Zyxel Zywall Firewall logs Analytics Using Splunk

Index

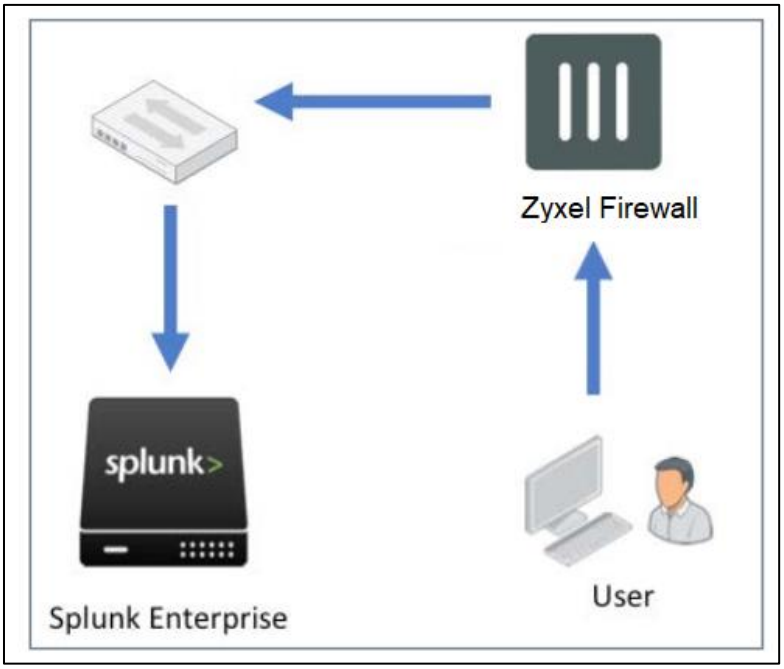
Table of Contents

Overview

ZyWALL firewalls are designed to deliver the fastest performance for multi-site deployments. The ZyWALL supports high-throughput IPSec, L2TP over IPSec, and SSL VPN for a wide range of site-to-client and site-to-site VPN deployments. Zyxel VPN Firewall simplifies complex firmware updates with its new Cloud Helper service. This firewall also generates the logs in various categories like traffic log, system monitoring, DHCP logs, security policy control logs and many more. So, having the one location where you can see everything related this information will give a quick glance of network environment.
The Zyxel firewall monitor app is based on logs that has being forwarded to splunk by receiving at port 514 which is default. Also, the apps default setting for index, sourcetype is being saved in Eventtype, you can change this setting as per your configuration from the link provided in apps home dashboard.

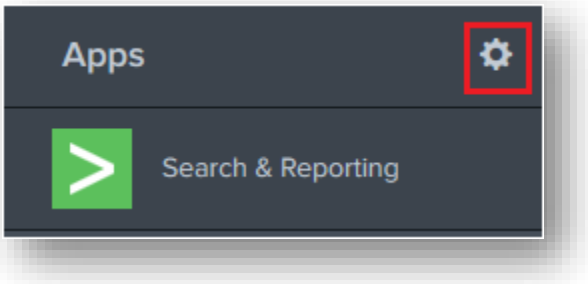
About Splunk

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.

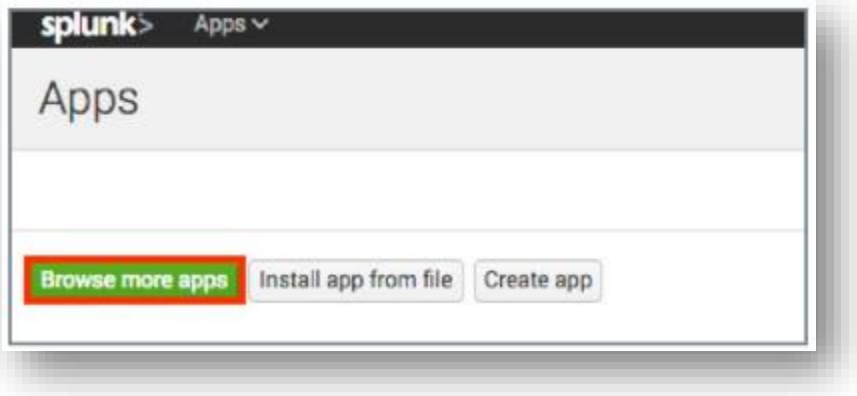


Splunk Configuration

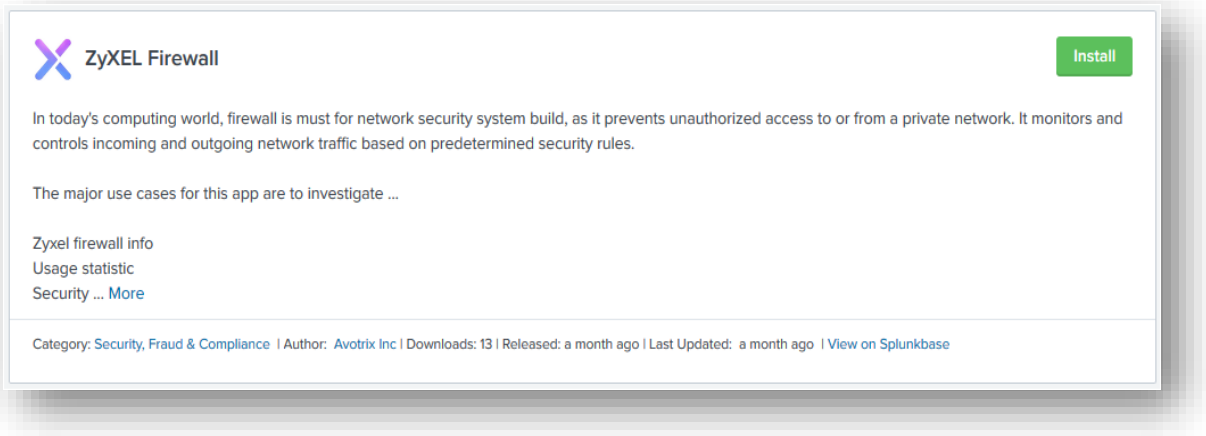
1. To install Splunk Apps, click the gear.



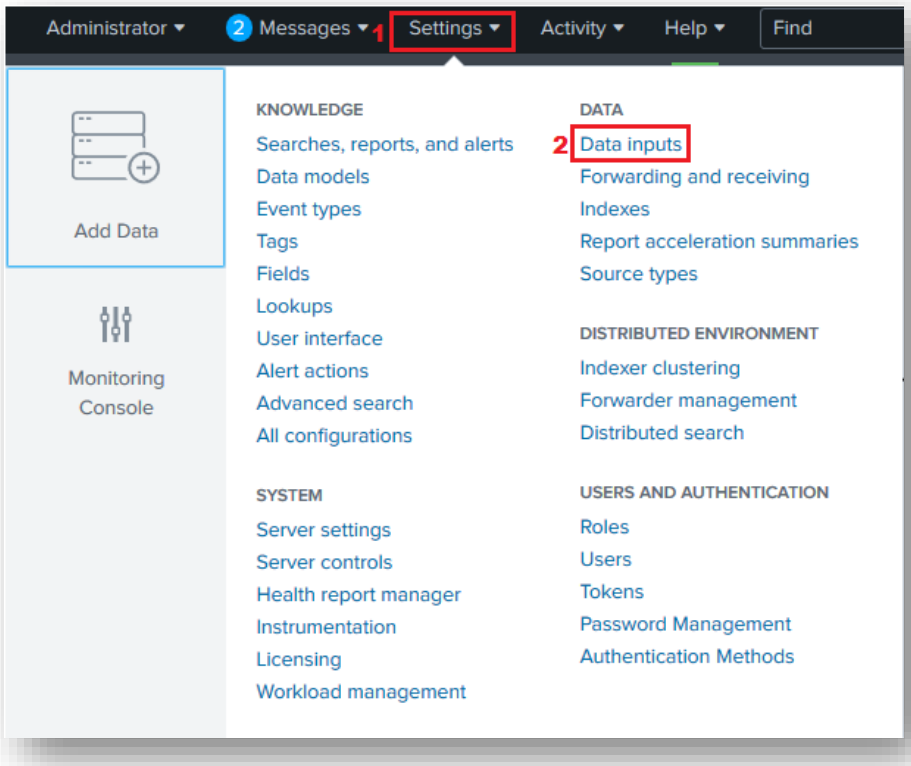
2. To install Splunk Apps, click the gear. Click Browse more apps and search for “Zyxel Firewall”



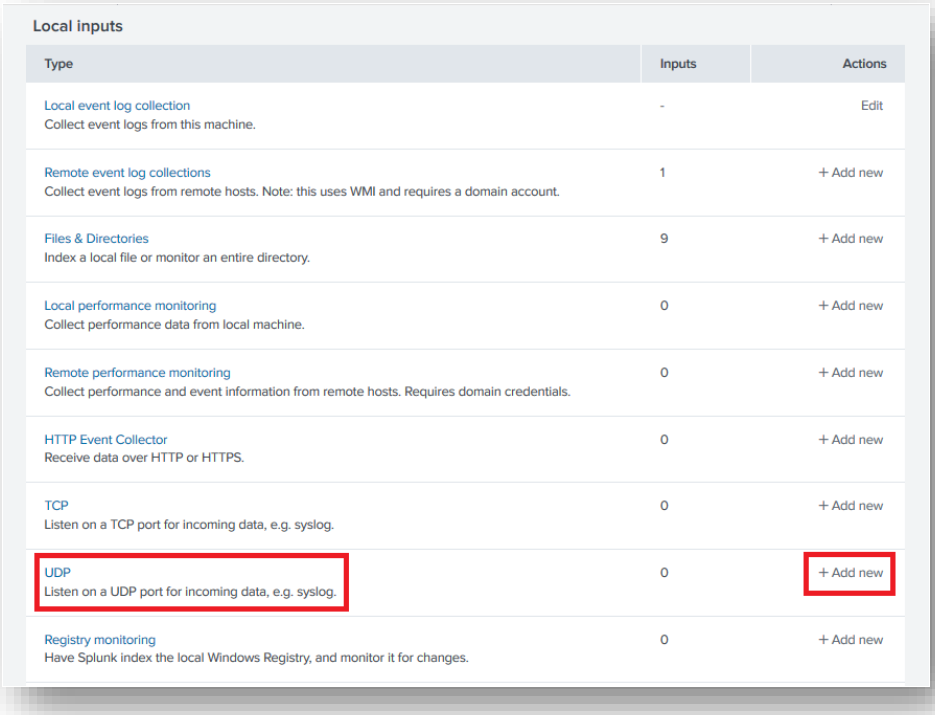
3. Install Zyxel Firewall App for Splunk. Enter your splunk.com username & password.



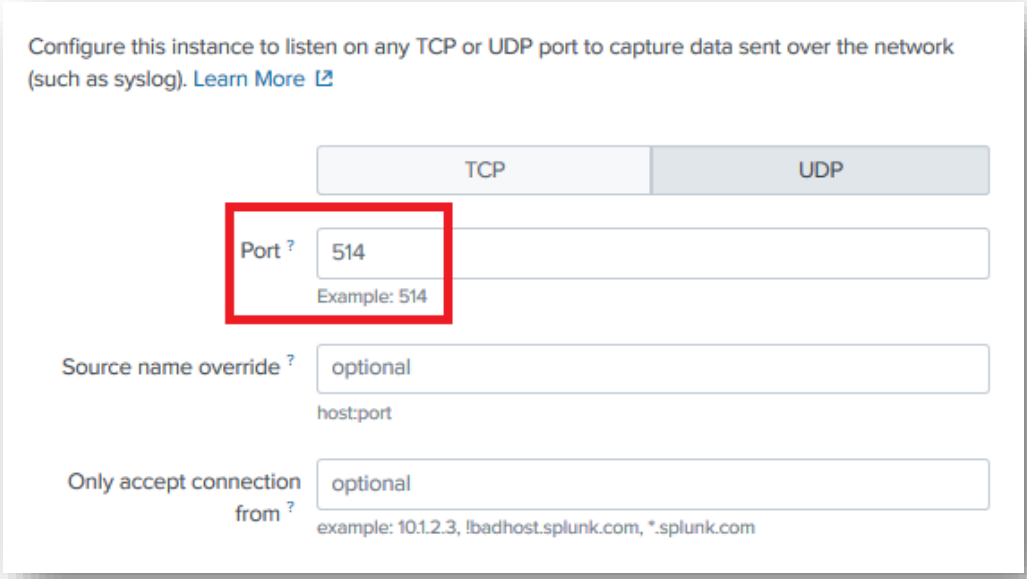
4. From the setting click Data Inputs.



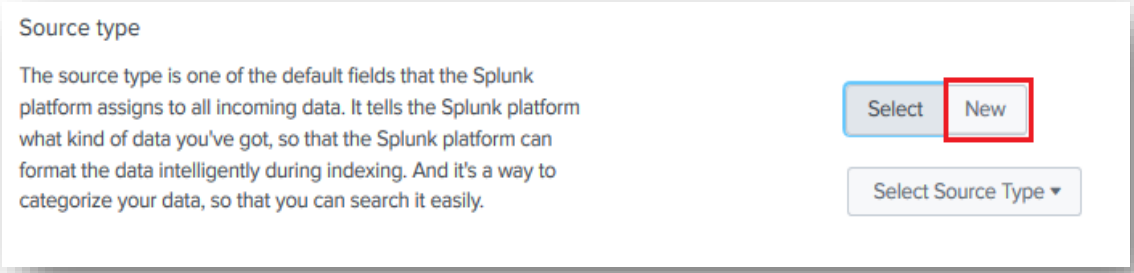
5. Under Data Inputs create a new UDP input by clicking Add new on the right.



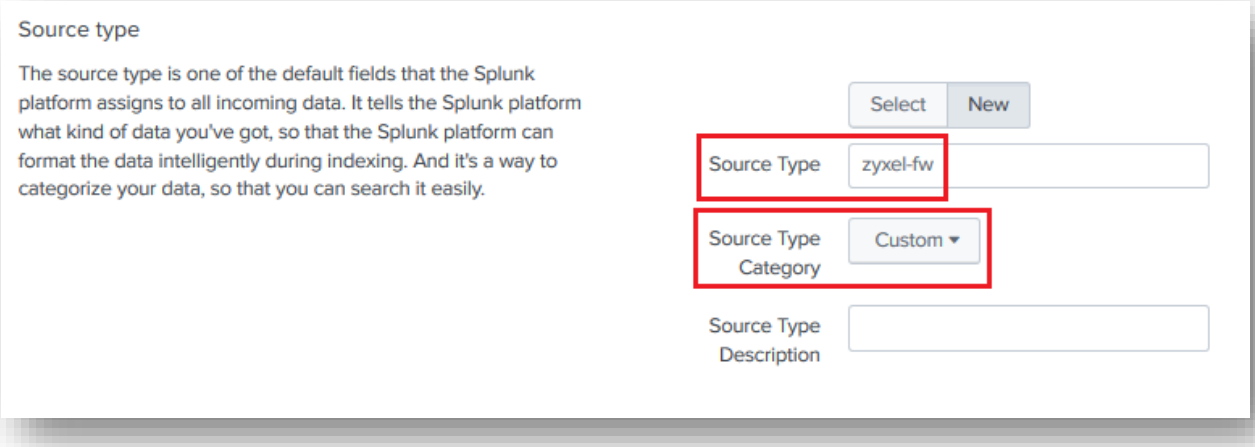
6. Create a UDP Data Source on Port 514.



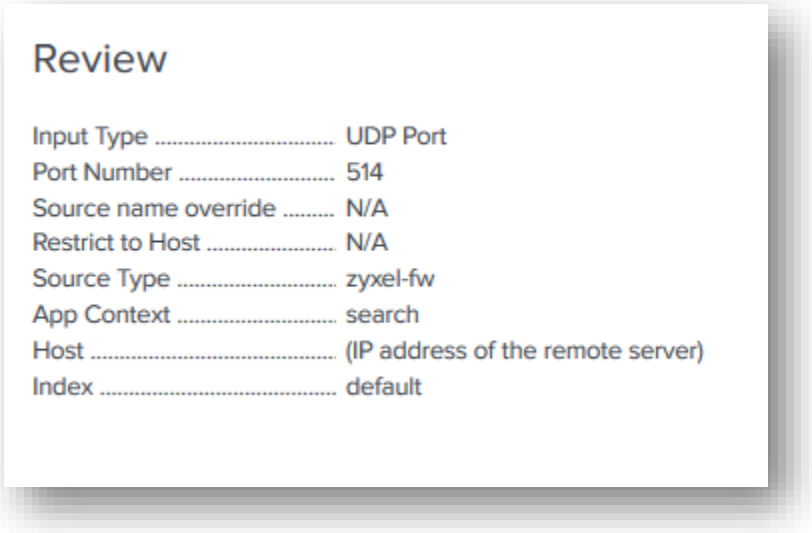
7. Click New



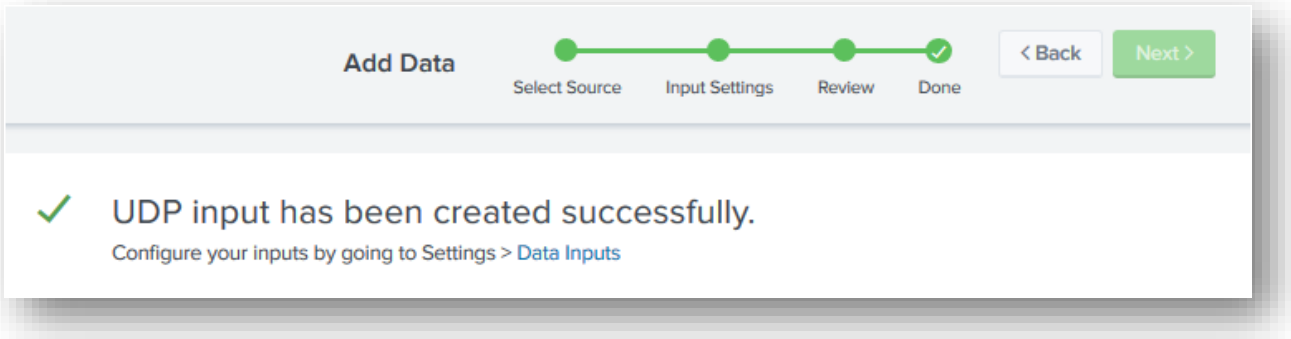
8. Under Input Settings set the Source Type to “zyxel-fw”. Set the Source Type Category to Custom.



9. Click Review.

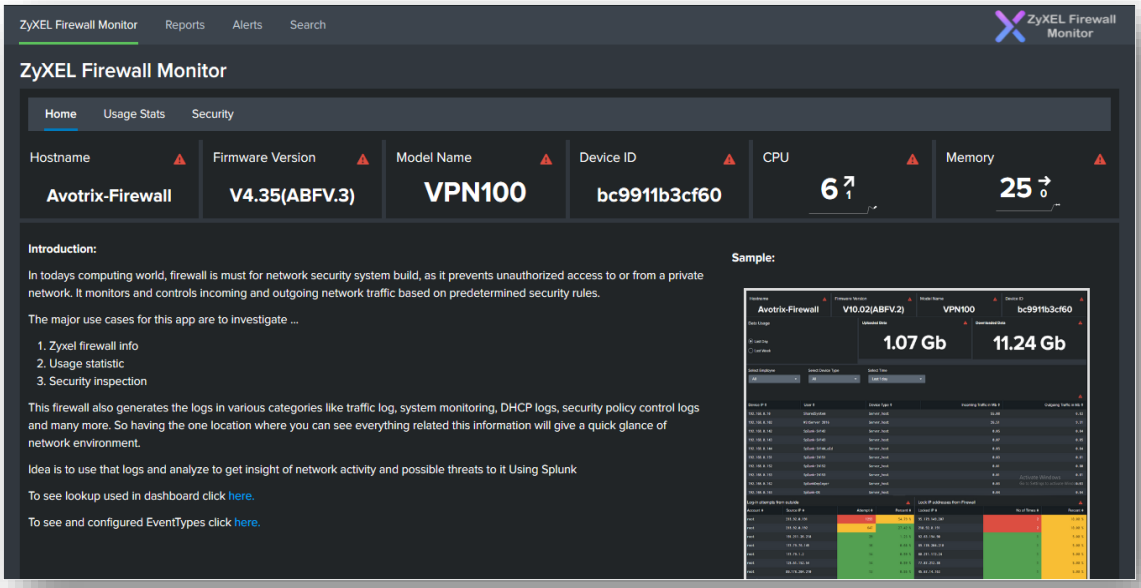


10. Click Submit.



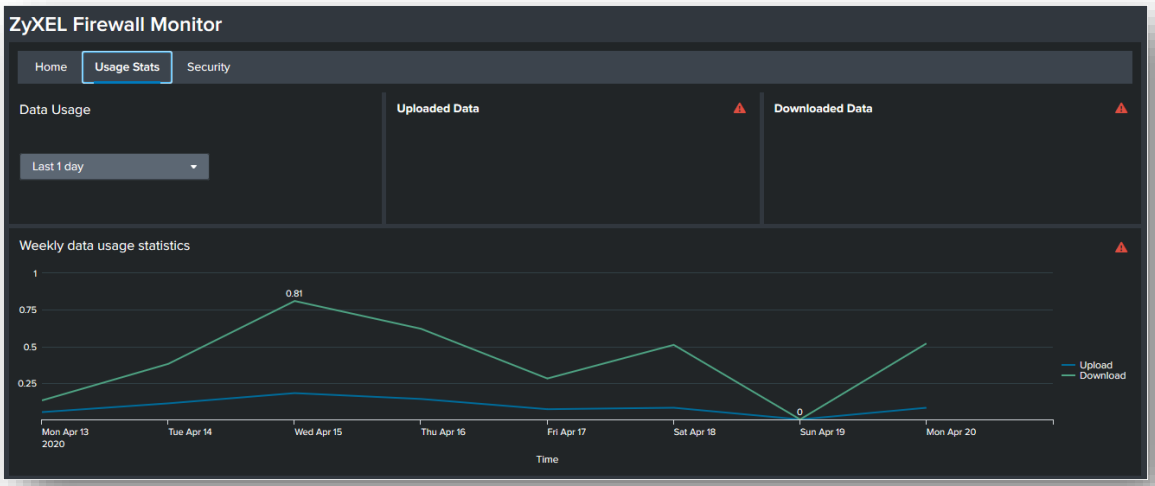
Zyxel Firewall Monitor

It provides information related to hardware firewall device incorporated in company environment.



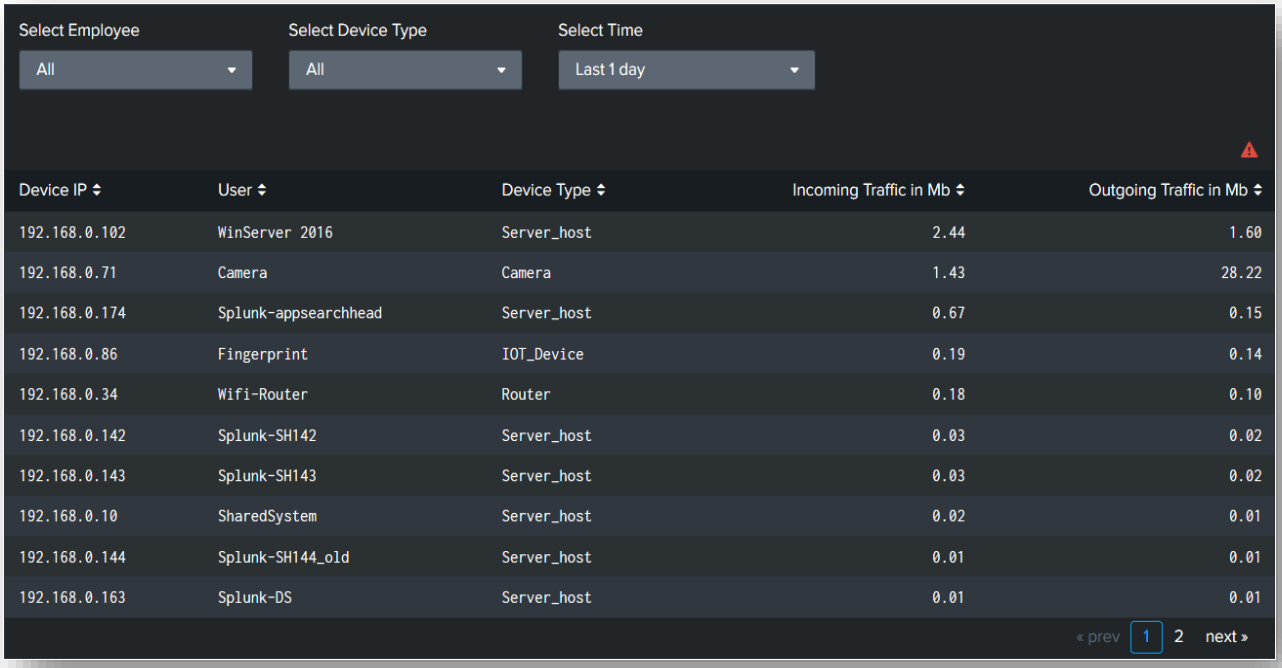
Usage Status

It shows daily or weekly data consumption through network i.e outgoing and incoming Traffic.



Data usage:

It shows Outgoing /incoming data consumption of all the network devices connected to our company network. The traffic logs contain Data usage based on the MAC addresses available in firewall logs, so to get the actual list of devices we had to create the Lookup with MAC and IP addresses along with devices owner.

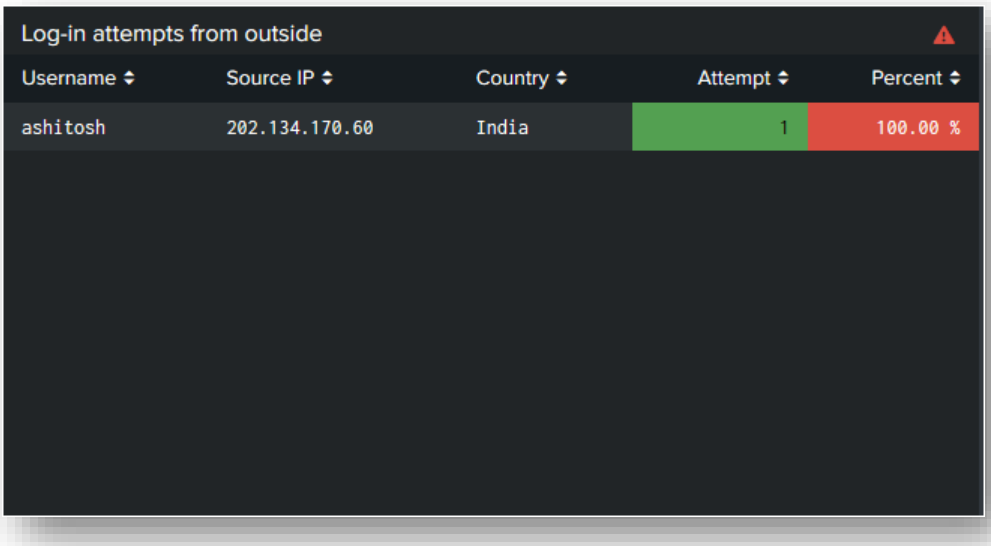


Device IP	User	Device Type	Incoming Traffic in Mb	Outgoing Traffic in Mb
192.168.0.102	WinServer 2016	Server_host	2.44	1.60
192.168.0.71	Camera	Camera	1.43	28.22
192.168.0.174	Splunk-appsearchhead	Server_host	0.67	0.15
192.168.0.86	Fingerprint	IOT_Device	0.19	0.14
192.168.0.34	Wifi-Router	Router	0.18	0.10
192.168.0.142	Splunk-SH142	Server_host	0.03	0.02
192.168.0.143	Splunk-SH143	Server_host	0.03	0.02
192.168.0.10	SharedSystem	Server_host	0.02	0.01
192.168.0.144	Splunk-SH144_old	Server_host	0.01	0.01
192.168.0.163	Splunk-DS	Server_host	0.01	0.01

« prev 1 2 next »

Security

It gives insight of multiple root login attempts in our network by outside network and show IP addresses that has been locked by firewall. By this information we can track the brute force attacks, we could then block those specific attackers too.



Log-in attempts from outside

Username	Source IP	Country	Attempt	Percent
ashitosh	202.134.170.60	India	1	100.00 %

Troubleshooting

What to do if data doesn't show up in the Dashboards?

1. Go to Settings > Data Inputs. Verify that you have a UDP data input enabled on port 514.

2. Verify sourcetype="zyxel-fw".

Summary

Zyxel firewall also generates the logs in various categories like traffic log, system monitoring, DHCP logs, security policy control logs and many more. So, having the one location where you can see everything related this information will give a quick glance of network environment. Zyxel firewall app use that logs and analyze to get insight of network activity and possible threats to it.

Answers community: -https://community.splunk.com/t5/tag/ZyXEL%20Firewall/tg-p/board-id/apps-add-ons-all

Zyxel firewall App: - https://splunkbase.splunk.com/app/4907

YouTube: https://www.youtube.com/watch?v=TAPoPvUjgGc