

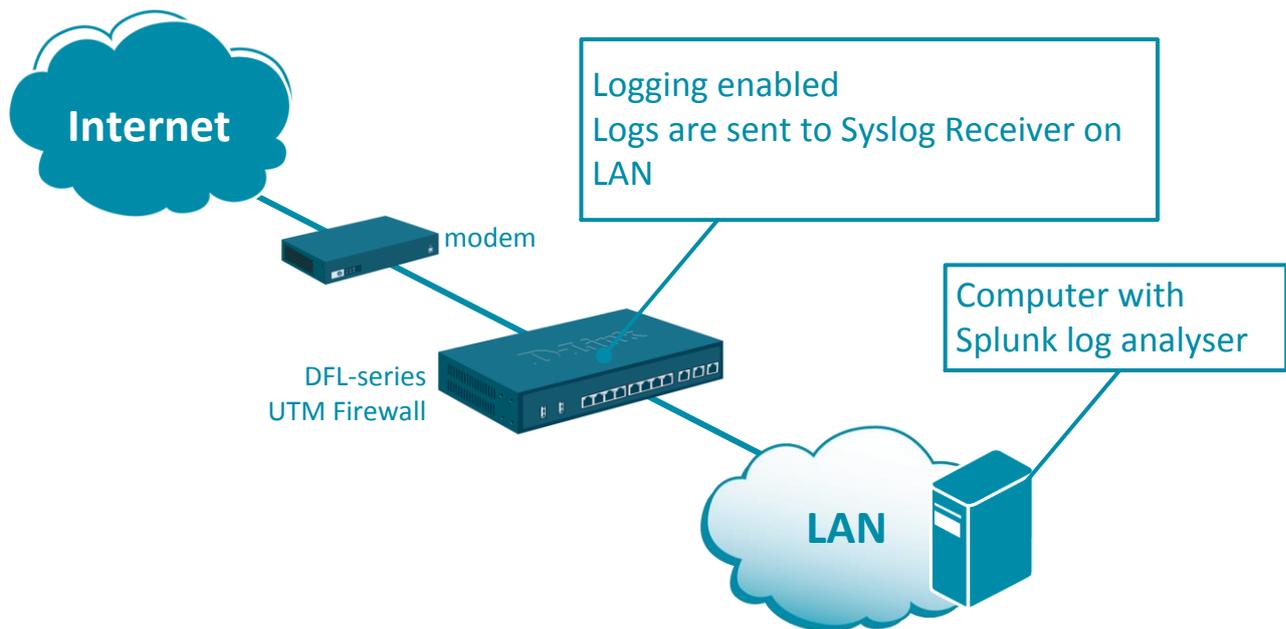
# **NETDEFEND**

## Configuration examples for the D-Link NetDefend Firewall series



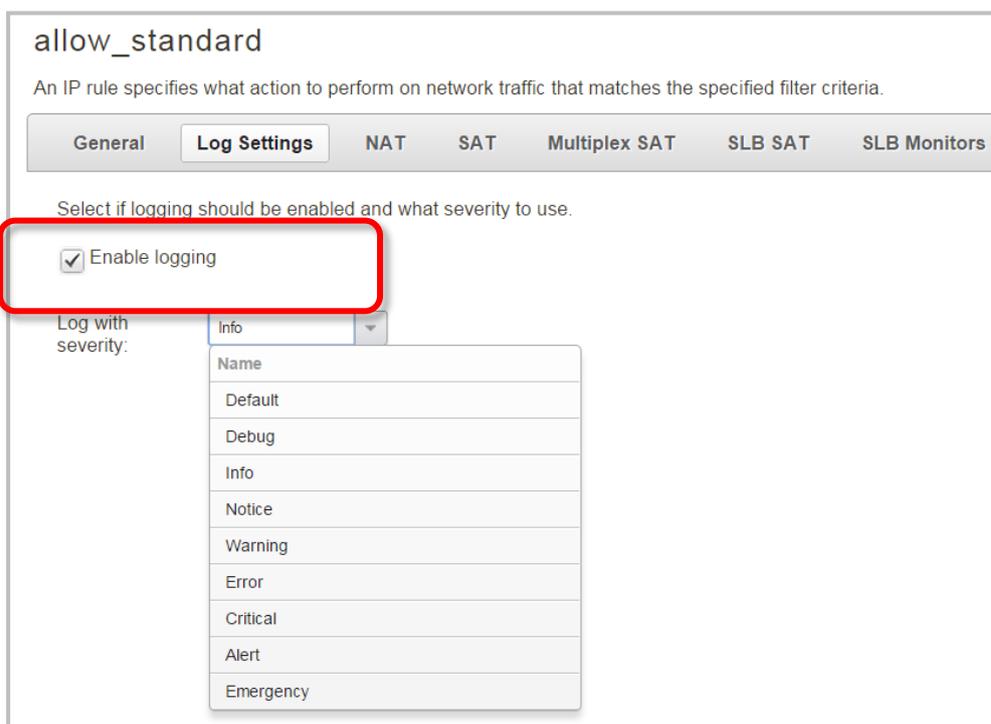
### Setting up logging and reporting

This configuration example is based on the following setup:

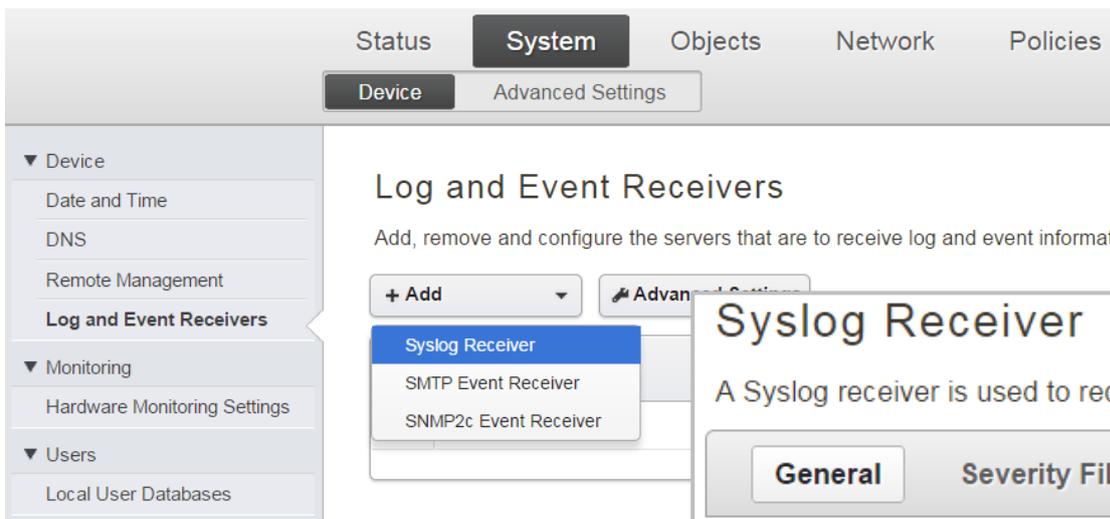


**Step 1.** Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is “admin” and password is “admin”. Set your firewall’s WAN settings as per Internet provider requirements.

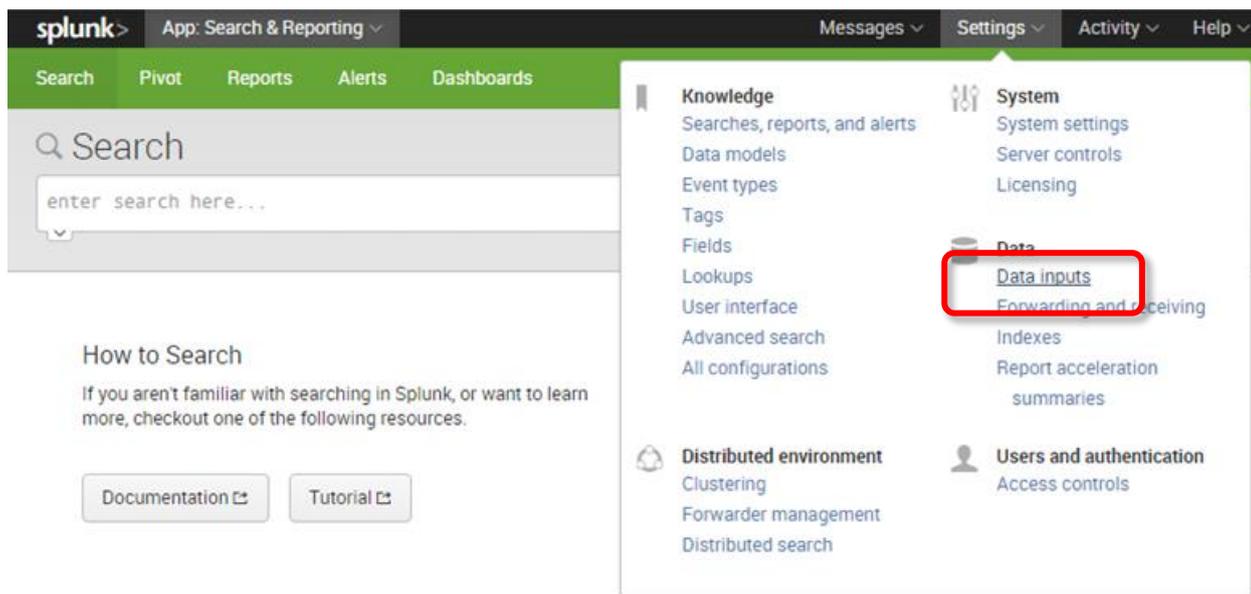
**Step 2.** Enable logging for the desired IP rules. For monitoring outgoing traffic it is important to enable logging in the main NAT rule: Go to Policies > Main IP Rules > lan\_to\_wan > edit the “allow\_standard” rule. Select “Enable logging”.



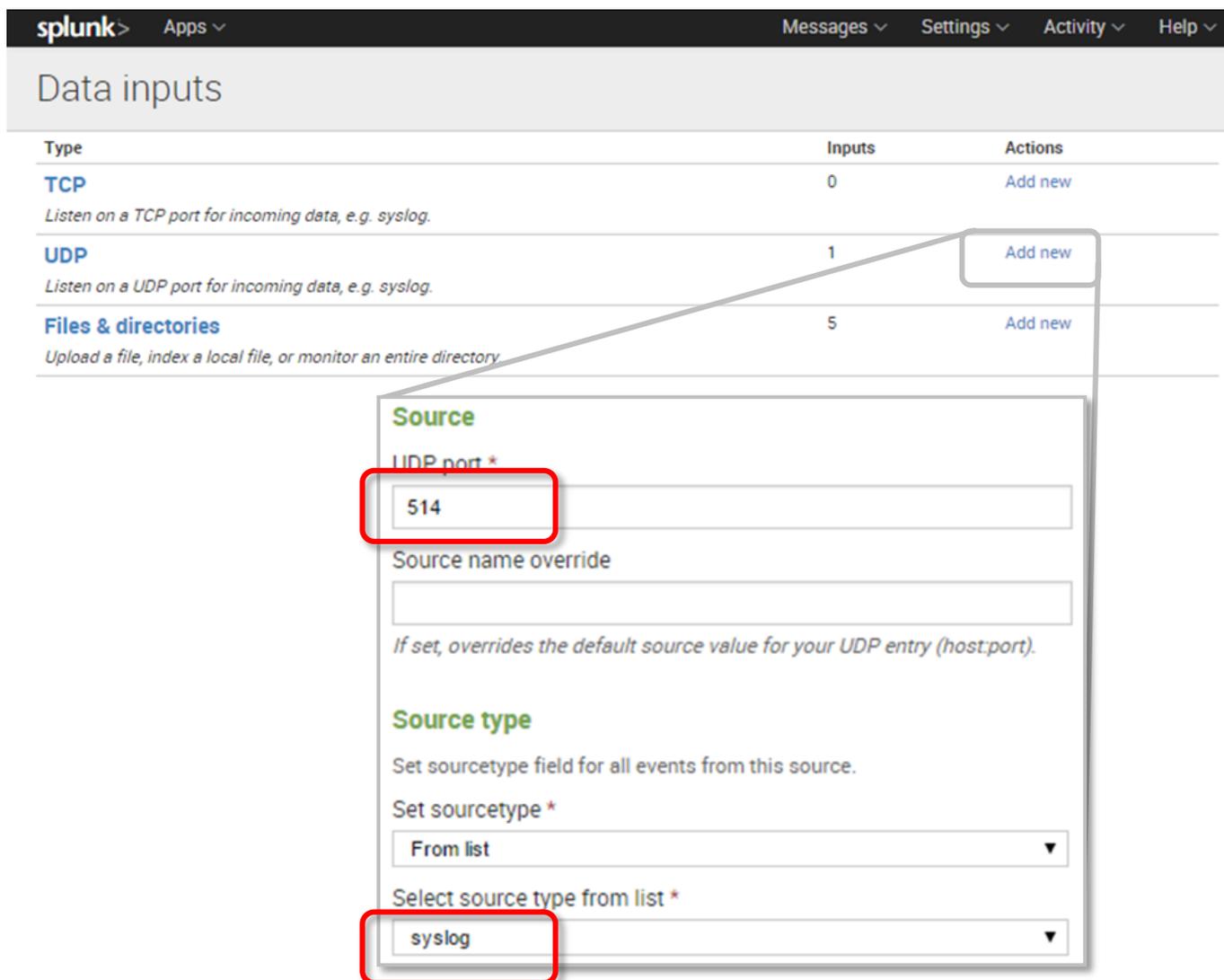
**Step 3.** Go to Objects > Address Book. Add new IP4 address entry – specify your Syslog/Reporting server IP. Go to System > Device > Log and Event Receivers. Add a new Syslog Receiver which points to your server IP address. Click on Severity Filter tab. Specify the event that you want to be logged.



**Step 4.** Download Splunk Enterprise from [www.splunk.com](http://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.

The screenshot shows the Splunk Search & Reporting interface. At the top, there's a navigation bar with 'splunk>' and 'App: Search & Reporting'. Below that, a search bar contains the query 'host="192.168.21.1"'. The results show 20,322 events from 10/10/14 7:00:00.000 AM to 10/10/14 11:00:00.000 AM. A visualization shows a bar chart of events over time. Below the chart, there's a table of results with columns for 'i', 'Time', and 'Event'. On the left sidebar, there's a 'Selected Fields' section and an 'Interesting Fields' section, which is highlighted with a red box. The 'Interesting Fields' section lists:

- a conn 2
- a conndestif 1
- a conndestport 100+
- # conndestport 91

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

Events (30,021) | Statistics | Visualization

Format Timeline | Zoom Out

application

17 Values, 3.504% of events | Selected Yes No

Reports

Top values | Top values by time | Rare values

Events with this field

Top 10 Values	Count	%
http	489	46.483%
steam	175	16.635%
tcp	74	7.034%
google	73	6.939%
yahoo_groups	64	6.084%
dns	46	4.373%
yahoo	28	2.662%
youtube	28	2.662%
akamai	18	1.711%
gstatic	16	1.521%

Selected Fields: a action 15, a application 17, a destip 100+, # destport 94, a host 1, a srcip 54

Interesting Fields: a conn 2, a conndestif 1, a conndestip 100+, # conndestport 100, a connipproto 2, a connnewdestip 100+, # connnewdestport 100, a connnewscrip 1

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):

Events (20,322) | Statistics

Format Timeline | Zoom Out

srcip

39 Values, 29.648% of events | Selected Yes No

Reports

Top values | Top values by time | Rare values

Events with this field

Top 10 Values	Count	%
192.168.21.122	1,647	27.336%
192.168.21.117	1,298	21.544%
192.168.20.88	344	5.71%
192.168.21.111	320	5.311%
192.168.21.103	305	5.062%
0.0.0.0	215	3.568%
192.168.21.114	207	3.436%
202.126.168.253	196	3.253%
192.168.21.116	189	3.137%
192.168.0.249	154	2.556%

Selected Fields: a action 15, a application 17, a destip 100+, # destport 81, a host 1, a srcip 39

Interesting Fields: a conn 2, a conndestif 1, a conndestip 100+, # conndestport 91

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

Events (30,402) Statistics

Format Timeline  - Zoom Out

< Hide Fields  All Fields

Selected Fields

- a action 19
- a application 29
- a categories 12**
- a destip 100+
- # destport 100+
- a host 1
- a srcip 54
- a url 100+

Interesting Fields

- a conn 2

categories

12 Values, 1.23% of events Selected  Yes  No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
Business oriented	206	55.08%
Search sites	60	16.043%
Shopping	30	8.021%
Advertising	26	6.952%
Drugs/Alcohol	17	4.545%
Chatrooms	14	3.743%
Chatrooms, Computing/IT	10	2.674%
Entertainment, Chatrooms	3	0.802%
Computing/IT	3	0.802%

The URLs are also logged:

Events (30,402) Statistics

Format Timeline  - Zoom Out

< Hide Fields  All Fields

Selected Fields

- a action 19
- a application 29
- a categories 12
- a destip 100+
- # destport 100+
- a host 1
- a srcip 54
- a url 100+**

Interesting Fields

- a conn 2

url

>100 Values, 1.233% of events Selected  Yes  No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values

- [http://www.milandirect.com.au/catalog/product/view/id/12296%3Fgclid%3D\\*](http://www.milandirect.com.au/catalog/product/view/id/12296%3Fgclid%3D*)
- [www.milandirect.com.au/orderpopup/index/show/](http://www.milandirect.com.au/orderpopup/index/show/)
- [platform.twitter.com/widgets/tweet\\_button.2df3b13213b70e6d91180bf64c17db20.en.html](https://platform.twitter.com/widgets/tweet_button.2df3b13213b70e6d91180bf64c17db20.en.html)
- [www.jimbeam.com.au/sites/default/files/heroes/Mila and Fred\\_0.jpg](http://www.jimbeam.com.au/sites/default/files/heroes/Mila and Fred_0.jpg)
- [www.shoppingsquare.com.au/images/products/58478\\_thumb.jpg](http://www.shoppingsquare.com.au/images/products/58478_thumb.jpg)
- [http%3A%2F%2Fwww.thespiritsbusiness.com%2F2014%2F10%2Fjim-beam-moves-into-cinnamon-flavored-](http://www.thespiritsbusiness.com/2014/10/27/jim-beam-moves-into-cinnamon-flavored/)
- [www.google-analytics.com/ga.js](http://www.google-analytics.com/ga.js)
- [www.jimbeam.com.au/](http://www.jimbeam.com.au/)
- [www.milandirect.com.au/media/catalog/product/cache/2/thumbnail/68x/9df78eab33525d08d6e5fb8d2713-size-3-white-base.jpg](http://www.milandirect.com.au/media/catalog/product/cache/2/thumbnail/68x/9df78eab33525d08d6e5fb8d2713-size-3-white-base.jpg)
- [www.milandirect.com.au/newsletter/subscriber/check](http://www.milandirect.com.au/newsletter/subscriber/check)

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 Splunk has limitation on the size of the logs you can keep (500MB), old data is purged automatically.

