Configuration examples for the D-Link NetDefend Firewall series

DFL-210/800/1600/2500

Scenario: ZoneDefense for D-Link switch model DES-3226S

Last update: 2005-10-20

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**.

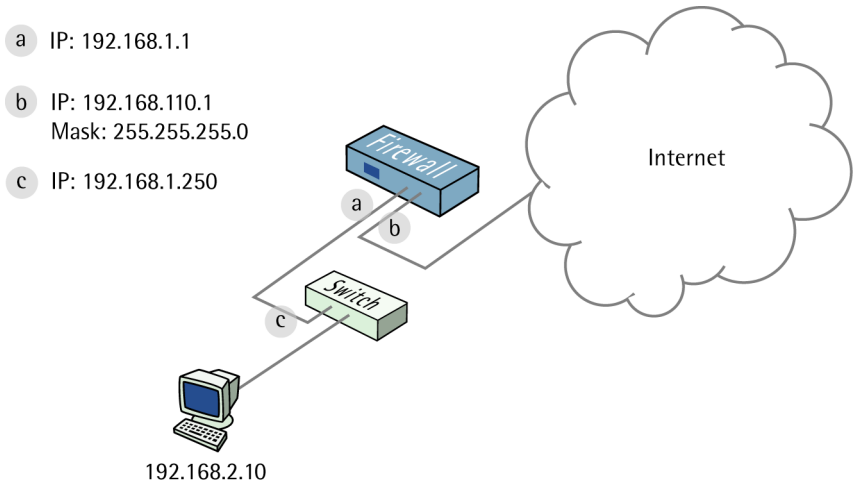
Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and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

The screenshots in this document is from firmware version 2.04.00. If you are using a later version of the firmware, the screenshots may not be identical to what you see on your browser.

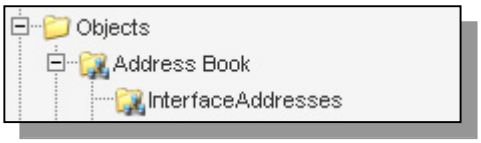
To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

8 ZoneDefense for D-Link switch model DES-3226S

This example will show how to configure the firewall to use ZoneDefense.
Details:
The local network contains a D-Link DES-3226S switch. This example shows how to define a **Microsoft-DS Threshold** (TCP port 445) of 10 connections/second (eg, the work SASSER.A will send out a large amount of TCP SYN on port 445). If the number of connections exceeds this limitation, the firewall will block the specific hosts port on the switch (host 192.168.2.10 in this scenario). The switch port connected to the firewall should be configured to use 192.168.1.250 and the community string MyCompany.



1. Addresses



Go to *Objects -> Address book -> InterfaceAddresses*.
Edit the following items:
Change **lan_ip** to **192.168.1.1**
Change **lannet** to **192.168.1.0/24**

Change **wan1_ip** to **192.168.110.1**
Change **wan1net** to **192.168.110.0/24**

Go to *Objects -> Address book*.

Add a new Address Folder called **LocalHosts**.

In the new folder, add a new IP4 Host/Network:
Name: **DES-3226S**
IP Address: **192.168.1.250**

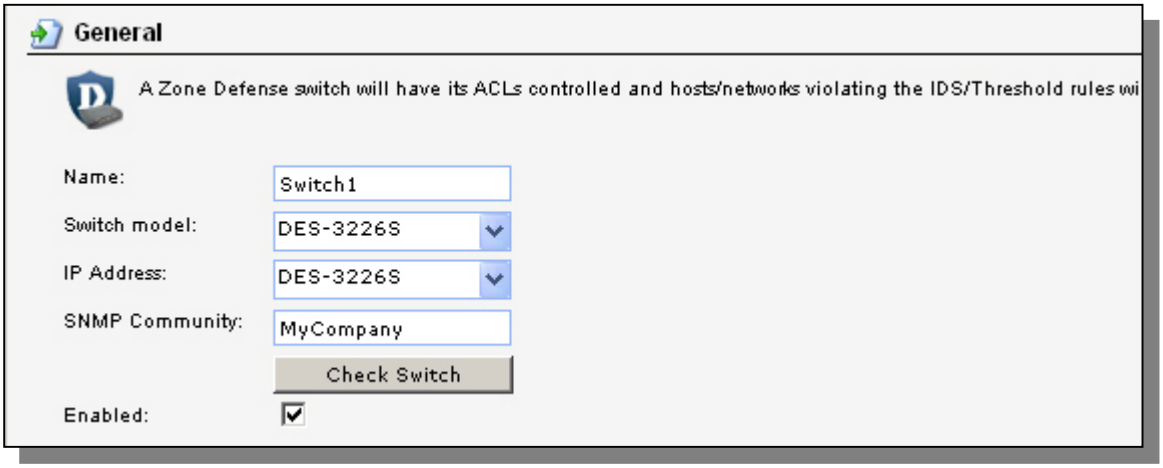
Click Ok

2. Switch set up

Go to *Zone Defence -> Switches*.

Add a new Switch:

General:



Name: **Switch1**
Switch Model: **DES-3226S**
IP Address: **DES-3226S** (this is the IP of the port on the switch that is connected to the firewall)
SNMP Community: **MyCompany**
Check the **Enabled** box

Clicking Check Switch can check the settings and connectivity.

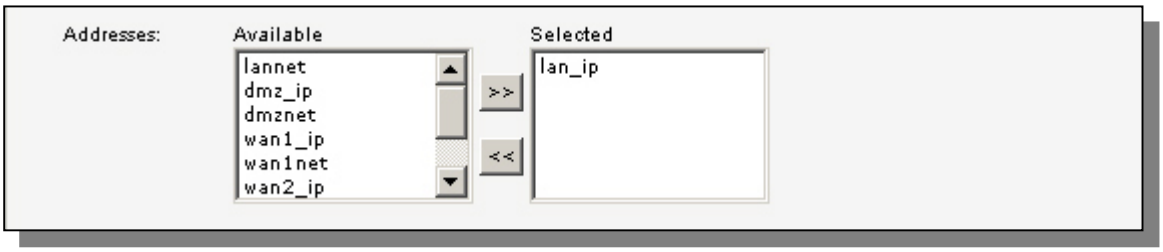
Click Ok.

3. Exclude list

To prevent the firewall from accidentally being locked out from accessing the switch, add the firewall's interface for managing the switch into the exclude list.

Go to *Zone Defense -> Exclude*.

General:



Select **`lan_ip`** and add it to the selected list.

Click Ok.

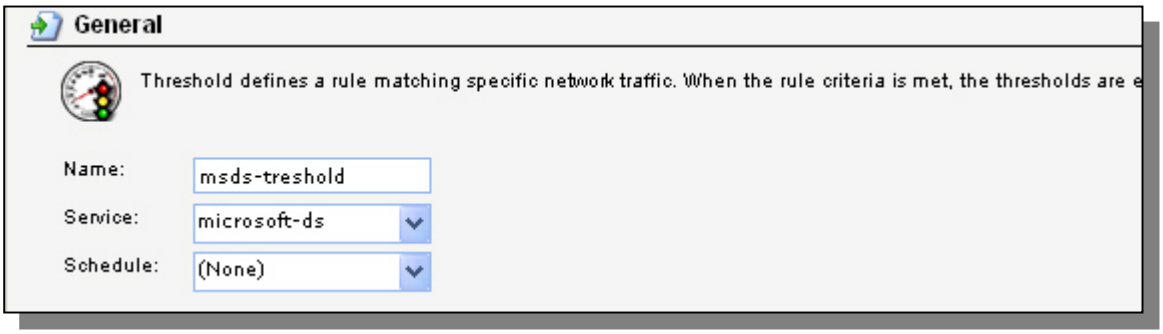
4. Threshold rules

Go to *Zone Defense -> Threshold*.

Add a new Threshold.

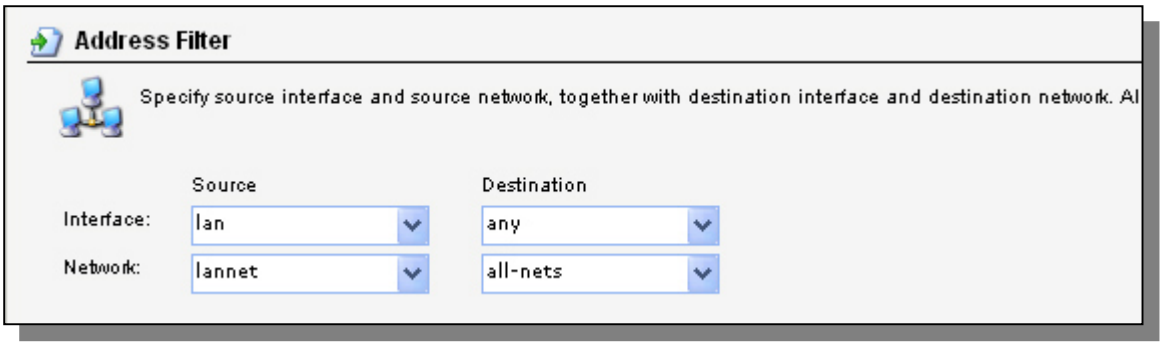
In the General tab:

General:



Name: **`msds-threshold`**
Service: **`microsoft-ds`**
Schedule: **`(None)`**

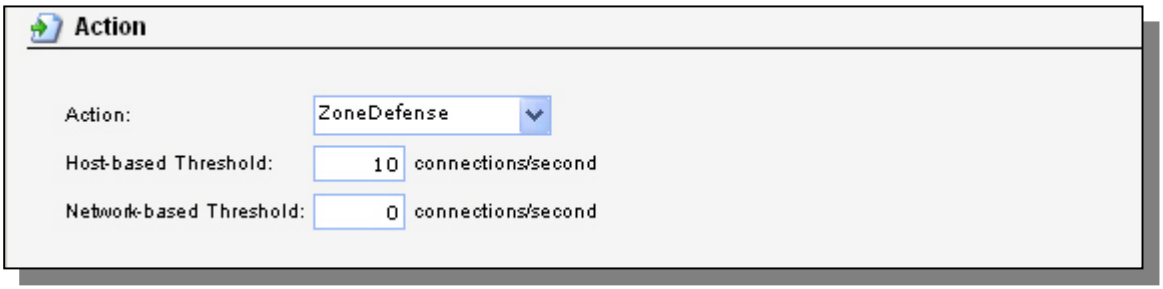
Address Filter:



Source interface: **lan**
Source network: **lannet**
Destination interface: **any**
Destination network: **all-nets**

In the Action tab:

Action:



Action: **ZoneDefense**
Host-based Threshold: **10**
Network-based Threshold: **0**

Click Ok.

Save and activate the configuration.