

VPN LOGS

1. Filter Firewall Event logs.

`index="fortinet" sourcetype="fortigate_event"`

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Haydar Akyurek', '998 Messages', 'Settings', 'Activity', and 'Help'. Below this is a 'Search & Reporting' section with a search bar containing the query `index=fortinet sourcetype="fortigate_event"`. The search results show 35 events from 10/6/25 9:11:00.000 AM to 10/6/25 9:26:00.000 AM. The interface includes tabs for 'Events (35)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is active, showing a timeline visualization with a green bar representing the event duration. At the bottom, there are buttons for 'List', 'Format', and '20 Per Page'.

2. List VPN users and their assigned internal IP addresses in the last 15 minutes.

`index=fortinet sourcetype="fortigate_event" | stats count by xauthuser assignip`

The screenshot shows the Splunk Enterprise interface with the same search bar as before, but the query is now `index=fortinet sourcetype="fortigate_event" | stats count by xauthuser assignip`. The search results show 35 events from 10/6/25 9:13:02.000 AM to 10/6/25 9:28:02.000 AM. The interface includes tabs for 'Events', 'Patterns', 'Statistics (4)', and 'Visualization'. The 'Statistics' tab is active, showing a table with columns for 'xauthuser', 'assignip', and 'count'. The table has one row with 'N/A' for both 'xauthuser' and 'assignip', and a 'count' of 3.

xauthuser	assignip	count
N/A	N/A	3

3. List VPN users and their external IP addresses in the last 15 minutes.

`index=fortinet sourcetype="fortigate_event" xauthuser!=N/A earliest=-1h latest=now | stats count by xauthuser, remip`

The screenshot shows the Splunk Enterprise interface with the same search bar as before, but the query is now `index=fortinet sourcetype="fortigate_event" xauthuser!=N/A earliest=-1h latest=now | stats count by xauthuser, remip`. The search results show 12 events from 10/6/25 9:15:14.000 AM to 10/6/25 9:30:14.000 AM. The interface includes tabs for 'Events', 'Patterns', 'Statistics (2)', and 'Visualization'. The 'Statistics' tab is active, showing a table with columns for 'xauthuser', 'remip', and 'count'. The table has two rows, one for 'xauthuser' and one for 'remip', both with a 'count' of 1.

xauthuser	remip	count
		1
		1

4. List VPN users and their internal IP addresses that have failed login attempts in the last 24 hours.

splunk>enterpriseApps

Haydar Akyurek998MessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New Search

Save AsCreate Table ViewClose

index=fortinet sourcetype="fortigate_event" action=failure xauthuser!=N/A |stats count by xauthuser remipLast 24 hours

2 events (10/5/25 10:00:00.000 AM to 10/6/25 10:01:31.000 AM)No Event SamplingJobPauseRefreshDownloadSmart Mode

EventsPatternsStatistics (1)Visualization

20 Per PageFormatPreview

xauthuser

remip

count