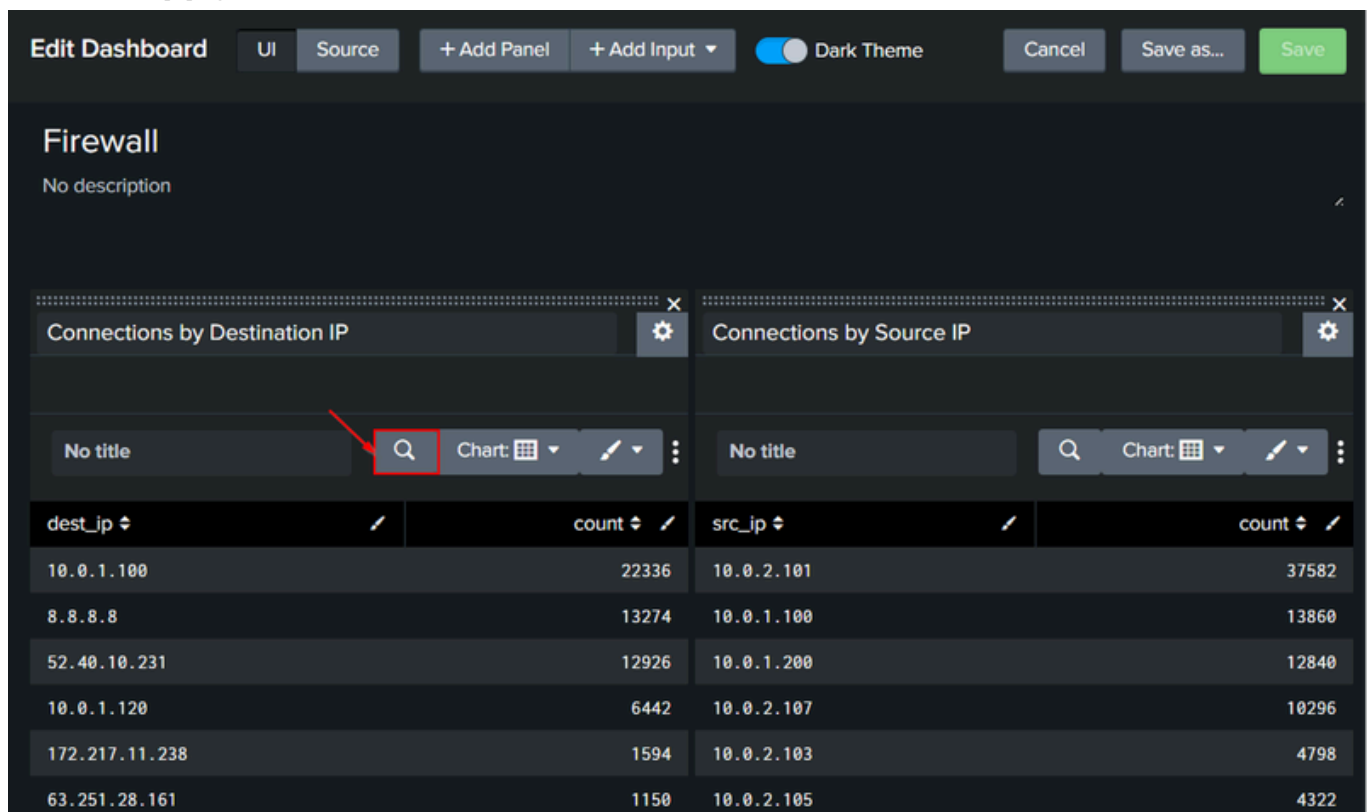
Connections by Destination IP		Connections by Source IP	
dest_ip	count	src_ip	count
10.0.1.100	22336	10.0.2.101	37582
8.8.8.8	13274	10.0.1.100	13860
52.40.10.231	12926	10.0.1.200	12840

2. Remove any hardcoded time from the SPL query (e.g., earliest=... latest=...).

- Example clean SPL:

```
index=botsv2 sourcetype="pan:traffic" | stats count by dest_ip | sort -count
```

3. Click **Apply**.



Connections by Destination IP		Connections by Source IP	
dest_ip	count	src_ip	count
10.0.1.100	22336	10.0.2.101	37582
8.8.8.8	13274	10.0.1.100	13860
52.40.10.231	12926	10.0.1.200	12840
10.0.1.120	6442	10.0.2.107	10296
172.217.11.238	1594	10.0.2.103	4798
63.251.28.161	1150	10.0.2.105	4322

Edit Search

Title

Search String: `index=botsv2 sourcetype=pan:traffic
| stats count by dest_ip
| sort -count`

Run Search

Time Range: Use time picker ▾
Last 24 hours ▾

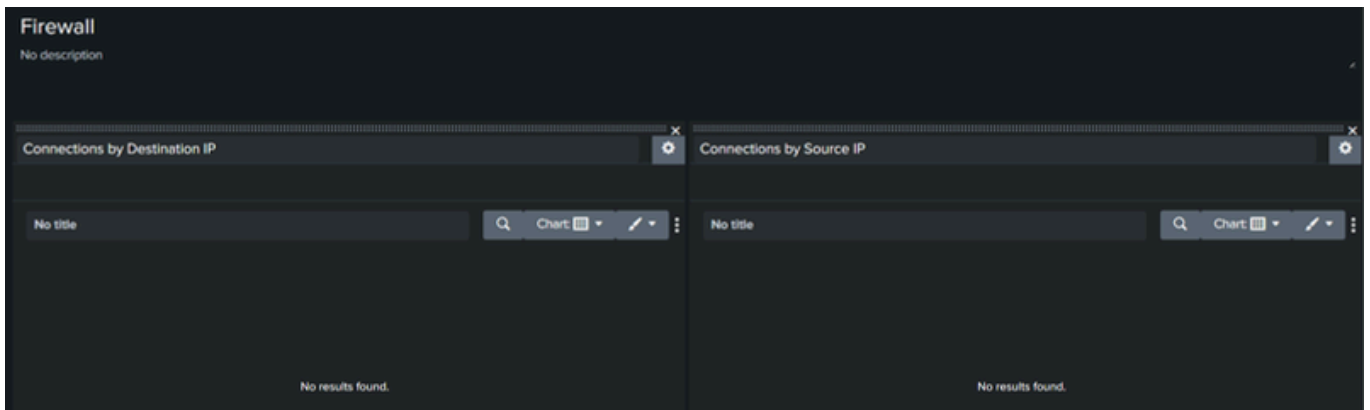
Auto Refresh Delay: No auto refresh ▾

Refresh Indicator: Progress bar ▾

Cancel Convert to Report **Apply**

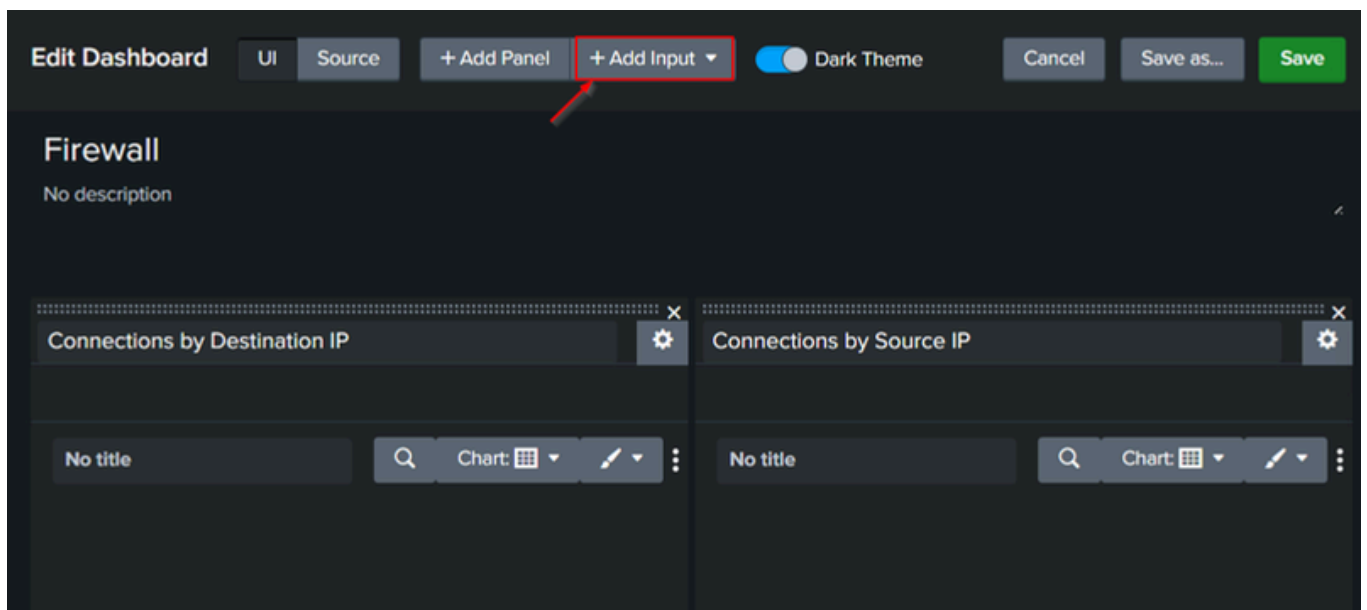
4. Repeat for all panels you want controlled by the shared picker.

- Panels showing “No results” after removing hardcoded time.

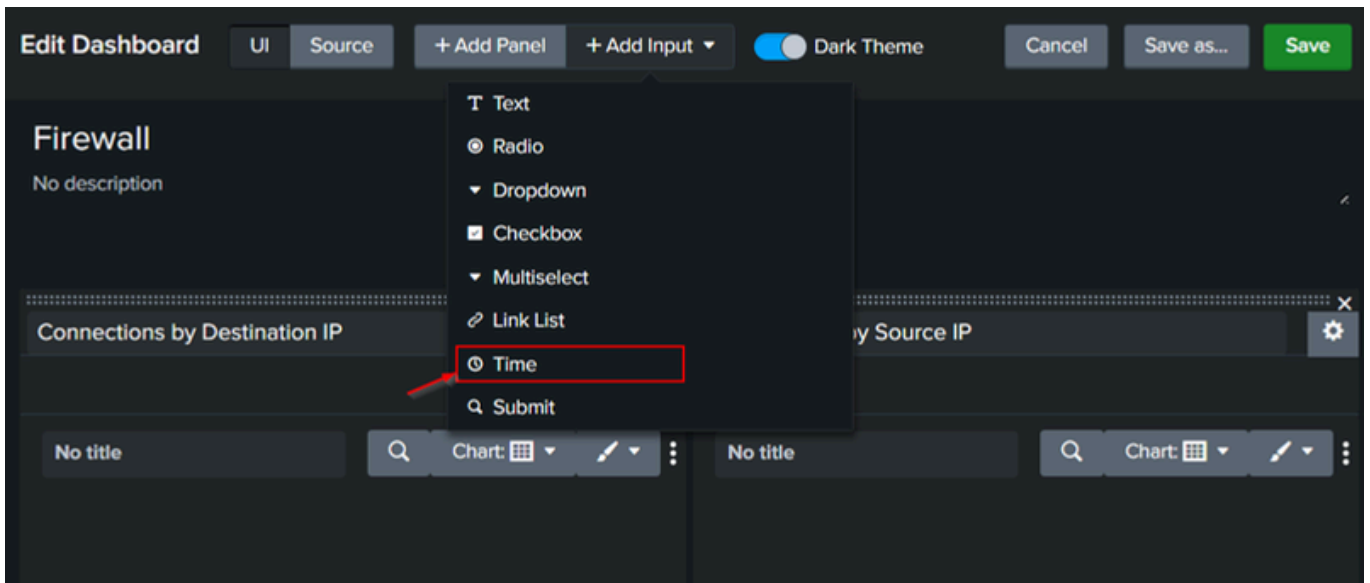


Step 2: Add the Shared Time Picker

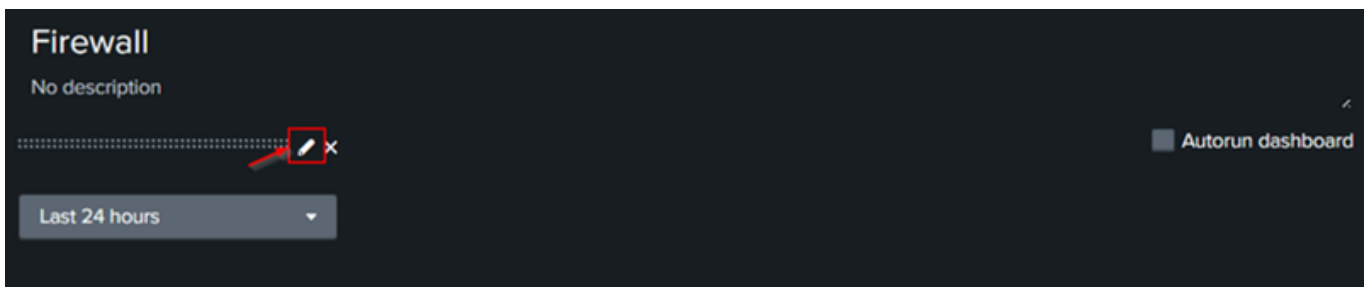
1. In **Edit Dashboard** mode, click **+ Add Input**.



2. Select **Time** from the dropdown.

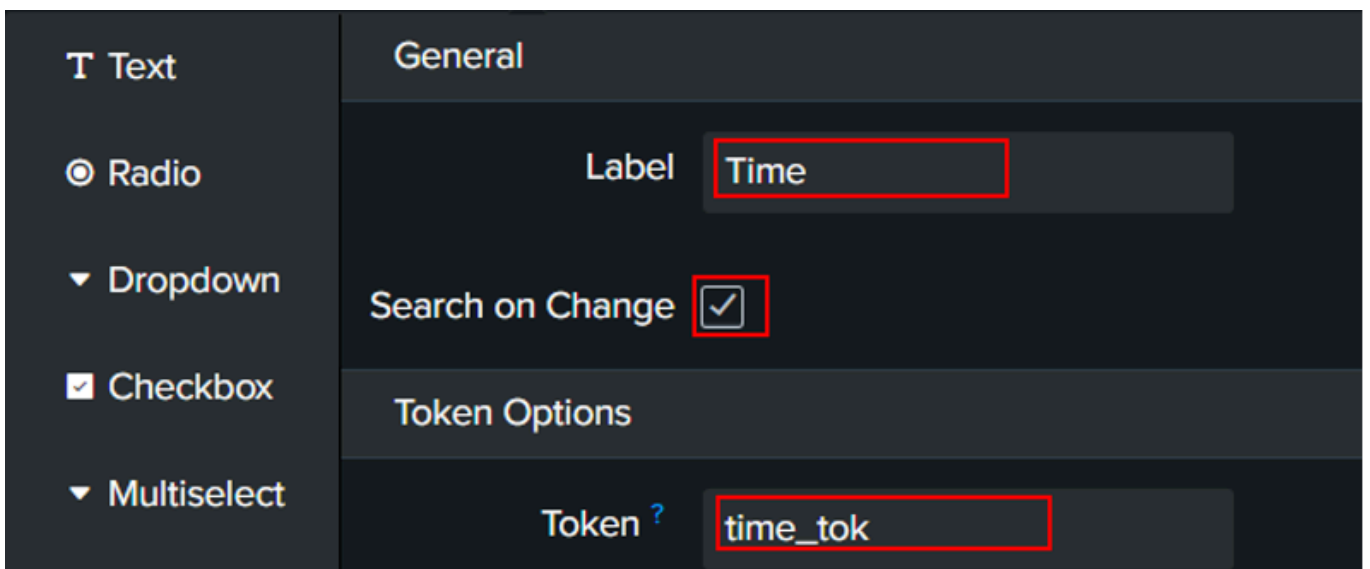


3. Pencil icon for editing input.



3. Configure:

- **Label:** Time
- **Search on Change:** Checked
- **Token:** time_tok



- Configure the default **Data & Time Range**.

The screenshot shows a configuration panel with a sidebar on the left containing 'Link List' and 'Time' (selected). The main area has a 'Default ?' label next to a dropdown menu currently set to 'Last 24 hours'. A red arrow points to the dropdown. At the bottom are 'Cancel' and 'Apply' buttons.

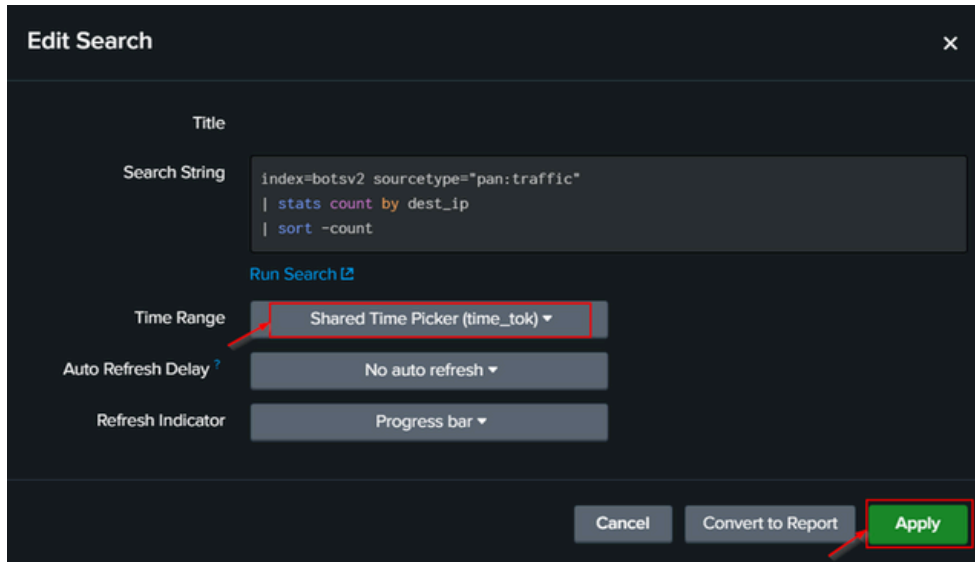
The screenshot shows a configuration panel with a sidebar on the left containing 'Presets', 'Relative', 'Real-time', 'Date Range', 'Date & Time Range' (selected), and 'Advanced'. The main area shows a 'Between' dropdown (highlighted with a red box and arrow) followed by two date/time inputs: '8/31/2017' and '00:00:00.000' (both highlighted with green boxes), followed by 'and', then '9/1/2017' and '00:00:00.000' (both highlighted with green boxes). Below these are the labels 'HH:MM:SS.SSS'. A red arrow points to the 'Apply' button at the bottom right.

- Click **Apply**.

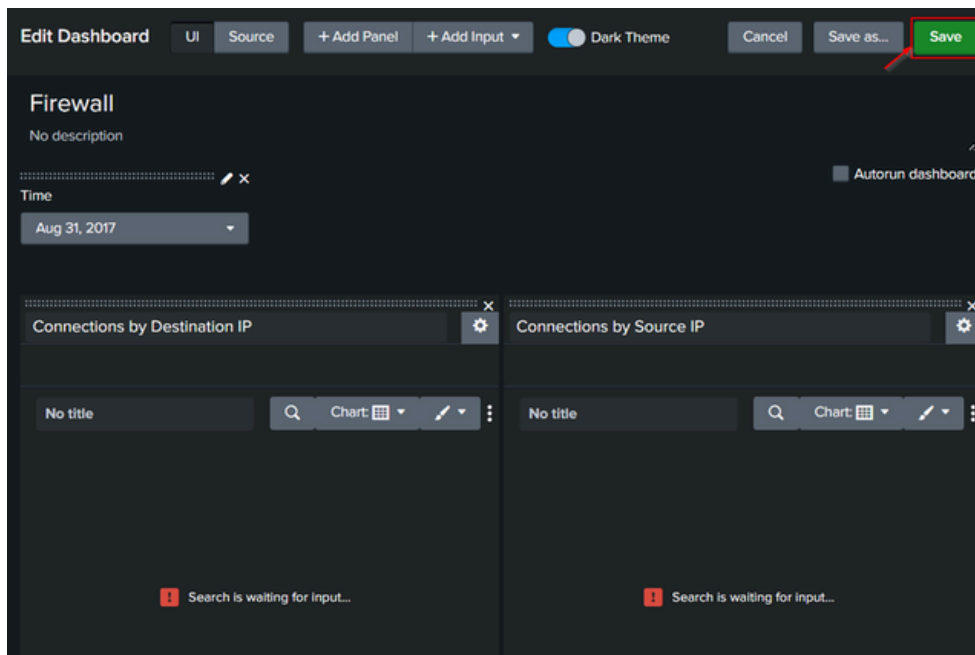
The screenshot shows a configuration panel with a sidebar on the left containing 'Text', 'Radio', 'Dropdown', 'Checkbox', 'Multiselect', 'Link List', 'Time' (selected), and 'Time'. The main area has a 'General' section with a 'Label' field set to 'Time'. Below is a 'Search on Change' checkbox which is checked. The 'Token Options' section has a 'Token ?' field set to 'time_tok'. The 'Default ?' field is a dropdown menu set to 'Aug 31, 2017', which is highlighted with a red box and a red arrow. At the bottom are 'Cancel' and 'Apply' buttons, with the 'Apply' button highlighted by a red box and a red arrow.

Step 3: Connect Panels to the Token

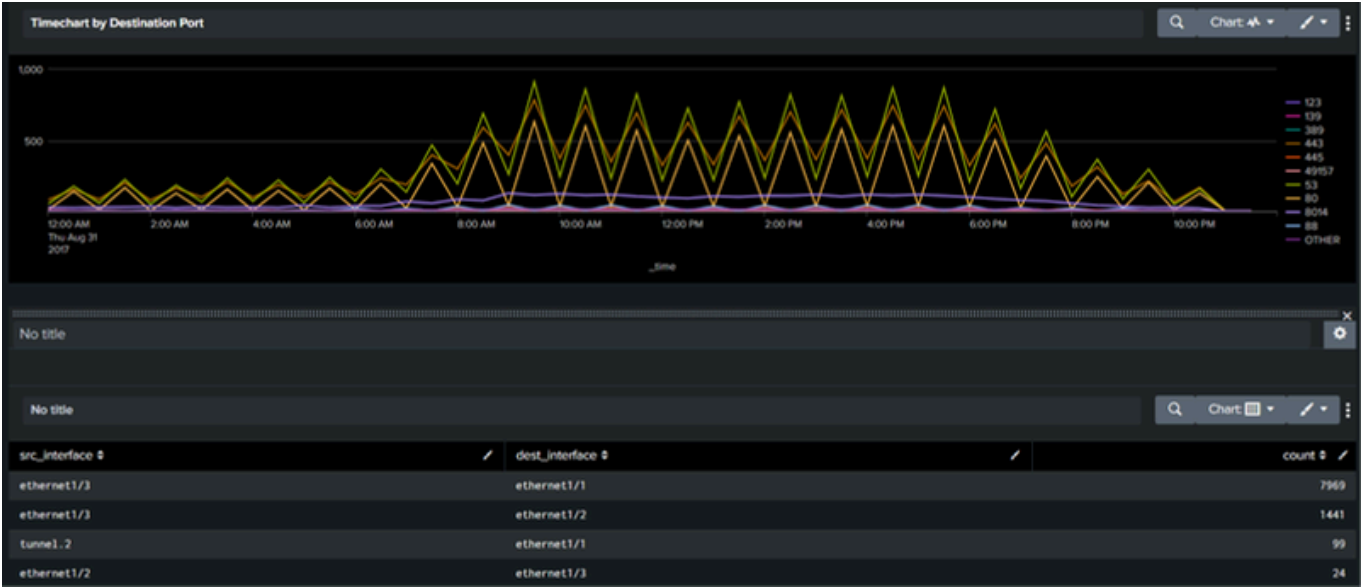
1. Edit each panel's **Time Range** setting.
2. Select **Shared Time Picker (time_tok)**.
3. Click **Apply**.



4. Then **Save Dashboard**.



- Dashboard with shared time filter applied:



Creating Dynamic Forms with Token Management

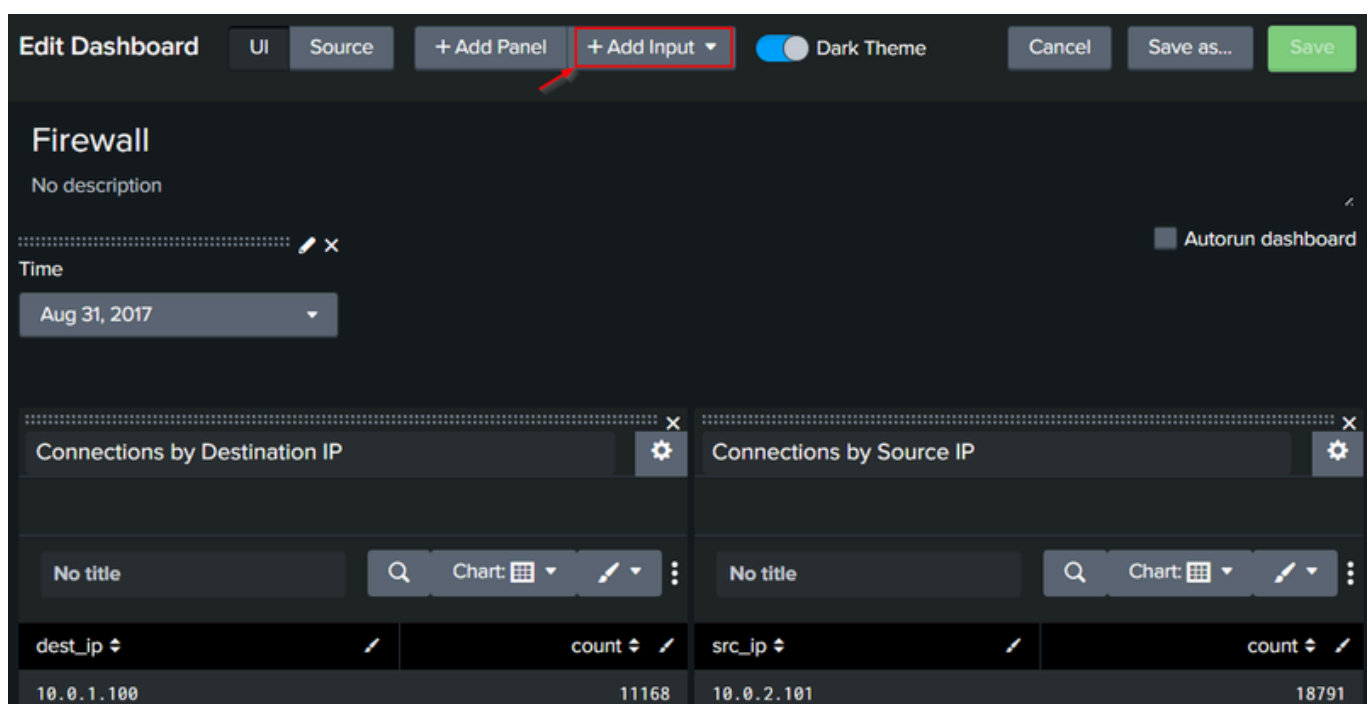
Static dashboards are great for monitoring, but dynamic dashboards give analysts the power to filter data on the fly. By using tokens, you can inject user input (like IP addresses) directly into SPL queries making dashboards interactive and highly customizable.

Understanding Splunk Tokens

- **What are tokens?**
 - Tokens are variables that store user input from dashboard elements (like text boxes or time pickers).
- **How to use them in SPL?**
 - Syntax: \$token_name\$
 - Example: \$src_ip_tok\$
- **Prefix & Suffix:**
 - Add these to build complete clauses:
 - Prefix: src_ip=
 - Suffix: "
 - So if the user enters 10.0.1.100, the SPL becomes:
 - src_ip="10.0.1.100"

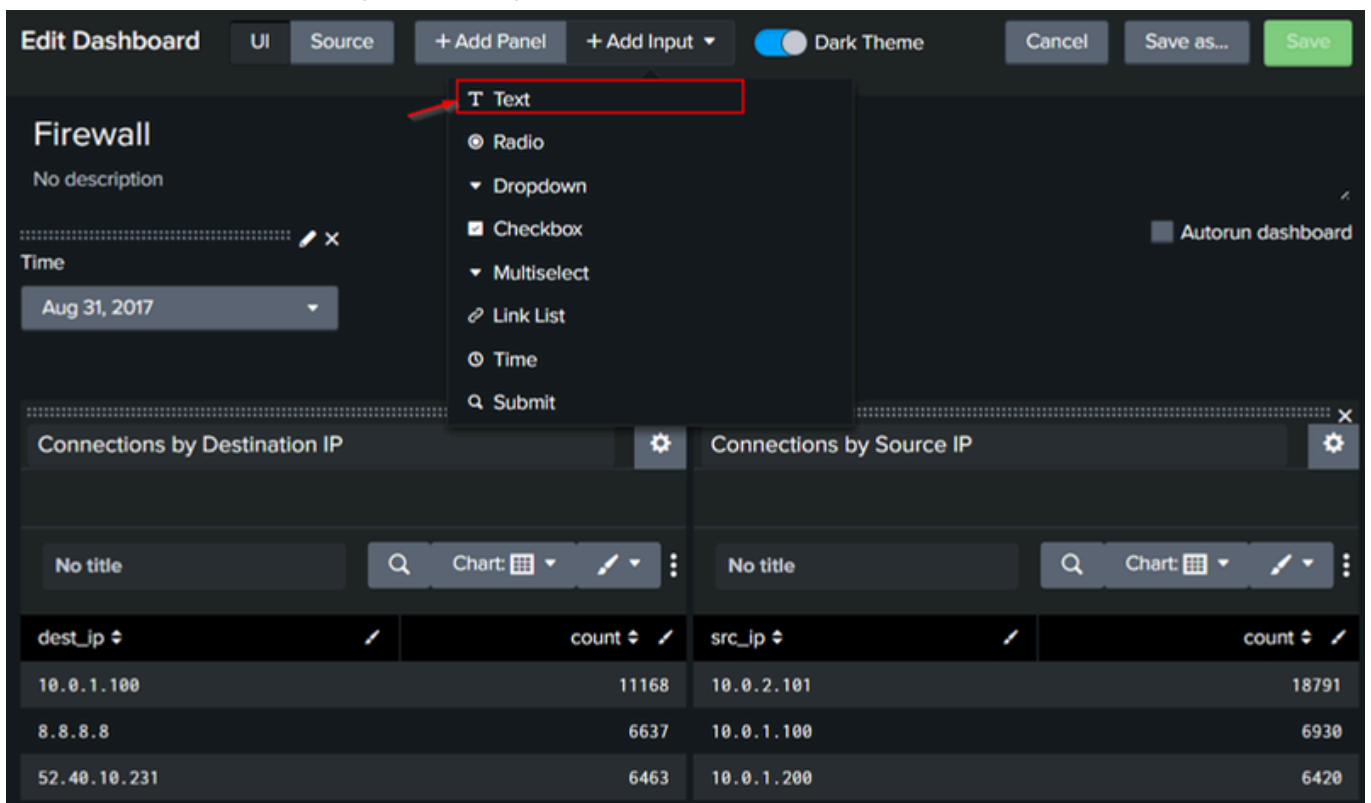
Step 1: Add Input Fields

1. In **Edit Dashboard** mode, click **+ Add Input**.



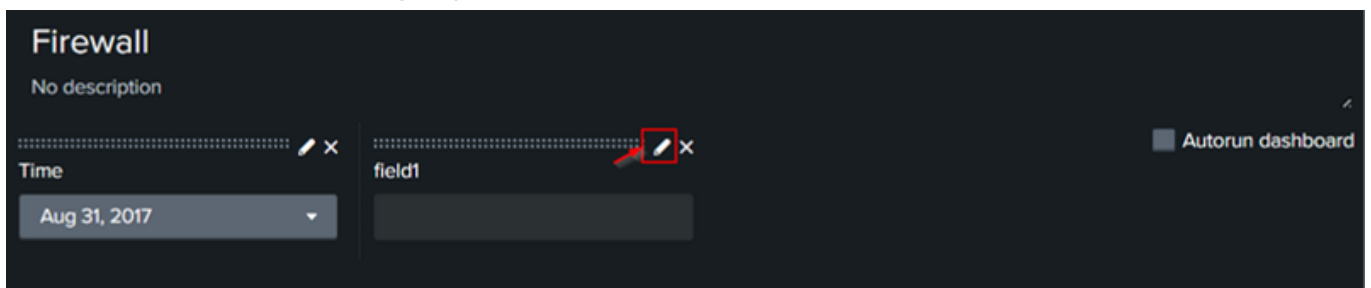
The screenshot shows the Splunk dashboard editor interface. At the top, there's a navigation bar with 'Edit Dashboard', 'UI', 'Source', '+ Add Panel', and '+ Add Input' (highlighted with a red box and an arrow). To the right of these are 'Dark Theme' (a toggle switch), 'Cancel', 'Save as...', and 'Save' buttons. Below the navigation bar, the dashboard title is 'Firewall' with 'No description'. There's a 'Time' picker set to 'Aug 31, 2017'. The dashboard contains two panels: 'Connections by Destination IP' and 'Connections by Source IP'. The 'Connections by Destination IP' panel shows a table with columns 'dest_ip' and 'count', displaying data for '10.0.1.100' with a count of 11168. The 'Connections by Source IP' panel shows a table with columns 'src_ip' and 'count', displaying data for '10.0.2.101' with a count of 18791. The interface is in dark theme.

- Select **Text** for single-line input.



Step 2: Configure Source IP Field

- Pencil icon for editing input.



- **Source IP configuration:**
 - **Label:** Source IP
 - **Token:** src_ip_tok
 - **Prefix:** src_ip="
 - **Suffix:** "
 - **Search on Change:** Checked
 - Click **Apply**.

The screenshot shows a configuration window for a 'Text' field. The 'General' tab is active. The 'Label' is set to 'Source IP'. The 'Search on Change' checkbox is checked. Under 'Token Options', the 'Token' is 'src_ip_tok', 'Default' is '*', 'Initial Value' is empty, 'Token Prefix' is 'src_ip=', and 'Token Suffix' is '='. The 'Apply' button at the bottom right is highlighted with a red arrow.

Step 3: Configure Destination IP Field

Repeat the same steps:

- **Label:** Destination IP
- **Token:** dest_ip_tok
- **Prefix:** dest_ip=
- **Suffix:** "
- Click **Apply**.

The screenshot shows the configuration window for a 'Text' field, now for 'Destination IP'. The 'Label' is 'Destination IP'. The 'Search on Change' checkbox is checked. Under 'Token Options', the 'Token' is 'dest_ip_tok', 'Default' is '*', 'Initial Value' is empty, 'Token Prefix' is 'dest_ip=', and 'Token Suffix' is '='. The 'Apply' button at the bottom right is highlighted with a red arrow.

Step 4: Update Panel Searches

Insert tokens into SPL:

- **Original:**

```
index=botsv2 sourcetype="pan:traffic" | stats count by src_ip | sort -count
```

- **Updated:**

```
index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$ | stats count by src_ip | sort -count
```

- Edit Search with tokens added and Apply changes.

Connections by Destination IP		Connections by Source IP	
dest_ip	count	src_ip	count
10.0.1.100	11168	10.0.2.101	18791
8.8.8.8	6637	10.0.1.100	6930

Edit Search

Title

Search String: `index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$ | stats count by src_ip | sort -count`

Run Search

Time Range: Shared Time Picker (time_tok)

Auto Refresh Delay: No auto refresh

Refresh Indicator: Progress bar

Buttons: Cancel, Convert to Report, **Apply**

- Do the same with the other panels.
- Save the dashboard.

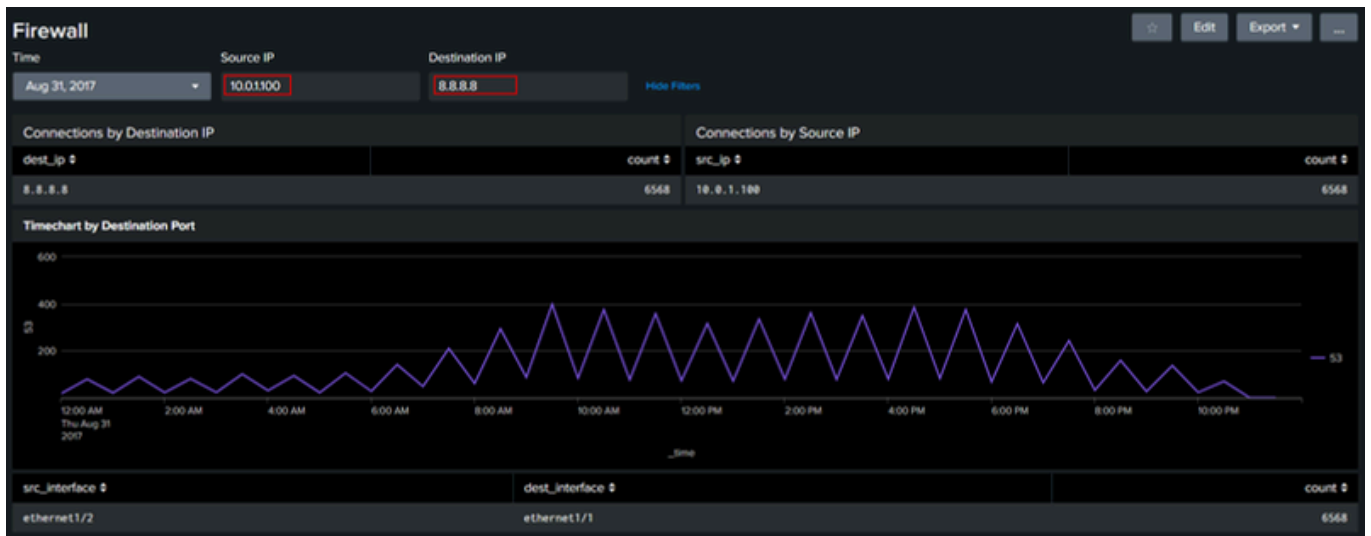
Dynamic Filtering in Action

When a user enters:

- Source IP: 10.0.1.100
- Destination IP: 8.8.8.8

The SPL becomes:

```
index=botsv2 sourcetype="pan:traffic" src_ip="10.0.1.100" dest_ip="8.8.8.8"  
| timechart count by dest_port
```



Improving Performance with Base Searches (Statistical Data)

Large dashboards often suffer from slow load times because multiple panels run similar searches independently. Base Searches solve this by running one main search and letting all panels reuse its results—making dashboards faster and more efficient.

The Problem

If two panels run:

index=botsv2 sourcetype=pan:traffic | stats count by src_ip

index=botsv2 sourcetype=pan:traffic | stats count by dest_ip

Splunk executes the **same initial query twice**, pulling similar data from indexers. This redundancy slows dashboards and wastes resources.

```
26 <title>Connections by Destination IP</title>
27 <table>
28 <search>
29 <query>index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$
30 | stats count by dest_ip
31 | sort -count</query>
32 <earliest>$time_tok.earliest$</earliest>
33 <latest>$time_tok.latest$</latest>
34 <sampleRatio>1</sampleRatio>
35 </search>
36 <option name="count">20</option>
37 <option name="dataOverlayMode">none</option>
38 <option name="drilldown">none</option>
39 <option name="percentagesRow">>false</option>
40 <option name="refresh.display">progressbar</option>
41 <option name="rowNumbers">>false</option>
42 <option name="totalsRow">>false</option>
43 <option name="wrap">>true</option>
44 </table>
45 </panel>
46 <panel>
47 <title>Connections by Source IP</title>
48 <table>
49 <search>
50 <query>index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$
51 | stats count by src_ip
52 | sort -count</query>
```

The Solution: Base Search

A **Base Search**:

- Runs **once** at the dashboard level.
- Fetches all required fields for all panels.
- Panels then apply lightweight **post-processing** (e.g., stats, sort).

Benefits:

- **Faster load times**
- **Lower resource usage**
- **Better scalability**

Step 1: Define the Base Search

In **Simple XML**, add:

```
<search id="base">
```

```
  <query>index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$ | stats  
  count by src_ip, dest_ip, src_port, dest_port, src_interface, dest_interface</query>
```

```
  <earliest>$time_tok.earliest$</earliest>
```

```
  <latest>$time_tok.latest$</latest>
```

```
</search>
```

- Navigate to Dashboards → Edit Source.
- Clone dashboard (Firewall v2).

The screenshot shows the Splunk Dashboards interface. At the top, the 'Dashboards' tab is selected in the navigation bar (1). Below the navigation bar, there's a 'Create New Dashboard' button. The main content area shows 'Latest Resources' and a list of 15 dashboards. A context menu is open for the 'Logs' dashboard, showing options like 'Edit panels', 'Edit source', 'Edit title or description', 'Edit permissions', 'Schedule PDF delivery', 'Set as home dashboard', 'Clone' (3), and 'Delete'. The 'Clone' option is highlighted with a red box. Below the context menu, the 'Firewall' dashboard row is visible, with its 'Edit' button highlighted (2). The table below shows the list of dashboards.

i	★	Title	Actions	Owner	App	Sharing	Type
>	☆	Logs	Edit panels Edit source Edit title or description Edit permissions Schedule PDF delivery Set as home dashboard Clone Delete	XML	lookup_editor	Global	Classic
>	☆	Look...		dy	lookup_editor	Global	Classic
>	☆	Look...		dy	lookup_editor	Global	Classic
>	☆	New		dy	lookup_editor	Global	Classic
>	☆	Over		dy	lookup_editor	Global	Classic
>	☆	Over		dy	lookup_editor	Global	Classic
>	☆	Statu		dy	lookup_editor	Global	Classic
>	☆	Firewall	Edit	admin	search	App	Classic
>	☆	Integrity Check of I...	Edit	nobody	search	App	Dashboard Studio

Clone

×

Title

Firewall v2

ID ?

firewall_v2

The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.

New Description

optional

Permissions

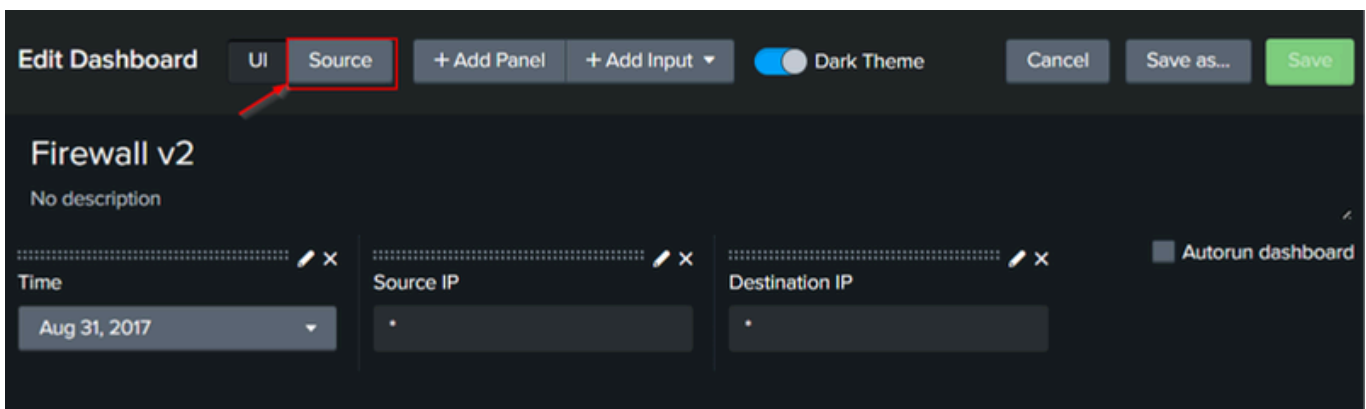
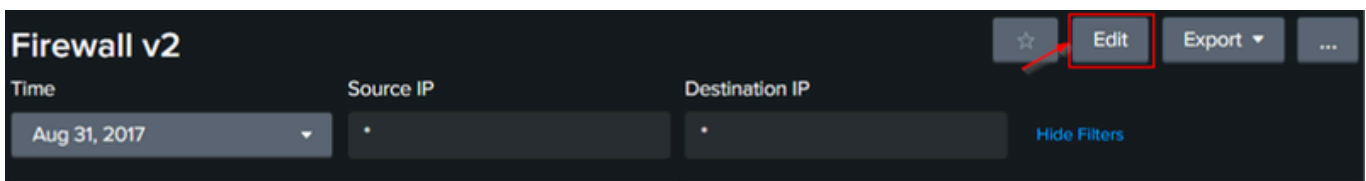
Private

Clone

Cancel

Clone Dashboard

- Edit dashboard in source mode.



- Base search added at top.

```

1 <form version="1.1" theme="dark">
2   <label>Firewall v2</label>
3   <search id="base">
4     <query> index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$ | stats count by src_ip, dest_ip, src_port, dest_port, src_interface, dest_interface </query>
5     <earliest>$time_tok.earliest</earliest>
6     <latest>$time_tok.latest</latest>
7   </search>
8   <fieldset submitButton="false">
9     <input type="time" token="time_tok" searchWhenChanged="true">
10    <label>Time</label>

```

Step 2: Update Panels to Use Base Search

- Replace full searches with (For **Connections by Destination IP**):
<search base="base">
<query> | stats sum(count) by dest_ip | sort -sum(count)</query>
</search>

```

31 <title>Connections by Destination IP</title>
32 <table>
33 <search base="base">
34 <query>| stats sum(count) by dest_ip | sort -count</query>
35 </search>
36 <option name="count">20</option>
37 <option name="dataOverlayMode">none</option>
38 <option name="drilldown">none</option>
39 <option name="percentagesRow">>false</option>

```

- For **Connections by Source IP**:

```

44 </table>
45 </panel>
46 <panel>
47 <title>Connections by Source IP</title>
48 <table>
49 <search base="base">
50 <query>| stats sum(count) by src_ip | sort -count</query>
51 </search>

```

- Dashboard showing optimized panels.

Firewall v2

☆

Edit

Export ▾

...

Time

Source IP

Destination IP

Aug 31, 2017 ▾

*

*

Hide Filters

Connections by Destination IP		Connections by Source IP	
dest_ip ↕	sum(count) ↕	src_ip ↕	sum(count) ↕
10.0.1.100	1318	10.0.1.100	6851
10.0.2.103	15	10.0.1.101	14
10.0.2.108	17	10.0.1.200	6420
10.0.2.250	48	10.0.1.220	48
104.131.53.252	15	10.0.1.222	30
129.6.15.29	24	10.0.2.102	69
138.91.159.158	51	10.0.2.103	366
172.217.11.238	15	10.0.2.105	212
192.43.172.30	16	10.0.2.107	275
198.58.110.84	37	10.0.2.108	252
198.60.22.240	14	10.0.2.109	314
199.7.91.13	29	10.0.2.110	175

Base Searches for Time-Based Visualizations (Timecharts)

Base Searches are one of the most effective ways to optimize Splunk dashboards. Beyond reducing redundancy, they can pre-aggregate data, making dashboards faster and more scalable.

1. Why Base Searches Matter

Instead of running full searches in every panel, a Base Search runs once, and all panels reuse its results. This eliminates repeated index lookups and heavy computations.

2. Added Technical Insight: Pre-Aggregation Strategy

A smart optimization is to pre-aggregate data in the Base Search.

Example:

```
<search id="base">
  <query>
    index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$
    | bin span=30m _time
    | stats count by _time, src_ip, dest_ip, src_port, dest_port, src_interface,
    dest_interface
  </query>
</search>
```

```
1 <form version="1.1" theme="dark">
2   <label>Firewall v2</label>
3   <search id="base">
4     <query> index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$ | bin span=30m _time | stats count by _time, src_ip, dest_ip, src_port, dest_port, src_interface, dest_interface </query>
5     <earliest>$time_tok.earliest$</earliest>
6     <latest>$time_tok.latest$</latest>
7   </search>
```

What's new here?

- Adds **binning** (bin span=30m _time) for time-based grouping.
- Calculates a **count field** usable by all panels.
- Panels now use **sum(count)** instead of recalculating stats.

3. Lightweight Dependent Searches

Panels only perform simple post-processing:

```
<search base="base">
  <query>| chart sum(count) by _time, dest_port</query>
```

```
64 <panel>
65   <chart>
66     <title>Timechart by Destination Port</title>
67     <search base="base">
68       <query>| chart sum(count) by _time, dest_port</query>
69     </search>
```

4. Performance Impact

Before Base Searches:

- Each panel ran a full search pipeline.
- Timecharts were slow due to repeated binning.

After Base Searches:

- One job retrieves and structures all data.
- Panels only summarize counts.
- Dashboard becomes **significantly faster and more responsive.**

Connections by Destination IP		Connections by Source IP	
dest_ip ↕	sum(count) ↕	src_ip ↕	sum(count) ↕
10.0.1.100	1318	10.0.1.100	6851
10.0.2.103	15	10.0.1.101	14
10.0.2.108	17	10.0.1.200	6420
10.0.2.250	48	10.0.1.220	48
104.131.53.252	15	10.0.1.222	30
129.6.15.29	24	10.0.2.102	69
138.91.159.158	51	10.0.2.103	366
172.217.11.238	15	10.0.2.105	212
192.43.172.30	16	10.0.2.107	275
198.58.110.84	37	10.0.2.108	252
198.60.22.240	14	10.0.2.109	314
199.7.91.13	29	10.0.2.110	175
204.13.251.34	25		
207.46.134.255	15		
207.46.153.155	25		
208.78.70.2	13		
216.229.0.49	15		
23.239.14.112	11		
23.97.150.21	15		
4.4.4.4	40		



Configuring Basic Drilldown Functionality

Drilldowns make dashboards interactive, allowing analysts to click on a data point and instantly investigate further. For security teams, this means faster threat analysis and deeper insights without leaving the dashboard.

What Are Drilldowns?

Drilldowns trigger an action when you click on a visualization element (e.g., a table row, chart bar, or single value). Common actions include:

- **No action** (default)
- **Link to search** - open a new search with the clicked value
- **Link to dashboard** - navigate to another dashboard
- **Link to report** - run a predefined report
- **Link to custom URL** - open external tools (e.g., VirusTotal)
- **Manage tokens** - update filters within the same dashboard

Step 1: Access the Drilldown Editor

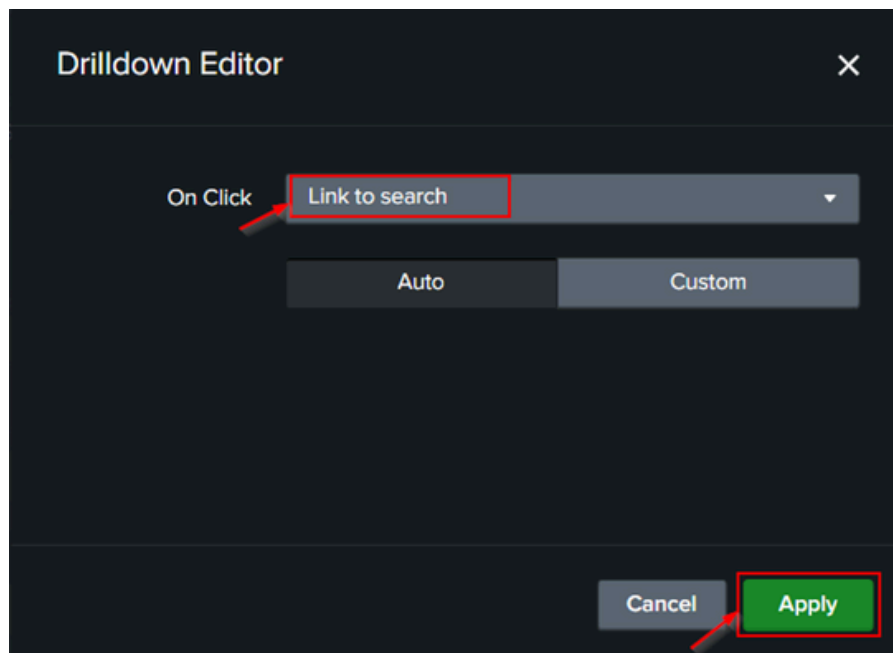
1. Open your dashboard (e.g., Firewall v2).
2. Hover over the visualization (e.g., Connections by Source IP).
3. Click **More actions** (three dots or gear icon).
4. Select **Edit Drilldown**.

The screenshot shows the 'Firewall v2' dashboard with filters for Time (Aug 31, 2017), Source IP, and Destination IP. Two visualizations are displayed: 'Connections by Destination IP' and 'Connections by Source IP'. The 'Connections by Source IP' visualization is a table with columns for destination IP, sum(count), and count. A red box labeled '1' points to the 'More actions' menu (three dots) in the top right of the visualization. A red box labeled '2' points to the 'sum(count)' field in the table.

dest_ip	sum(count)	count
10.0.1.100	15	14
10.0.2.103	17	6420
10.0.2.108	48	48
10.0.2.250	15	30
104.131.53.252	24	69
129.6.15.29	51	366
138.91.159.158	15	212
172.217.11.238		

Step 2: Choose the Action

- In the **Drilldown Editor**, set On Click to **Link to search**.
- Click **Apply**.



Step 3: Configure the Search

Two options:

A. Auto Configuration

Automatically builds a search using the clicked value.

- Example: Clicking **10.0.1.200** generates:

index=botsv2 sourcetype="pan:traffic" src_ip="10.0.1.200"

Connections by Destination IP		Connections by Source IP	
dest_ip ↕	sum(count) ↕	src_ip ↕	sum(count) ↕
10.0.1.100	1318	10.0.1.100	6851
10.0.2.103	15	10.0.1.101	14
10.0.2.108	17	10.0.1.200	6420
10.0.2.250	48	10.0.1.220	48
104.131.53.252	15	10.0.1.222	30
129.6.15.29	24	10.0.2.102	69
138.91.159.158	51	10.0.2.103	366
172.217.11.238	15	10.0.2.105	212
192.43.172.30	16	10.0.2.107	275
198.58.110.84	37	10.0.2.108	252
198.60.22.240	14	10.0.2.109	314
199.7.91.13	29	10.0.2.110	175
204.13.251.34	25		
207.46.134.255	15		

index=botsv2 sourcetype="pan:traffic" src_ip="*" dest_ip="*" dest_ip="10.0.1.100" | bin span=30m _time
| stats count by _time, src_ip, dest_ip, src_port, dest_port, src_interface, dest_interface

Time range: during Thu, Aug 31, 2017

✓ 11,168 events (8/31/17 12:00:00.000 AM to 9/1/17 12:00:00.000 AM) No Event Sampling Job

Events (11,168) Patterns **Statistics (1,188)** Visualization

Show: 20 Per Page Format Preview: On < Prev 1 2 3 4 5 6 7 8 ... Next >

_time	src_ip	dest_ip	src_port	dest_port	src_interface	dest_interface	count
2017-08-31 00:00:00	10.0.2.103	10.0.1.100	51441	53	ethernet1/3	ethernet1/2	1
2017-08-31 00:00:00	10.0.2.103	10.0.1.100	61622	53	ethernet1/3	ethernet1/2	1
2017-08-31 00:00:00	10.0.2.103	10.0.1.100	61646	53	ethernet1/3	ethernet1/2	1
2017-08-31 00:00:00	10.0.2.105	10.0.1.100	53623	88	ethernet1/3	ethernet1/2	1
2017-08-31 00:00:00	10.0.2.105	10.0.1.100	56376	53	ethernet1/3	ethernet1/2	1

B. Custom Configuration (Using Tokens)

For more control:

- Search string:

index=botsv2 sourcetype="pan:traffic" src_ip="\$click.value\$"

- Time Range: **Shared Time Picker (time_tok)**.
- Click **Apply**.

Drilldown Editor
×

On Click

Link to search

Auto
Custom

You can include predefined drilldown tokens in a custom search. [Learn more](#)

Search String

index=botsv2 sourcetype="pan:traffic" src_ip=\$click.value\$

Time Range

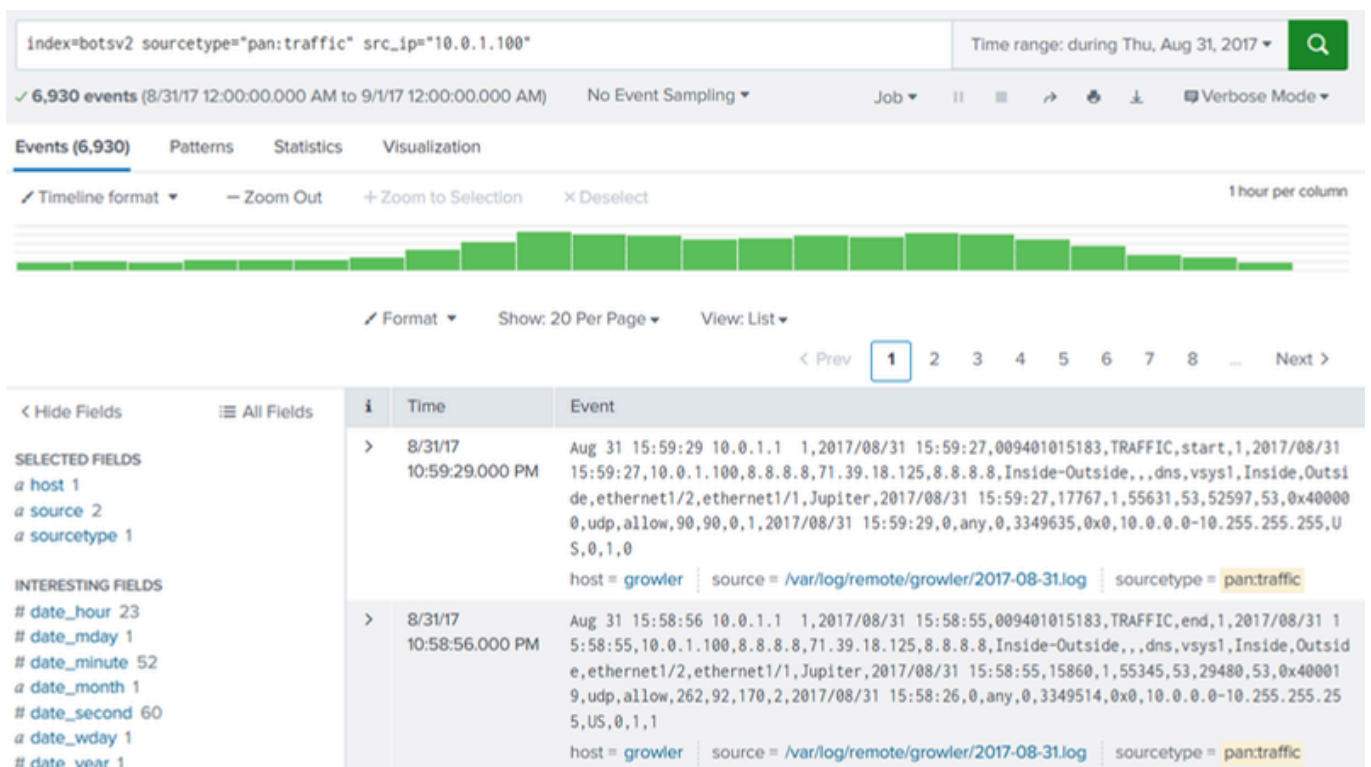
Shared Time Picker (time_tok)

☒ Open in new tab

Cancel
Apply

- Test:

Connections by Destination IP		Connections by Source IP	
dest_ip	sum(count)	src_ip	sum(count)
10.0.1.100	1318	10.0.1.100	6851
10.0.2.103	15	10.0.1.101	14
10.0.2.108	17	10.0.1.200	6420
10.0.2.250	48	10.0.1.220	48
104.131.53.252	15	10.0.1.222	30
129.6.15.29	24	10.0.2.102	69
138.91.159.158	51	10.0.2.103	366
172.217.11.238	15	10.0.2.105	212



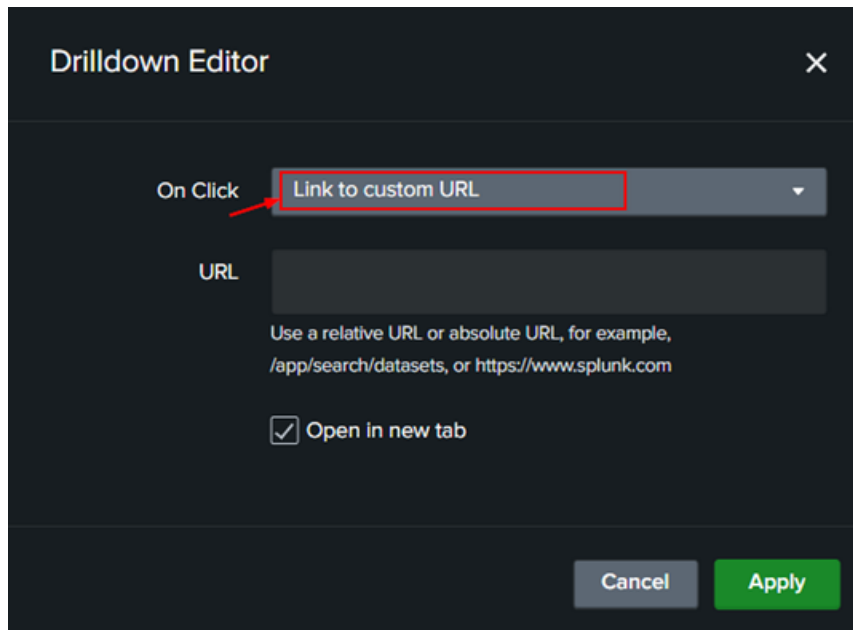
Step 4: External Drilldown (Threat Intelligence Integration)

To link to VirusTotal:

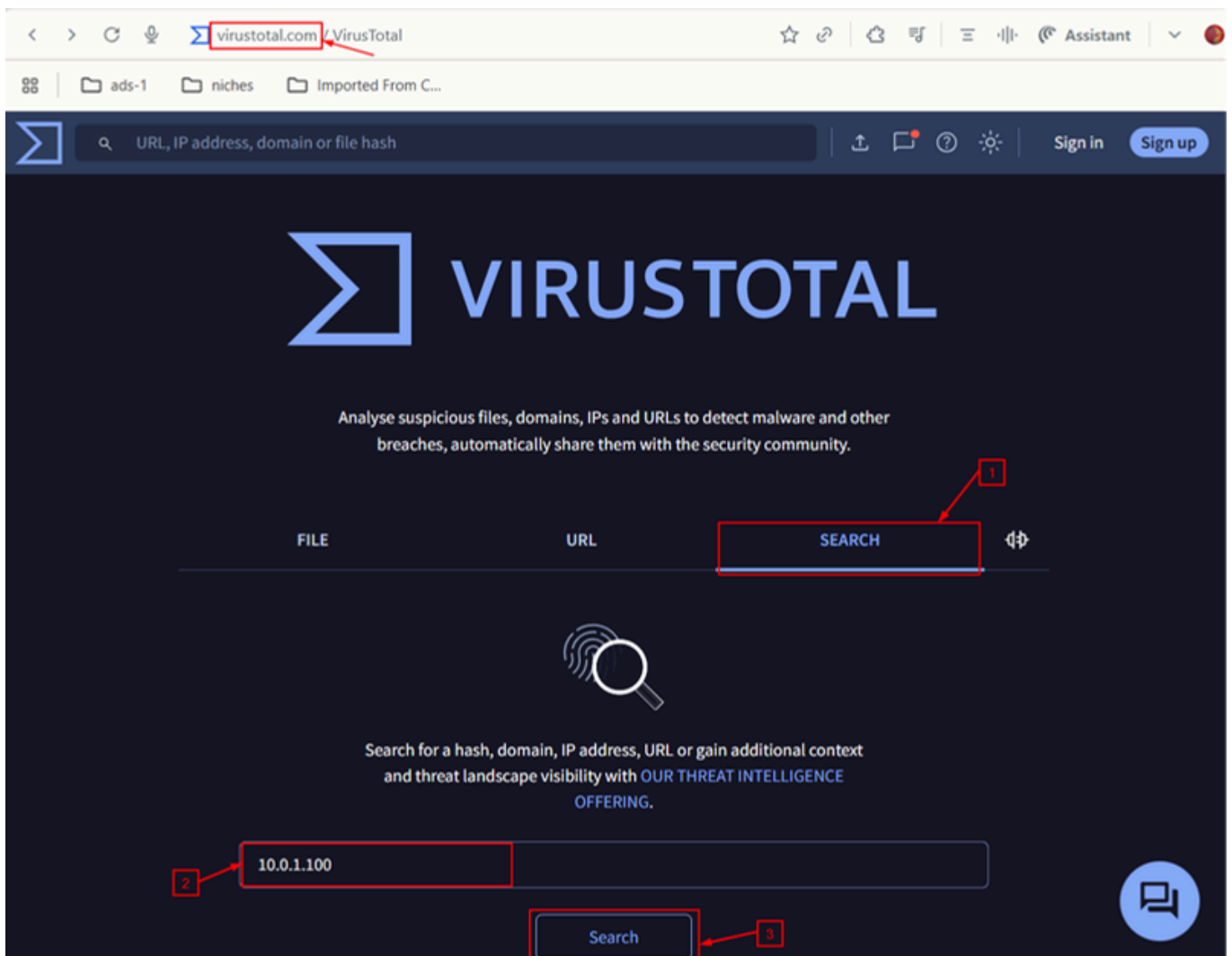
- Set **On Click** to **Link to custom URL**.
- URL:

[https://www.virustotal.com/gui/ip-address/\\$click.value\\$](https://www.virustotal.com/gui/ip-address/$click.value$)

- Enable **Open in new tab**.
- Click **Apply**.

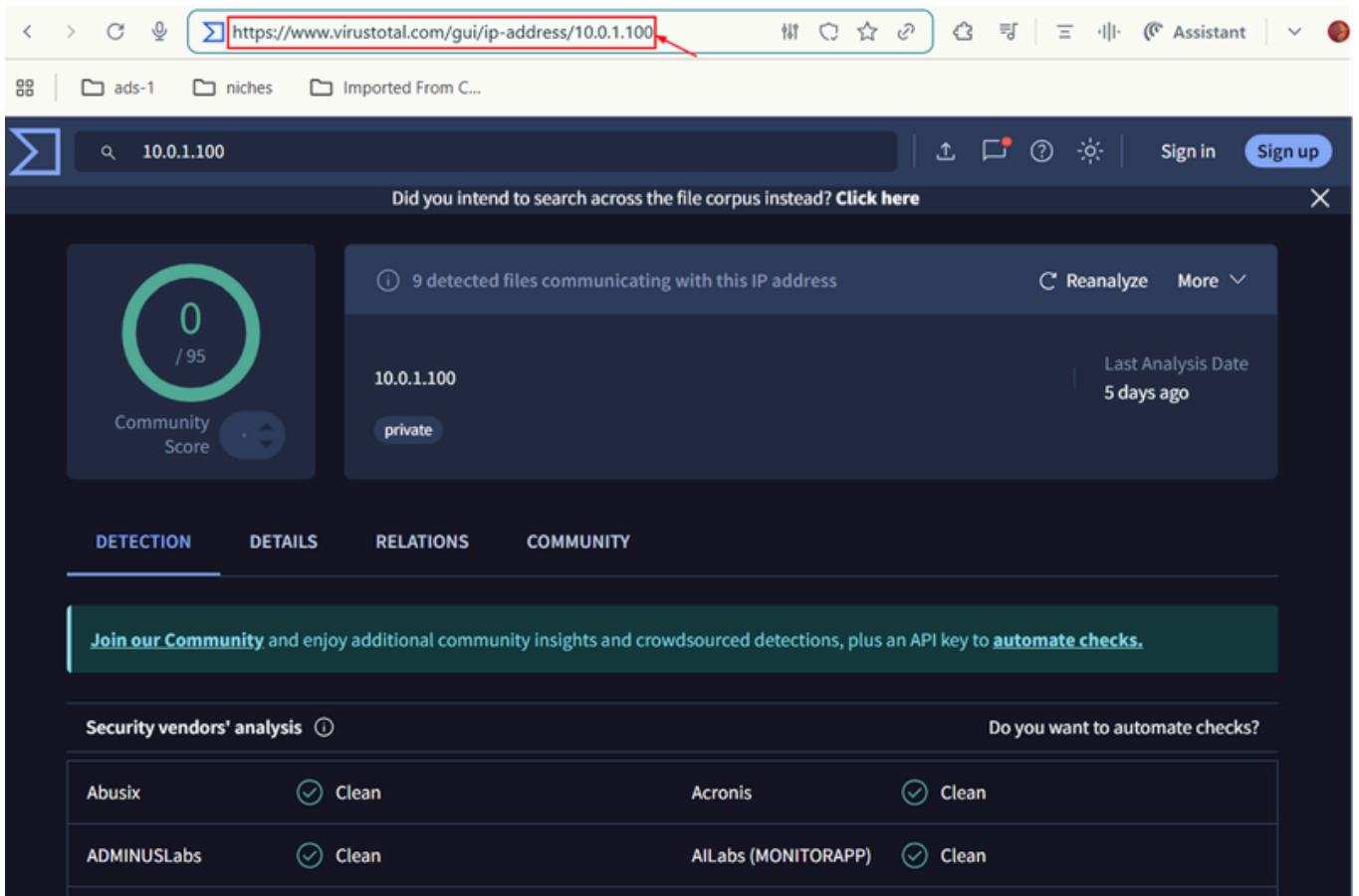


- Go to VirusTotal page "**virustotal.com**" → **SEARCH** → search for "**10.0.1.100**" → click **Search**

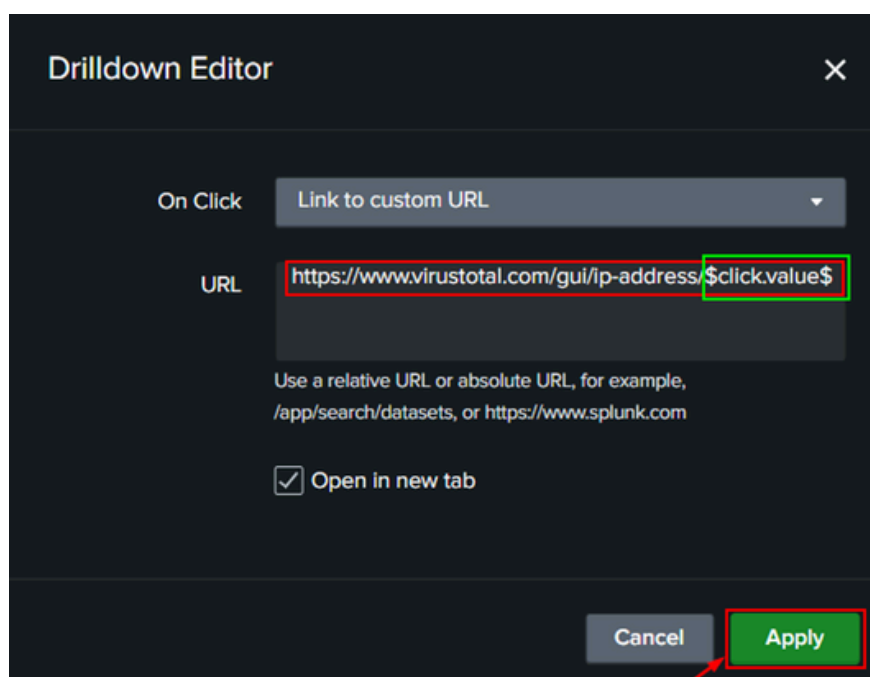


Creating Visualizations and Interactive Dashboards

- Copy the URL.



- Past the URL and change the ip adress with \$click.value\$:
https://www.virustotal.com/gui/ip-address/\$click.value\$
- Enable **Open in new tab**.
- Click **Apply**.



Creating Visualizations and Interactive Dashboards

- Test:

Firewall v2 ☆ Edit Export ▾ ...

Time: Aug 31, 2017 ▾ Source IP: * Destination IP: * Hide Filters

Connections by Destination IP		Connections by Source IP	
dest_ip ▴	sum(count) ▴	src_ip ▴	sum(count) ▴
10.0.1.100	1318	10.0.1.100	6851
10.0.2.103	15	10.0.1.101	14
10.0.2.108	17	10.0.1.200	6420
10.0.2.250	48	10.0.1.220	48
104.131.53.252	15	10.0.1.222	30
129.6.15.29	24	10.0.2.102	69

https://www.virustotal.com/gui/ip-address/10.0.1.100

10.0.1.100

0 / 95
Community Score

9 detected files communicating with this IP address Reanalyze More ▾

10.0.1.100
private
Last Analysis Date
5 days ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean

Implementing Logic in Drilldowns

Conditional drilldowns make dashboards smarter by changing the action based on the data clicked. For security analysts, this means automatically directing investigations to the right resource internal documentation for private IPs or threat intelligence for public IPs.

Why Conditional Drilldowns?

Instead of a one-size-fits-all drilldown, you can:

- Open **RFC 1918** for private IPs.
- Open **VirusTotal** for public IPs. This saves time and ensures context-aware navigation.

Step 1: Enrich Data with IP Classification

The base search adds classification fields:

```
<search id="base">
<query>
  index=botsv2 sourcetype="pan:traffic" $src_ip_tok$ $dest_ip_tok$
  | eval src_class = if(src_class="unknown", "public", src_class)
  | eval dest_class = if(dest_class="unknown", "public", dest_class)
  | bin span=30m _time
  | stats count by _time, src_ip, dest_ip, src_port, dest_port, src_interface,
dest_interface, src_class, dest_class
</query>
</search>
```

```
1 <form version="1.1" theme="dark">
2   <label>Firewall v2</label>
3   <search id="base">
4     <query> index=botsv2 sourcetype=pan:traffic $src_ip_tok$ $dest_ip_tok$ | eval src_class = if(src_class="unknown", "public", src_class) | eval
5       dest_class = if(dest_class="unknown", "public", dest_class) | bin span=30m _time | stats count by _time, src_ip, dest_ip, src_port, dest_port,
6       src_interface, dest_interface, src_class, dest_class </query>
7     <earliest>$time_tok.earliest$</earliest>
8     <latest>$time_tok.latest$</latest>
9   </search>
```

Step 2: Display Classification in Panels

Panels retain classification fields:

- **Source IP Table:**

```
| stats sum(count) by src_ip, src_class | sort -count
```

```
31 <title>Connections by Source IP</title>
32 <table>
33   <search base="base">
34     <query>| stats sum(count) by src_ip, src_class | sort -count</query>
35   </search>
36   <option name="count">10</option>
```

- **Destination IP Table:**

| stats sum(count) by dest_ip, dest_class | sort -count

```
49 <title>Connections by Destination IP</title>
50 <table>
51 <search base="base">
52 <query>| stats sum(count) by dest_ip, dest_class | sort -count</query>
53 </search>
```

- Dashboard view showing IPs with private or public.

Firewall v2 ☆ Edit Export ▾ ...

Time: Aug 31, 2017 ▼ Source IP: * Destination IP: * Hide Filters

Connections by Source IP			Connections by Destination IP		
src_ip ▴	src_class ▴	sum(count) ▴	dest_ip ▴	dest_class ▴	sum(count) ▴
10.0.1.100	private	6851	10.0.1.100	private	1318
10.0.1.101	private	14	10.0.2.103	private	15
10.0.1.200	private	6420	10.0.2.108	private	17
10.0.1.220	private	48	10.0.2.250	private	48
10.0.1.222	private	30	104.131.53.252	public	15
10.0.2.102	private	69	129.6.15.29	public	24
10.0.2.103	private	366	138.91.159.158	public	51
10.0.2.105	private	212	172.217.11.238	public	15
10.0.2.107	private	275	192.43.172.30	public	16
10.0.2.108	private	252	198.58.110.84	public	37

« Prev **1** 2 Next » « Prev **1** 2 3 4 Next »

Step 3: Configure Conditional Drilldowns

Use <condition> inside <drilldown>:

- **Source IP Table:**

<drilldown>

<condition match='\$row.src_class\$ == "private"'>

<link target="_blank"><https://www.rfc-editor.org/rfc/rfc1918></link>

</condition>

<condition match='\$row.src_class\$ == "public"'>

<link target="_blank">[https://www.virustotal.com/gui/ip-address/\\$row.src_ip\\$](https://www.virustotal.com/gui/ip-address/$row.src_ip$)</link>

</condition>

</drilldown>

```

30 <panel>
31   <title>Connections by Source IP</title>
32   <table>
33     <search base="base">
34       <query>| stats sum(count) by src_ip, src_class | sort -count</query>
35     </search>
36     <option name="count">10</option>
37     <option name="dataOverlayMode">none</option>
38     <option name="drilldown">cell</option>
39     <option name="percentagesRow">>false</option>
40     <option name="rowNumbers">>false</option>
41     <option name="totalsRow">>false</option>
42     <option name="wrap">>true</option>
43     <drilldown>
44       <condition match='$row.src_class$ == "private"'>
45         <link target="_blank">https://www.rfc-editor.org/rfc/rfc1918</link>
46       </condition>
47       <condition match='$row.src_class$ == "public"'>
48         <link target="_blank">https://www.virustotal.com/gui/ip-address/$row.src_ip$</link>
49       </condition>
50     </drilldown>
51   </table>
52 </panel>

```

- **Destination IP Table:**

```

<drilldown>
<condition match='$row.dest_class$ == "private"'>
  <link target="_blank">https://www.rfc-editor.org/rfc/rfc1918</link>
</condition>
<condition match='$row.dest_class$ == "public"'>
  <link target="_blank">https://www.virustotal.com/gui/ip-address/$row.dest_ip$</link>
</condition>
</drilldown>

```

```

53 <panel>
54   <title>Connections by Destination IP</title>
55   <table>
56     <search base="base">
57       <query>| stats sum(count) by dest_ip, dest_class | sort -count</query>
58     </search>
59     <option name="count">10</option>
60     <option name="dataOverlayMode">none</option>
61     <option name="drilldown">cell</option>
62     <option name="percentagesRow">>false</option>
63     <option name="rowNumbers">>false</option>
64     <option name="totalsRow">>false</option>
65     <option name="wrap">>true</option>
66     <drilldown>
67       <condition match='$row.dest_class$ == "private"'>
68         <link target="_blank">https://www.rfc-editor.org/rfc/rfc1918</link>
69       </condition>
70       <condition match='$row.dest_class$ == "public"'>
71         <link target="_blank">https://www.virustotal.com/gui/ip-address/$row.dest_ip$</link>
72       </condition>
73     </drilldown>
74   </table>
75 </panel>

```

- Dashboard with clickable IPs.

Firewall v2

☆

Edit

Export ▾

...

Time

Source IP

Destination IP

Aug 31, 2017 ▾

*

*

Hide Filters

Connections by Source IP

Connections by Destination IP

src_ip ▾	src_class ▾	sum(count) ▾	dest_ip ▾	dest_class ▾	sum(count) ▾
10.0.1.100	private	6851	10.0.1.100	private	1318
10.0.1.101	private	14	10.0.2.103	private	15
10.0.1.200	private	6420	10.0.2.108	private	17
10.0.1.220	private	48	10.0.2.250	private	48
10.0.1.222	private	30	104.131.53.252	public	15
10.0.2.102	private	69	129.6.15.29	public	24
10.0.2.103	private	366	138.91.159.158	public	51
10.0.2.105	private	212	172.217.11.238	public	15
10.0.2.107	private	275	192.43.172.30	public	16
10.0.2.108	private	252	198.58.110.84	public	37

« Prev

1

2

Next »

« Prev

1

2

3

4

Next »

<

>

↺

↻

rfc-editor.org / RFC 1918: Address Allocation for Private Internets

☆

🔗

📄

🔍

☰

⋮

Assistant

⌵

🔴

🗂

ads-1

niches

Imported From C...

[\[RFC Home\]](#)
[\[TEXT\]](#)
[\[PDF\]](#)
[\[HTML\]](#)
[\[Tracker\]](#)
[\[IPB\]](#)
[\[Errata\]](#)
[\[Info page\]](#)

BEST CURRENT PRACTICE

Updated by: [6761](#)

Network Working Group

Request for Comments: 1918

Obsoletes: [1627](#), [1597](#)

BCP: 5

Category: Best Current Practice

Errata Exist

Y. Rekhter

Cisco Systems

B. Moskowitz

Chrysler Corp.

D. Karrenberg

RIPE NCC

G. J. de Groot

RIPE NCC

E. Lear

Silicon Graphics, Inc.

February 1996

Address Allocation for Private Internets

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

1. Introduction

For the purposes of this document, an enterprise is an entity autonomously operating a network using TCP/IP and in particular determining the addressing plan and address assignments within that network.

This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private.

2. Motivation

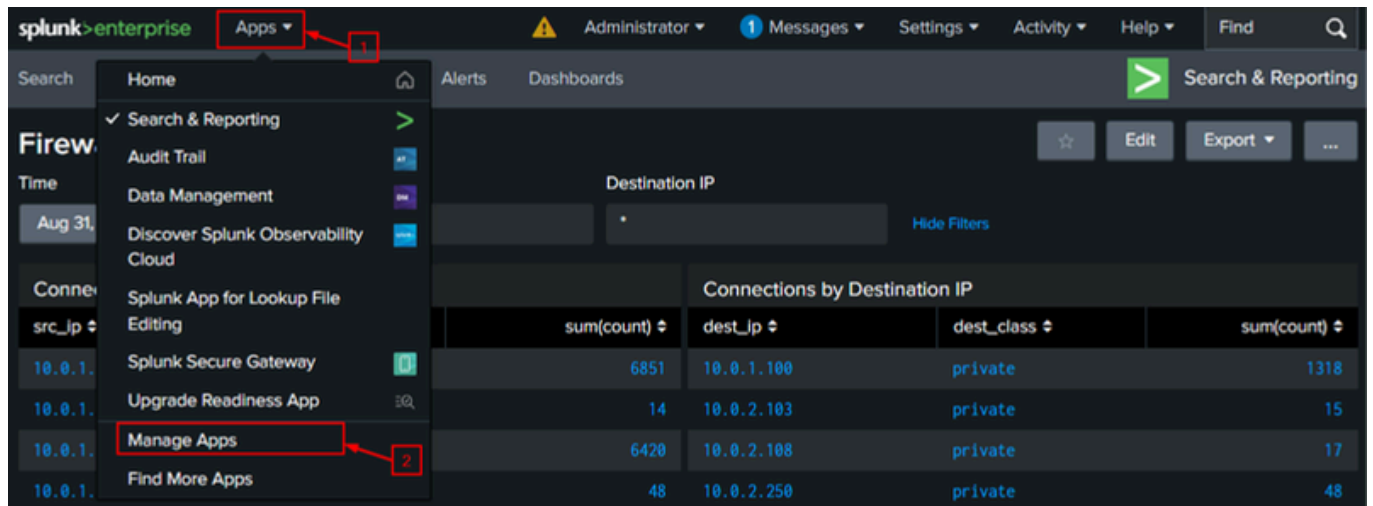
With the proliferation of TCP/IP technology worldwide, including outside the Internet itself, an increasing number of non-connected enterprises use this technology and its addressing capabilities for sole intra-enterprise communications. without any intention to ever

Customizing Dashboard Navigation and Layout

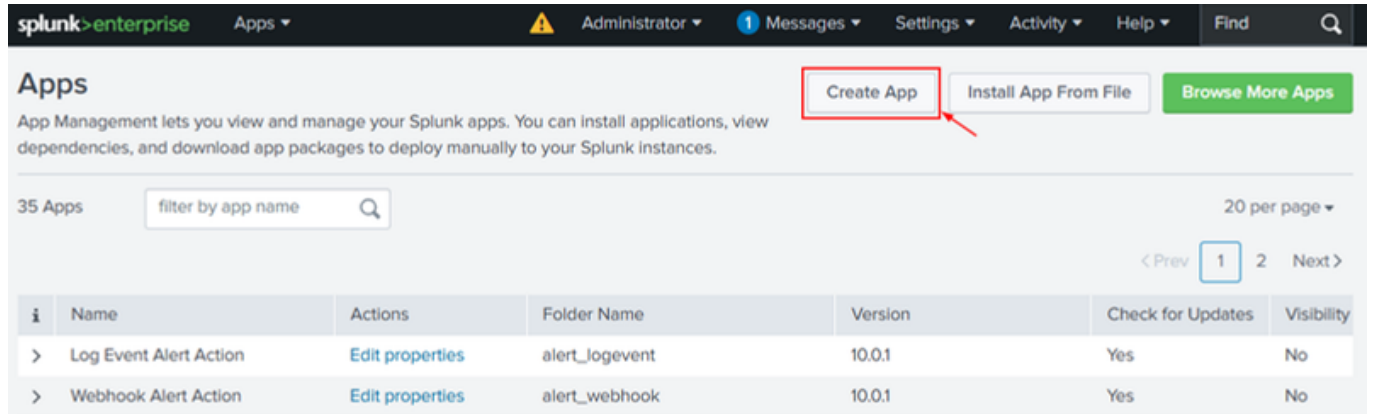
Creating a custom Splunk app with a tailored navigation bar ensures analysts land directly on the most relevant dashboard like a Firewall Analysis Dashboard for faster investigations.

Step 1: Create the Custom App

- Go to **Apps** → **Manage Apps**.



- Click **Create App**.



3. Fill in:

- Name:** Firewall
- Folder Name:** firewall
- Version:** 1.0.0
- Template:** barebones

4. Click **Save**.

Creating Visualizations and Interactive Dashboards

Create App

Name: Firewall
Give your app a friendly name for display in Splunk Web.

Folder name *: firewall
This name maps to the app's directory in \$SPLUNK_HOME/etc/apps/.

Version *: 1.0.0
App version

Visible: Yes No
Only apps with views should be made visible.

Author: Salma
Name of the app's owner.

Description:
Enter a description for your app.

Template: barebones sample app
These templates contain example views and searches.

Cancel Save

- Firewall app visible in the Apps menu.

splunk>enterprise Apps Administrator 1 Messages Settings Activity Help Find

Apps

App Management dependencies

36 Apps

Home

- Search & Reporting
- Audit Trail
- Data Management
- Discover Splunk Observability Cloud
- Firewall**
- Splunk App for Lookup File Editing
- Splunk Secure Gateway
- Upgrade Readiness App
- Manage Apps
- Find More Apps

Version 2 Data Set

Create App Install App From File Browse More Apps

20 per page

< Prev 1 2 Next >

	Folder Name	Version	Check for Updates	Visibility
rties	alert_logevent	10.0.1	Yes	No
rties	alert_webhook	10.0.1	Yes	No
rties	appsbrowser	10.0.1	Yes	No
rties	audit_trail	1.0.0	Yes	Yes
rties	botsv2_data_set		No	No

Step 2: Move Dashboard View to the App

Move the existing dashboard (firewall_v2.xml) into the new app:

`mv search/local/data/ui/views/firewall_v2.xml firewall/default/data/ui/views/`

```
root@splunk:/opt/splunk/etc/apps# mv search/local/data/ui/views/firewall_v2.xml firewall/default/data/ui/views/
```

Step 3: Customize Navigation

- Edit the app's navigation file:

```
sudo nano firewall/default/data/ui/nav/default.xml
```

- Update contents:

```
<nav search_view="search">
  <view name="firewall_v2" default='true' />
  <view name="search" />
</nav>
```

```
<nav search_view="search">
  <view name="firewall_v2" default='true' />
  <view name="search" />
</nav>
```

- default='true' makes Firewall v2 the landing page.
- Retain Search as a secondary tab.

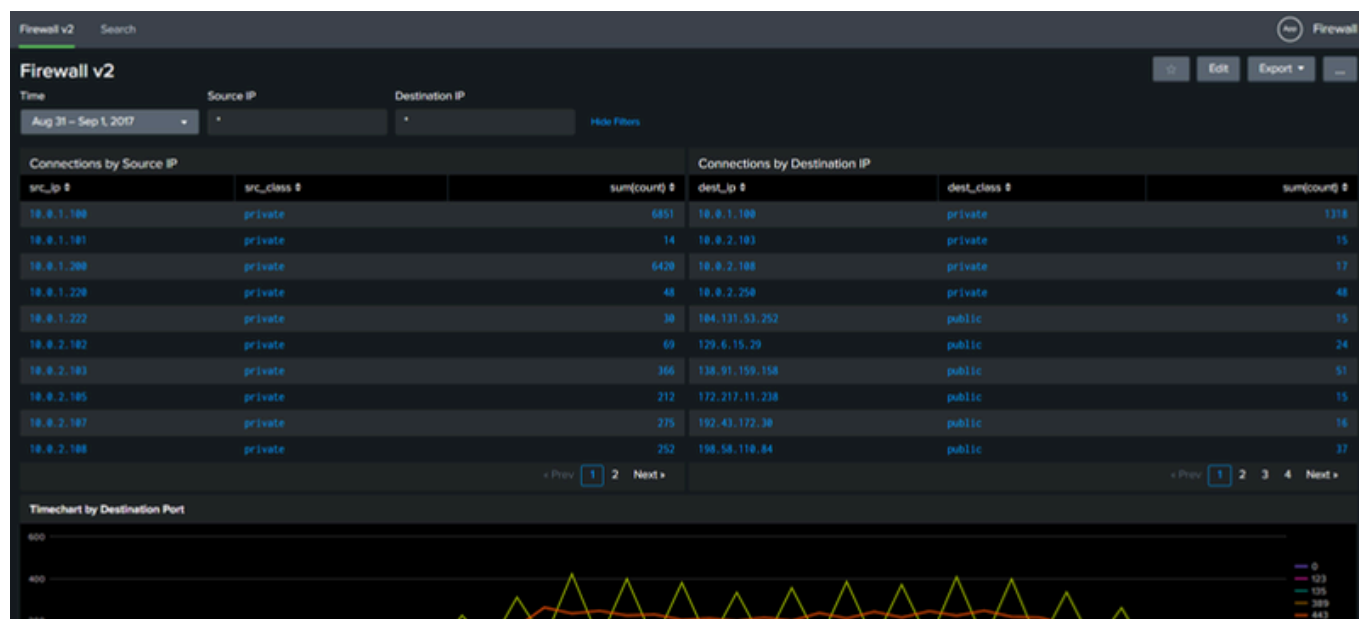
Step 4: Refresh and Verify

- Clear cache:

```
http://<splunk-server>:8000/en-US/debug/refresh
```



- Result:
 - URL shows **/en-US/app/firewall/firewall_v2**.
 - Navigation bar displays **Firewall v2** and **Search**.
 - Dashboard loads with panels for source/destination IPs and timechart.



Next-Gen Dashboards An Exploration of Dashboard Studio

Splunk's Dashboard Studio is the next generation of dashboard creation offering free positioning, custom graphics, and advanced styling for a modern, interactive experience. While the classic editor is still supported, new features are increasingly exclusive to Dashboard Studio.

Why Dashboard Studio?

- Full creative control over layout and design.
- Easy integration of images and custom visuals.
- Advanced configuration options for colors, fonts, and chart styling.

Cloning a Classic Dashboard into Dashboard Studio

You don't need to rebuild dashboards from scratch. Instead, clone your existing dashboard:

1. Open the classic dashboard (e.g., Firewall v2).
2. Click **More Options (three dots)** → **Clone in Dashboard Studio**.

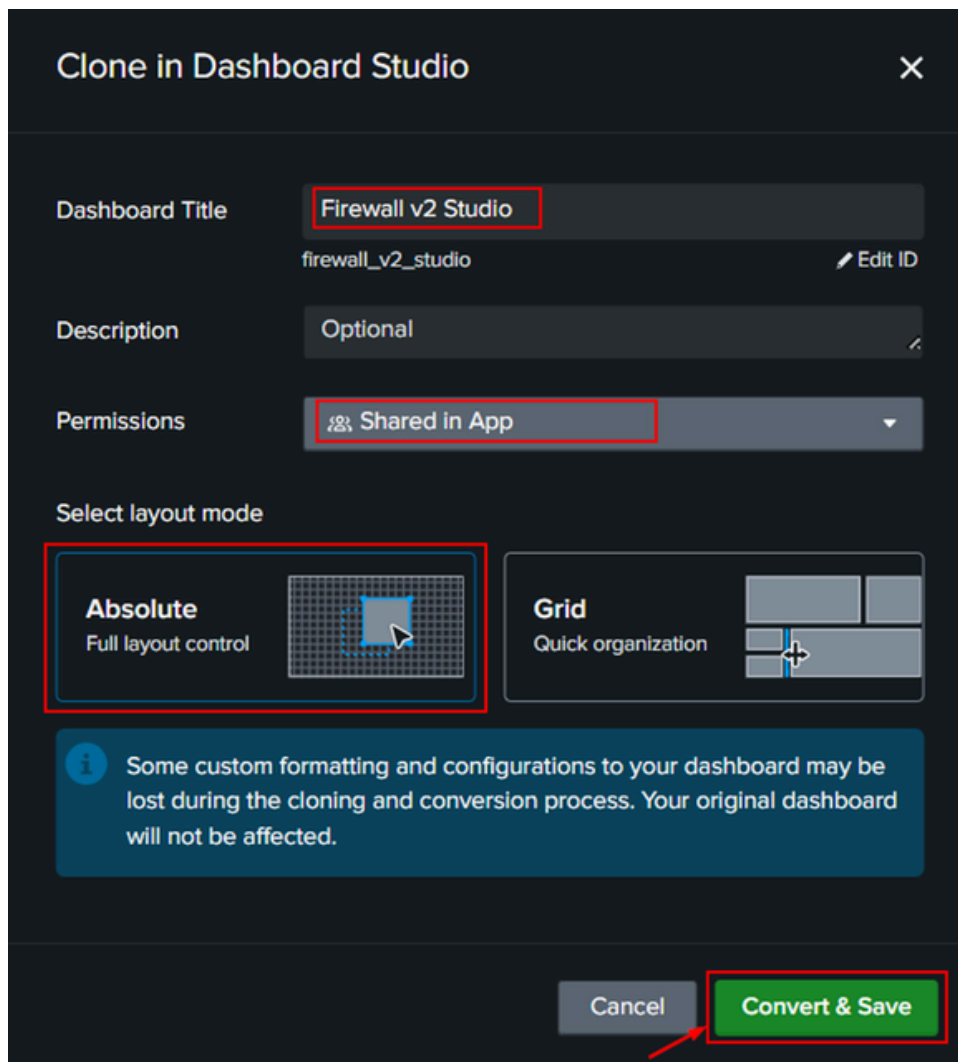
The screenshot shows the 'Firewall v2' dashboard in Splunk. At the top, there's a search bar and a 'Firewall' app icon. Below the title, there are buttons for 'Edit', 'Export', and a 'More Options' menu (three dots). A red box highlights the 'More Options' menu, and a red arrow points to the 'Clone in Dashboard Studio' option, which is also highlighted with a red box. Below the menu, there are two tables: 'Connections by Source IP' and 'Connections by Destination IP'. The 'Connections by Source IP' table has columns for 'src_ip', 'src_class', and 'sum(count)'. The 'Connections by Destination IP' table has columns for 'dest_ip' and 'sum(count)'. At the bottom, there's a 'Timechart by Destination Port' visualization showing a line chart with multiple data series.

Connections by Source IP			Connections by Destination IP	
src_ip	src_class	sum(count)	dest_ip	sum(count)
10.0.1.100	private	6851	10.0.1.100	15
10.0.1.101	private	14	10.0.2.103	15
10.0.1.200	private	6420	10.0.2.108	17
10.0.1.220	private	48	10.0.2.250	48
10.0.1.222	private	30	104.131.53.252	15
10.0.2.102	private	69	129.6.15.29	24
10.0.2.103	private	366	138.91.159.158	51
10.0.2.105	private	212	172.217.11.238	15
10.0.2.107	private	275	192.43.172.30	16
10.0.2.108	private	252	198.58.110.84	37

Conversion Settings

In the **Clone in Dashboard Studio** window:

- **Dashboard Title:** Set a name (e.g., Firewall v2 Studio).
- **Permissions:** Choose sharing level (e.g., Shared in App).
- **Layout Mode:**
 - **Absolute:** Full control for free positioning.
 - **Grid:** Quick organization similar to classic editor. Note: Some custom formatting may not transfer, but your original dashboard remains unchanged.
- Click **Convert & Save**.



The screenshot shows the 'Clone in Dashboard Studio' window with the following settings:

- Dashboard Title:** Firewall v2 Studio (with a red box around the text and 'firewall_v2_studio' below it).
- Description:** Optional.
- Permissions:** Shared in App (with a red box around the dropdown).
- Select layout mode:**
 - Absolute:** Full layout control (with a red box around the selection and a grid icon).
 - Grid:** Quick organization (with a grid icon).

A blue information box states: 'Some custom formatting and configurations to your dashboard may be lost during the cloning and conversion process. Your original dashboard will not be affected.'

At the bottom, there are two buttons: 'Cancel' and 'Convert & Save' (with a red box around it and a red arrow pointing to it).

Working in Dashboard Studio

Once cloned:

- Use the Configuration panel to customize:
 - Background color
 - Chart colors

- Axis titles
- Line styles and markers
- Add tabs, adjust gridlines, and apply dark/light themes

