# Configuration examples for the D-Link NetDefend Firewall series

# DFL-210/800/1600/2500

## Scenario: How to configure IDP/IPS rule

Last update: 2007-01-31

---

### Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

The screenshots in this document is from firmware version 2.11.02. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

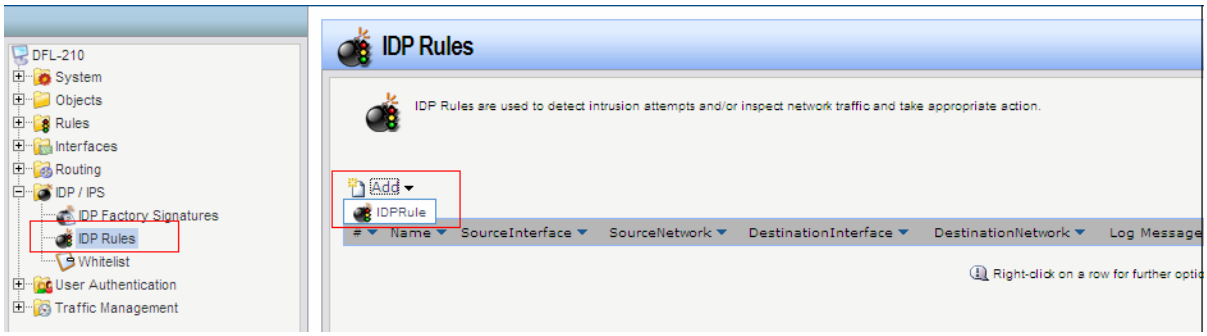
# How to configure IPS/IDP rule

The D-Link IPS Signature Service provides you with access to all the latest D-Link IPS Signatures, including the highly unique component based signatures.
The signatures are provided automatically to your D-Link DFL 210/800/1600/2500 Firewall through the D-Link NetDefend IPS Update Service which ensures the highest level of security and speed of delivery.

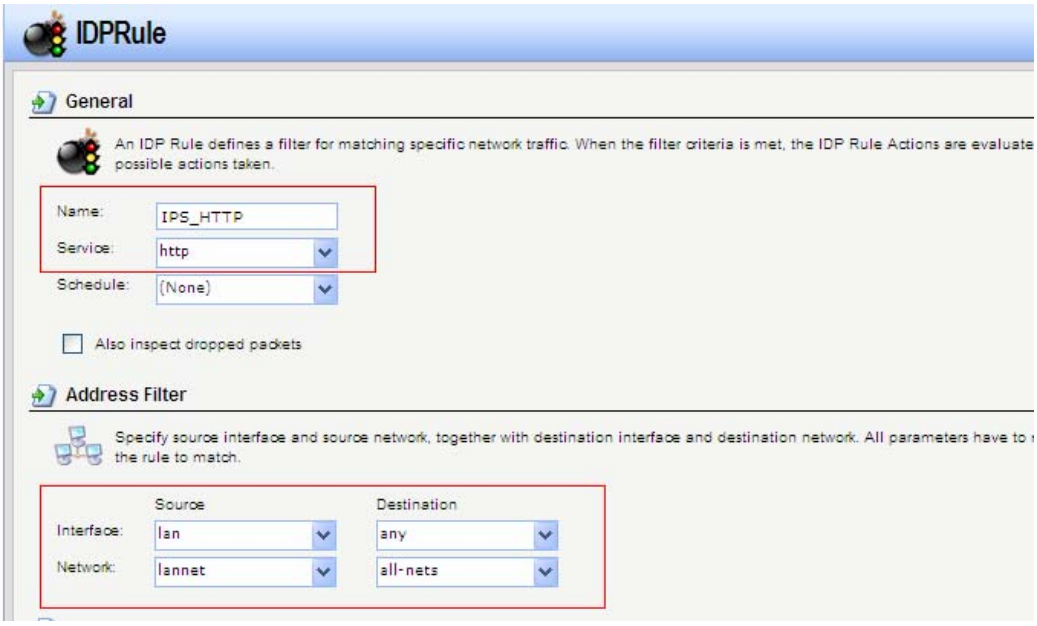
We would like to provide a configuration example to guide you for fine tuning your IPS rule of D-Link DFL-210/800/1600/2500 Firewall, you as an administrator can more easily configure a proper IPS signature usage. D-Link the latest IPS signature update is in a more fine-granular way which prompts for lower false-positives and a better overall performance.

Scenario: Configure all HTTP signatures for HTTP service (port 80) from LAN net to all net.

Step1: Create a IDP Rule

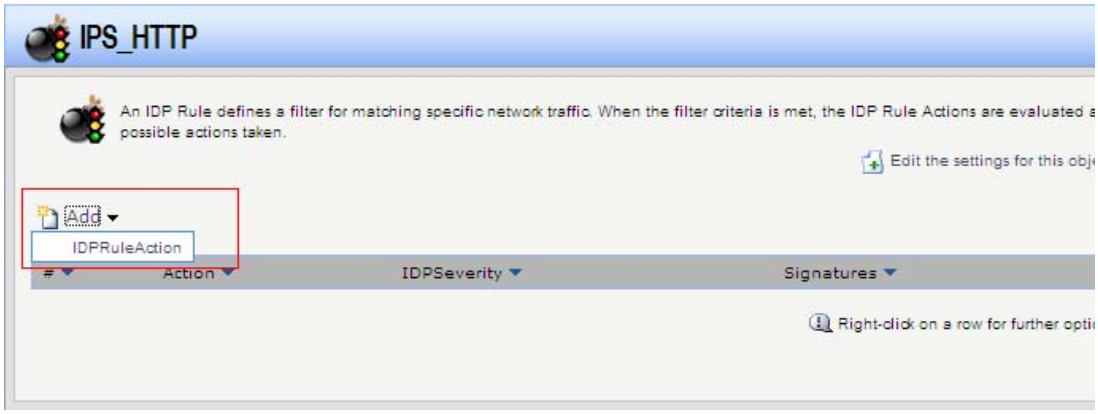



Step2: Specify Service, Source and Destination



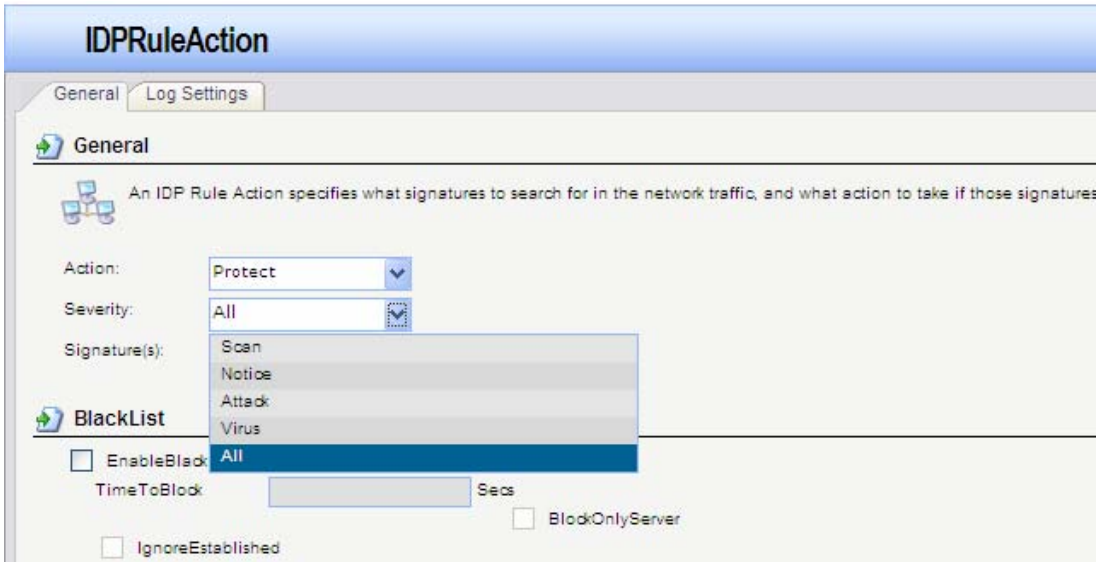

<Note> Based on our scenario, if we choose *http* in *Service* filed, which means this IDPRule ONLY monitor http traffic, any other traffic type will bypass this rule. You have to create another IDPRule for other services if you want to protect or monitor it.

Step3: Create IDPRuleAction

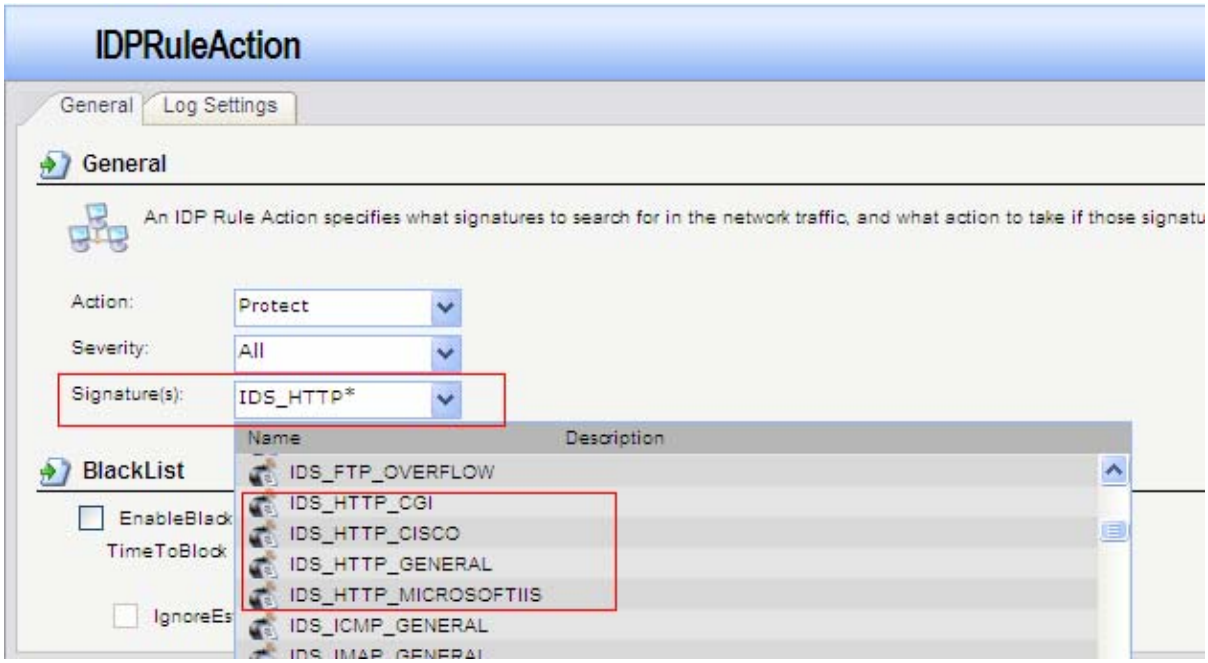



Step4: Select Protect that means “Drop connection”, Audit means “Allow all connect and log” only, or Ignore means “ Do Nothing”.


Step5: There are four Severity Scan, Notice, Attack and Virus, administrator can select one of them or all to specify this IDPRule's severity, Recommend selecting ":All" for fully protecting your network

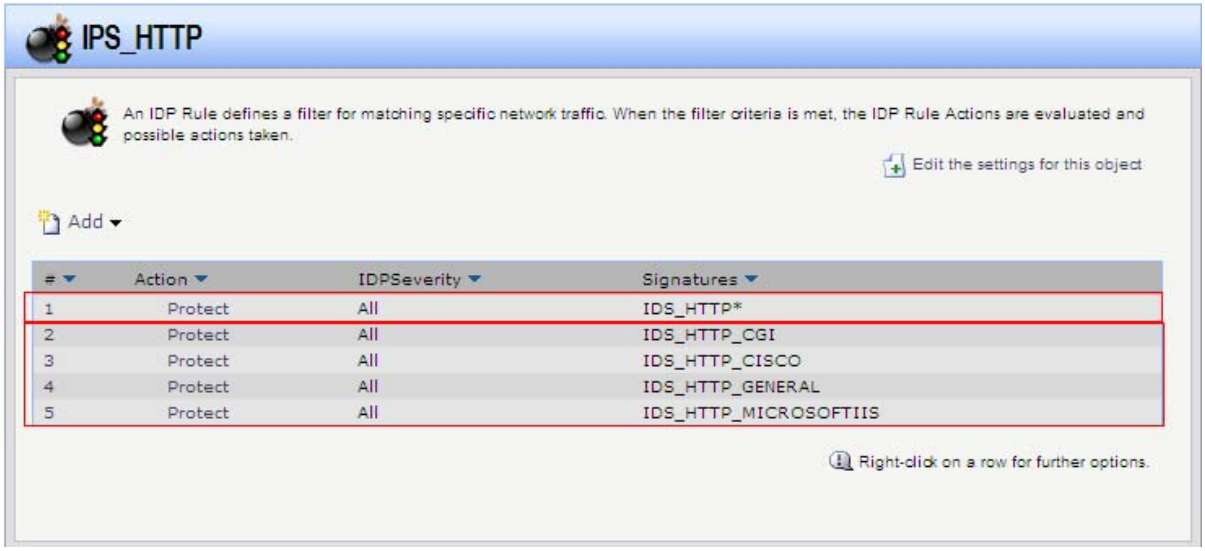



Step6: Select signature which you want to use it to protect your network, you can manual type IDS_HTTP* which includes IDS_HTTP_CGU, IDS_HTTP_CISCO, IDS_HTTP_GENERAL and IDS_HTTP_MICROSOFTIIS.

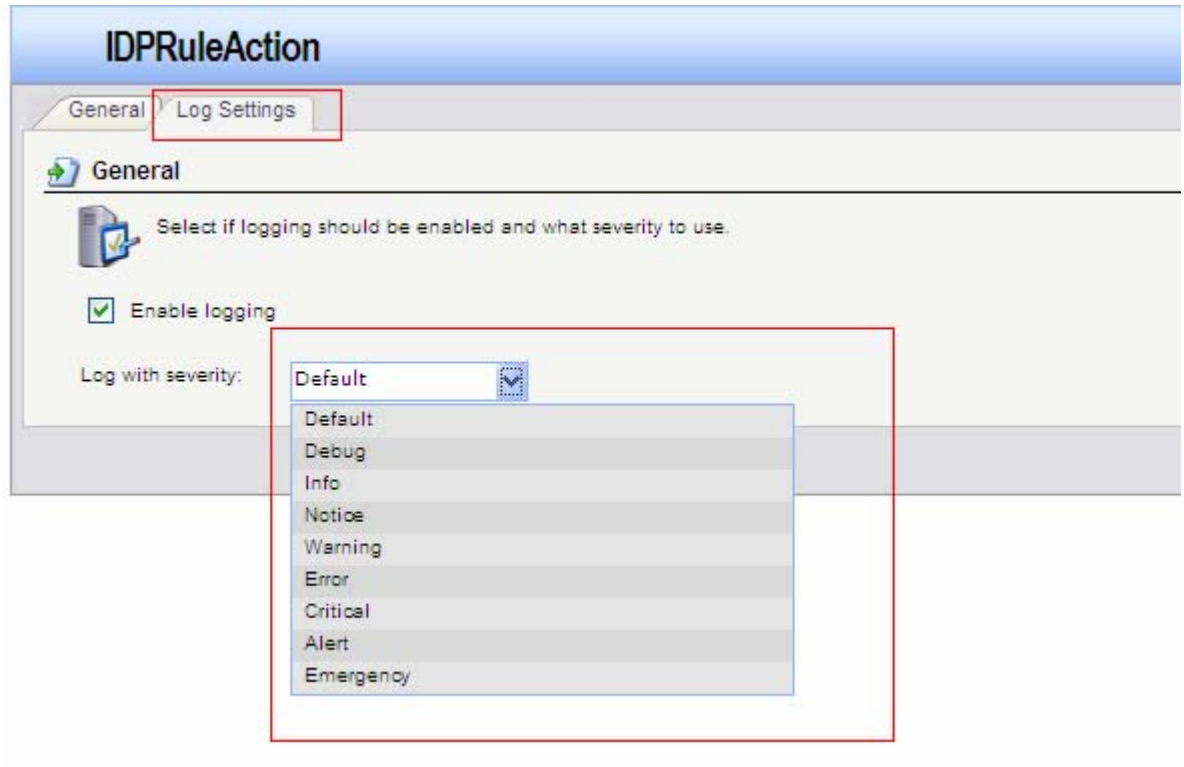



"*" means include all, for example, IDS_HTTP* is including all IDS_HTTP signature, IDS* is including all IDS signature, if you use ** that will include all signatures.

You can either create four IDPRuleAction, as below rule number 2 to number 5, or you can use rule number 1 instead of rule number 2 to number 5




Step7: Click "Log Settings" check "Enable logging" to receive IPS log, there are nine severities for IPS log, and you can select one of them to specify what the severity of this IPS log is. All IPS log will be shown on logging of Status in the mean bar of firewall Web UI.




! Reminder:

For avoiding False-Positive and False-Negative, administrator has to consider what kind of service or signature should be specified “Protect”, which kind of service or signature should be specified “Audit” or “Ignored”, for example, administrator selects all IDP signature for all service and the action is “Protect” in IDPRule, it may block some normal traffic as ping or scan, administrator can refer the detail description of IDP Factory Signature from firewall web UI or IPS advisory on NetDefend Center (http://security.dlink.com.tw) to help you set IDP rule correctly.