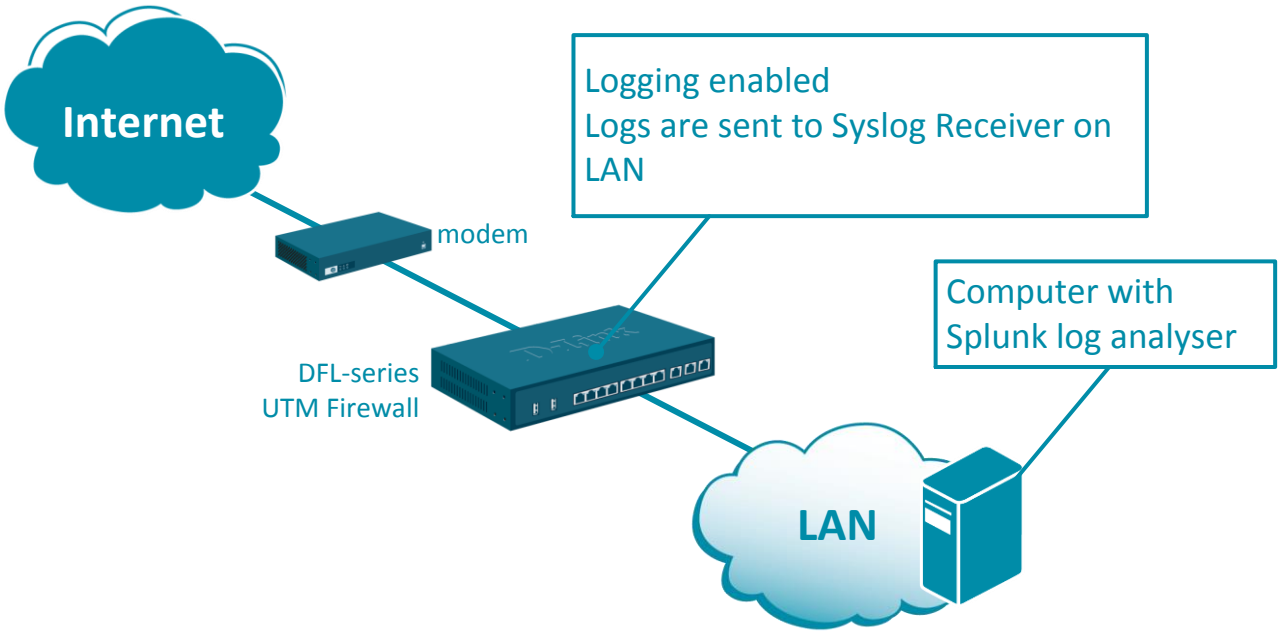
Configuration examples for the D-Link NetDefend Firewall series

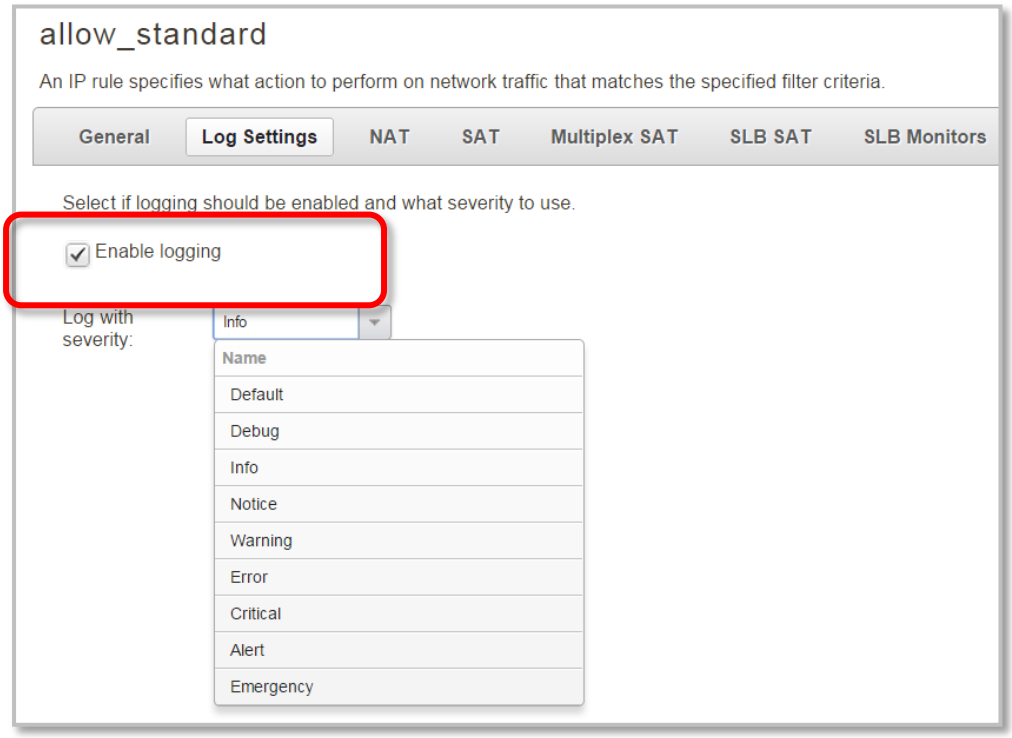
Setting up logging and reporting

This configuration example is based on the following setup:

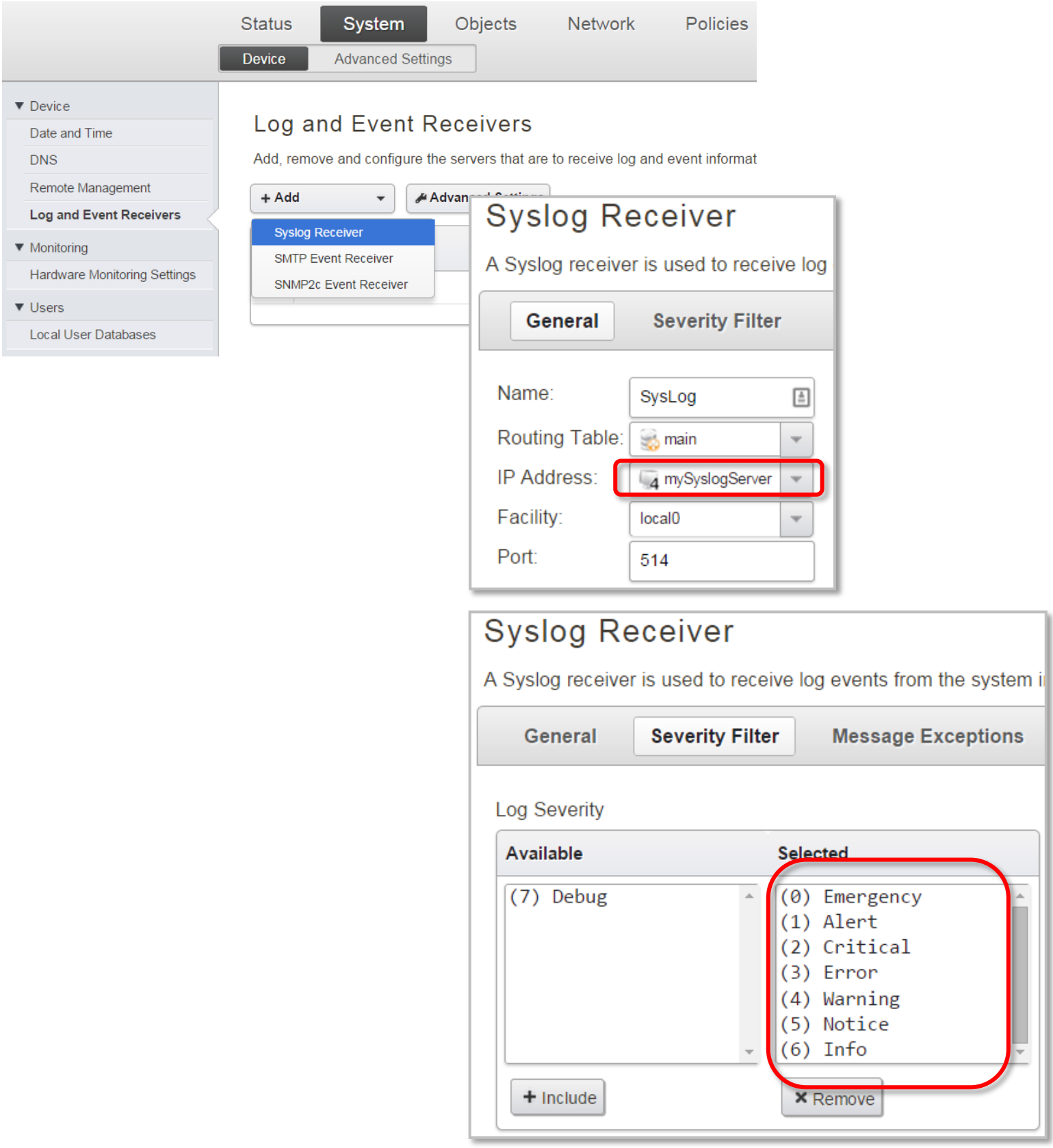


Step 1. Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is "admin" and password is "admin". Set your firewall's WAN settings as per Internet provider requirements.

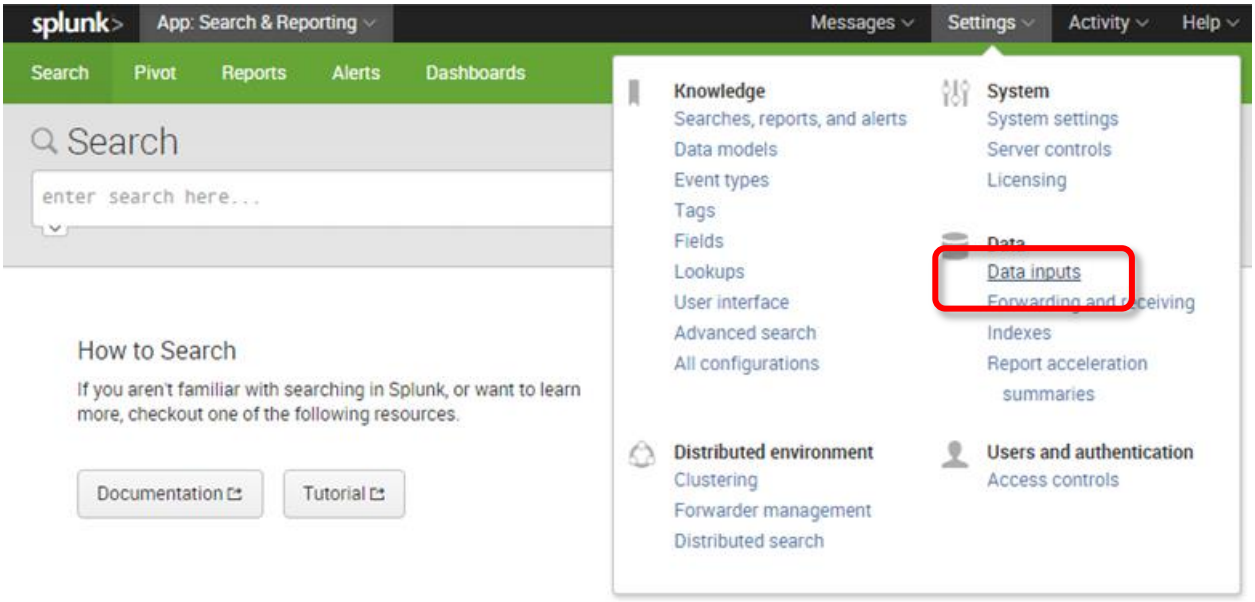
Step 2. Enable logging for the desired IP rules. For monitoring outgoing traffic it is important to enable logging in the main NAT rule: Go to Policies > Main IP Rules > lan_to_wan > edit the "allow_standard" rule. Select "Enable logging".



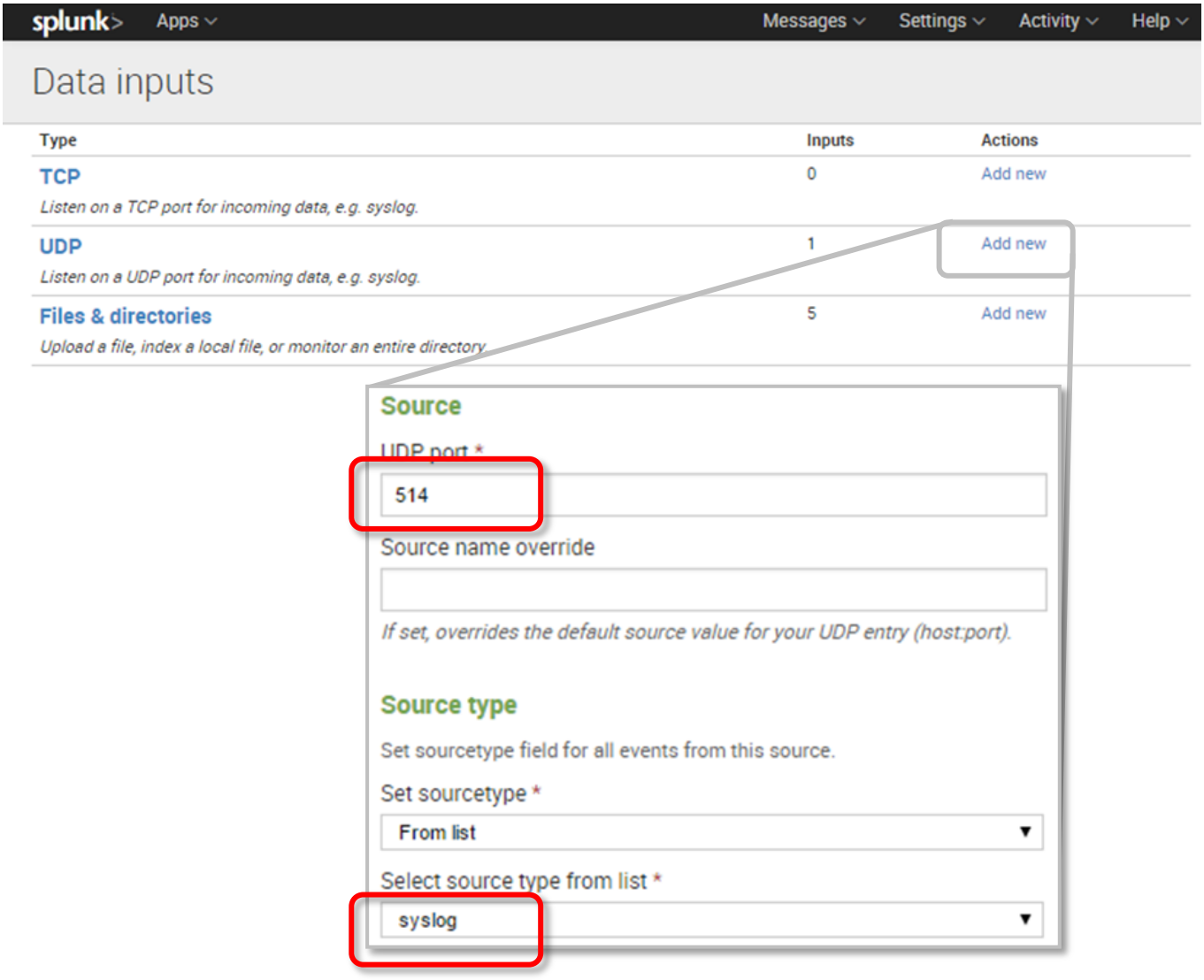
Step 3. Go to Objects > Address Book. Add new IP4 address entry – specify your Syslog/Reporting server IP.
Go to System > Device > Log and Event Receivers. Add a new Syslog Receiver which points to your server IP address.
Click on Severity Filter tab. Specify the event that you want to be logged.



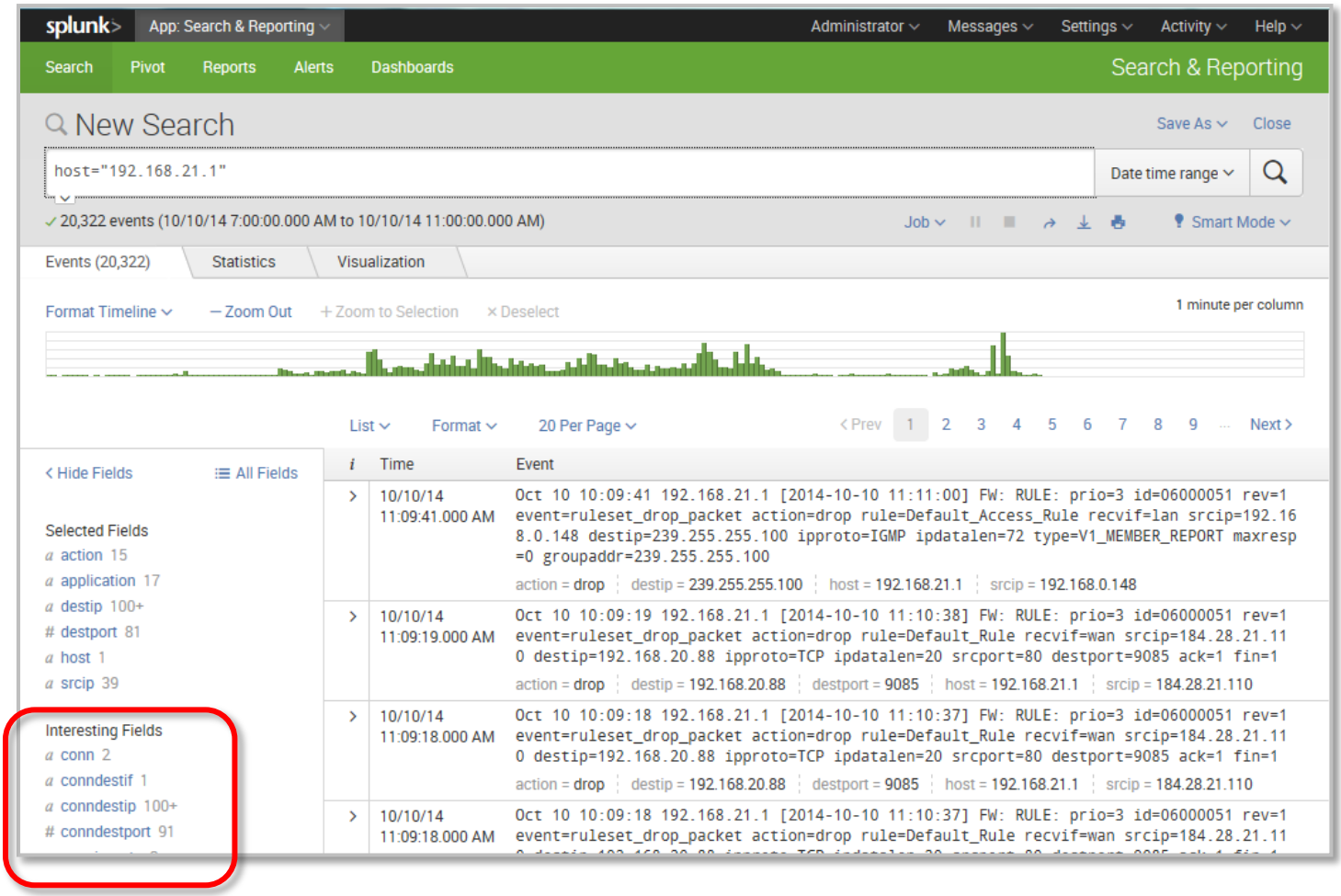
Step 4. Download Splunk Enterprise from www.splunk.com. After installing Splunk add your firewall as new "Data input".



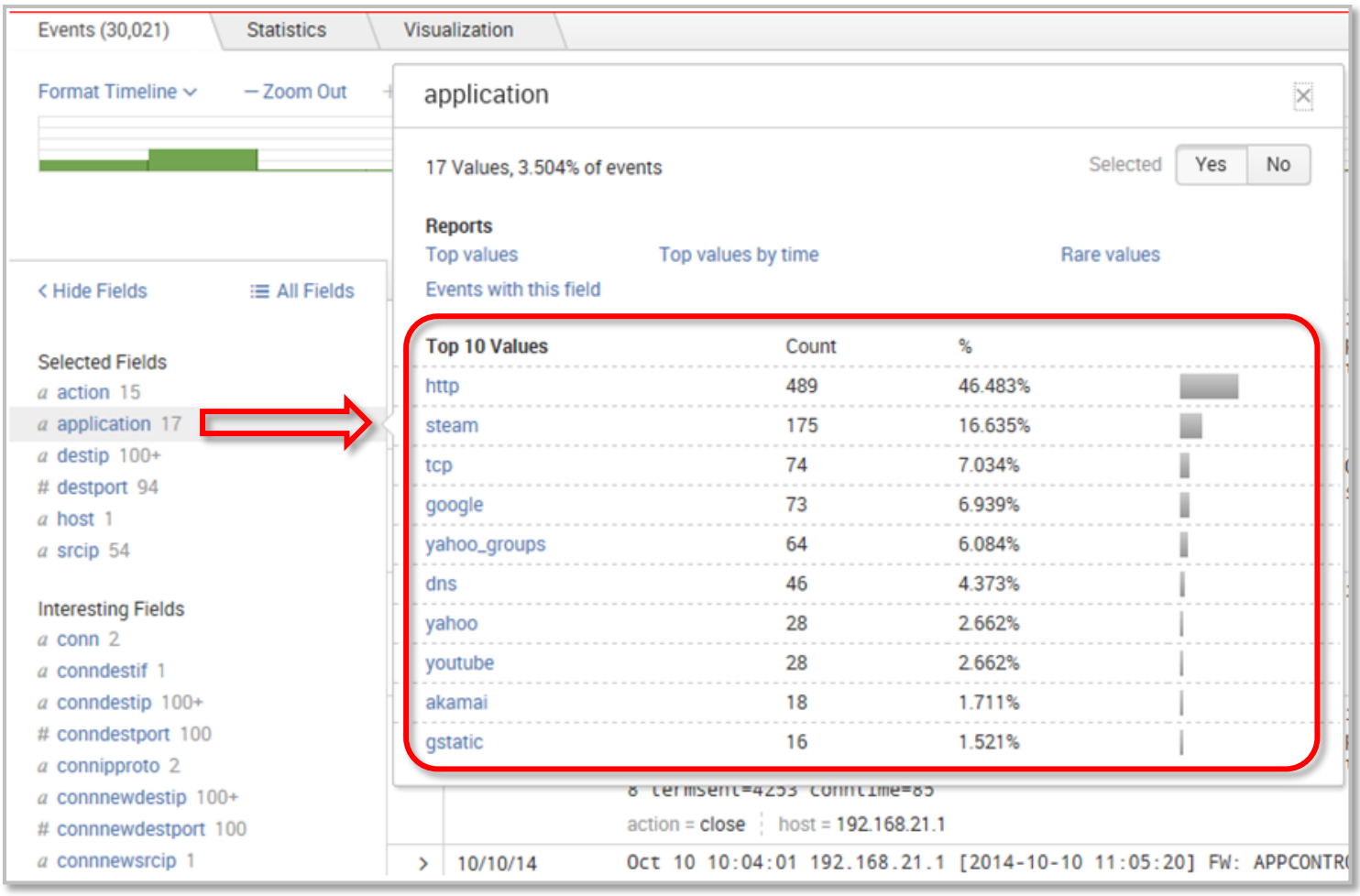
Select data input type as UDP on port 514.



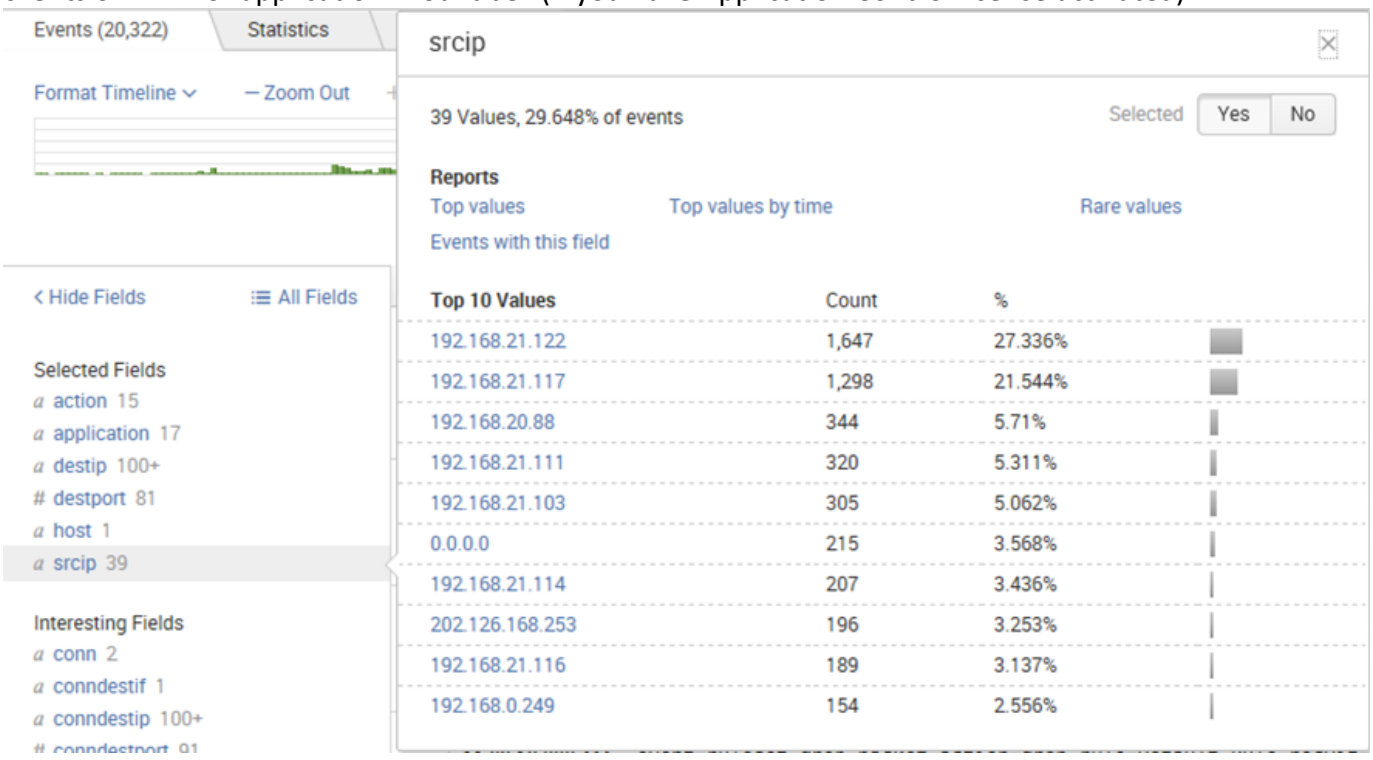
Splunk server will start collecting logs from your firewall and continuously analyse them, identifying “Interesting Fields” like destination IP, source IP, firewall action, type of application or web site being opened.



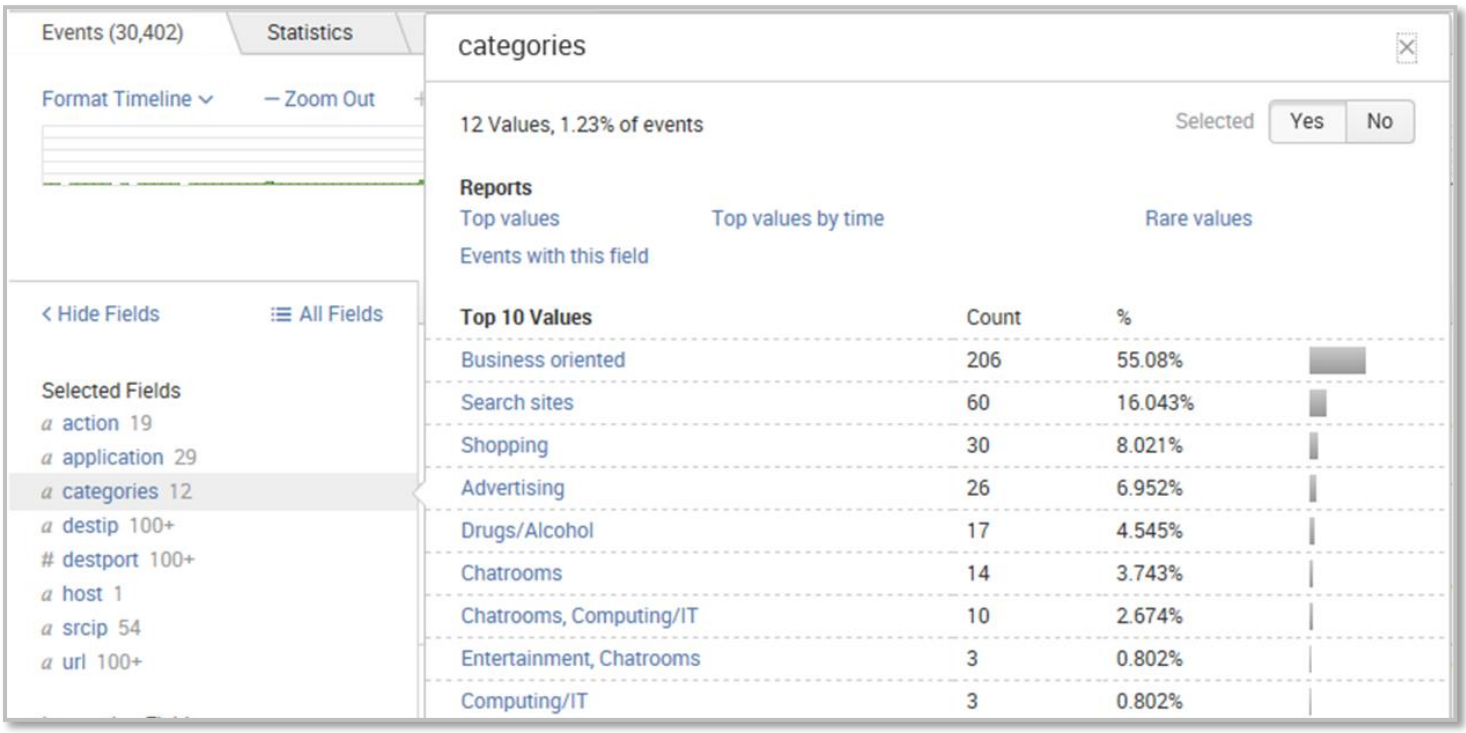
For each of the fields you can check the number of hits, top 10 values, etc.



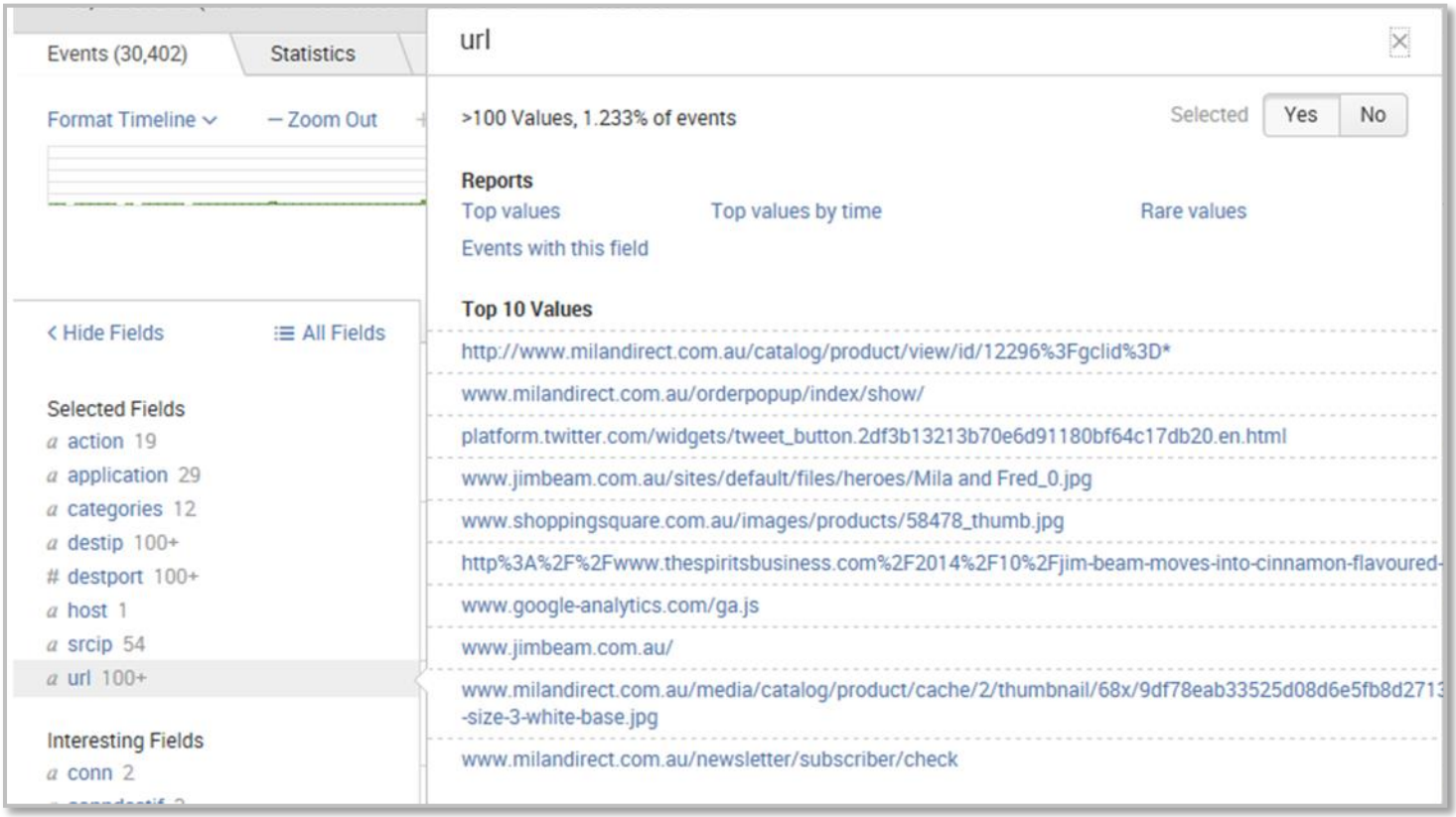
By clicking on each value you can then drill down to top source IPs, destination IPs and so on. E.g. top 10 clients on LAN for application “YouTube” (if you have Application Control license activated):



If your firewall has Web Content Filtering license you will be able to see web browsing categories:



The URLs are also logged:



Splunk allows you to create customizable dashboards and reports. You can view your firewall activity live or analyse the data logged earlier. The free version of Slunk has limitation on the size of the logs you can keep (500MB), old data is purged automatically.