Configuration examples for the D-Link NetDefend Firewall series

Scenario: How to configure ZoneDefense – Triggered by IPS/IDP Signature Database

Platform Compatibility: DFL-800/860/1600/2500

Last update: 2008-03-11

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.

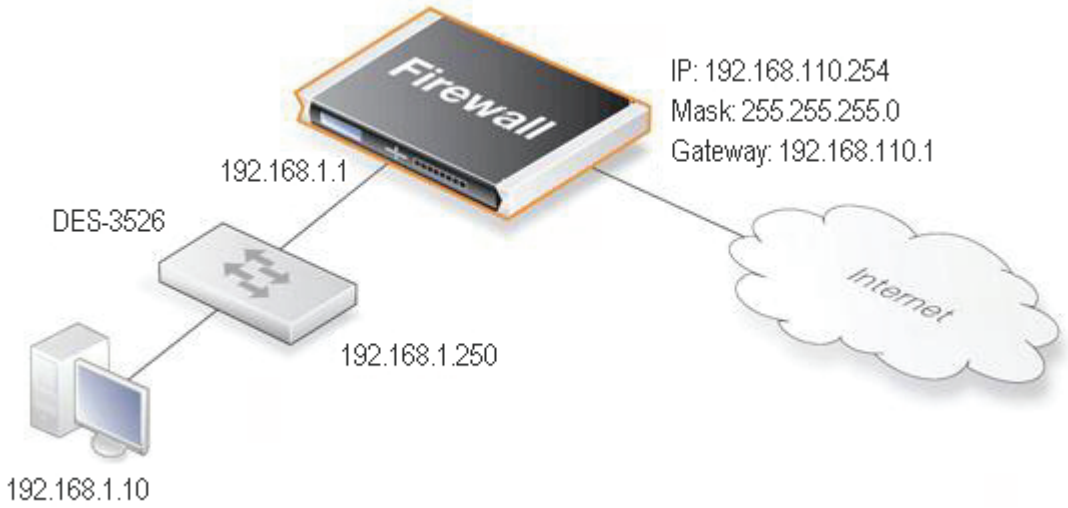
The screenshots in this document is from firmware version 2.12.00. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

How to configure ZoneDefense to be triggered by IDP signature database

This scenario is about End-Point security with D-Link ZoneDefense technology which integrate D-Link xStack switch. The firewall will be based on built-in IDP signature to detect abnormal traffic from LAN to WAN. Once firewalls detect malicious traffic, D-Link xStack switch device could quarantine these infected PCs.

Detail for this scenario:

- Basically, more and more network threat comes from internal network of company by HTTP protocol, especially for mobile users/employees. Therefore, IT manager intends to focus in **HTTP Protocol** to detect traffic from LAN to WAN.
- The signature database is based on **IDP maintenance service**.
- There is one D-Link **DES-3526** switch in LAN environment.



Prerequisites:

- Make sure that the switches have the minimum required firmware versions before activating ZoneDefense feature.
- The information needed in order to control a switch includes:
  - The IP address of the management interface of the switch
  - The switch model type
  - The SNMP community string (write access)
  - Make sure the SNMP feature of switch is enabled (Some switch SNMP is disabled by default)
- It's strongly recommended that the administrator clear the entire ACL rule-set on the switch before processing the ZoneDefense setup.

Note:

- The ZoneDefense feature is **Not available** in the **DFL-210/260** models.
- When NetDefendOS detects that a host or a network has reached the specified conditions, such as network threshold or IDP signature. The D-Link switches will turn block all traffic for the host or network displaying the unusual behavior.
- Blocked hosts and networks remain blocked until the system administrator manually unblocks them using the Web or Command Line interface.

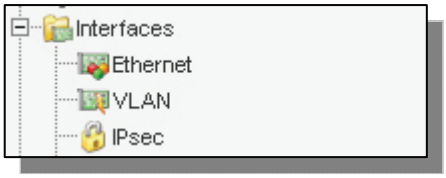
1. Interface address and default gateway.

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**

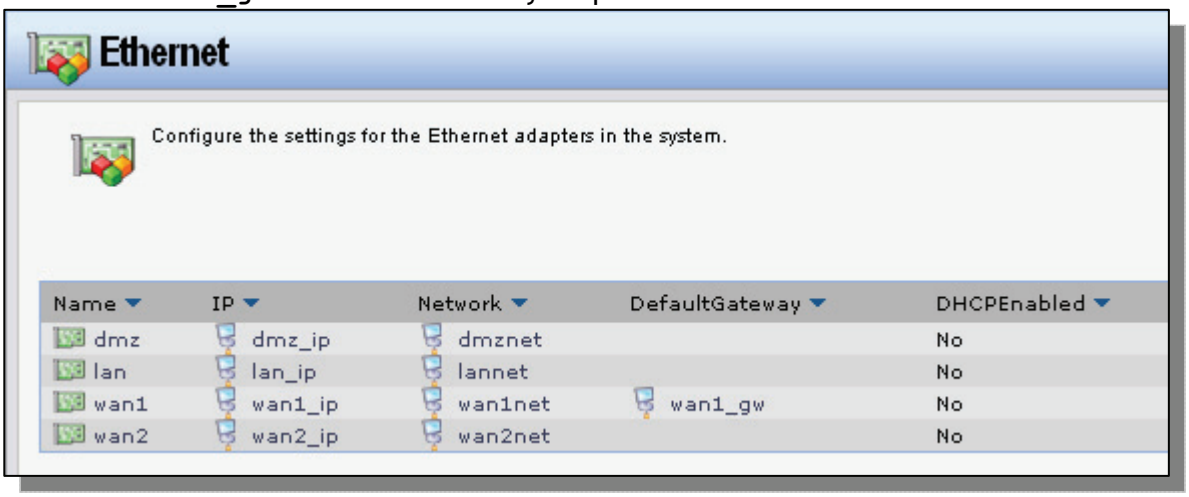
Change **wan1_ip** to **192.168.110.254**
Change **wan1net** to **192.168.110.0/24**
Change **wan1_gw** to **192.168.110.1** (If this object does not exist, create a new one)

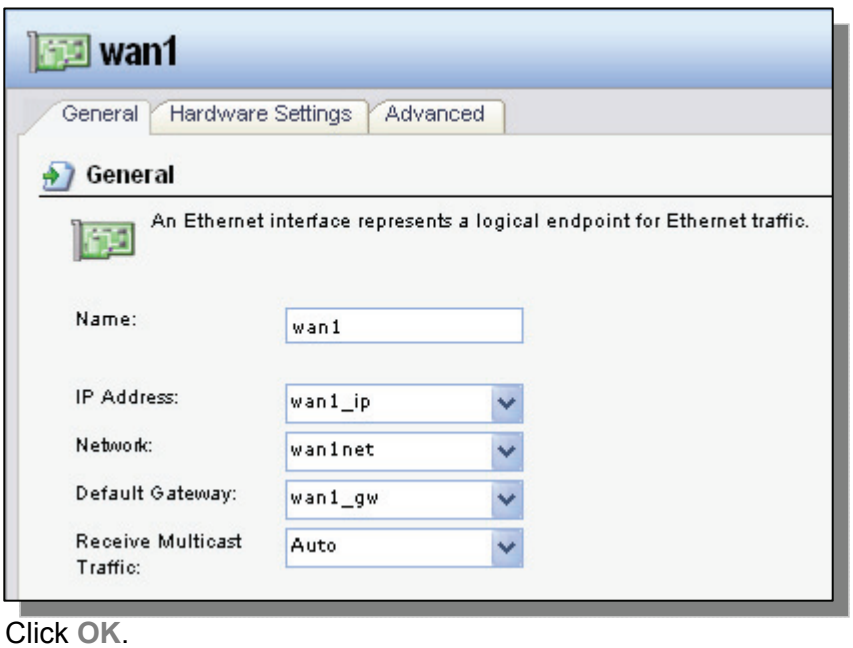
Add new IP Address objects with switch management interface
Name: **IP_DES-3526**
IP Address: **192.168.1.250**



Go to ***Objects ->Interfaces -> Ethernet*:**

Select **wan1** interface
Select the **wan1_gw** on Default Gateway drop-down menu for wan1 interface



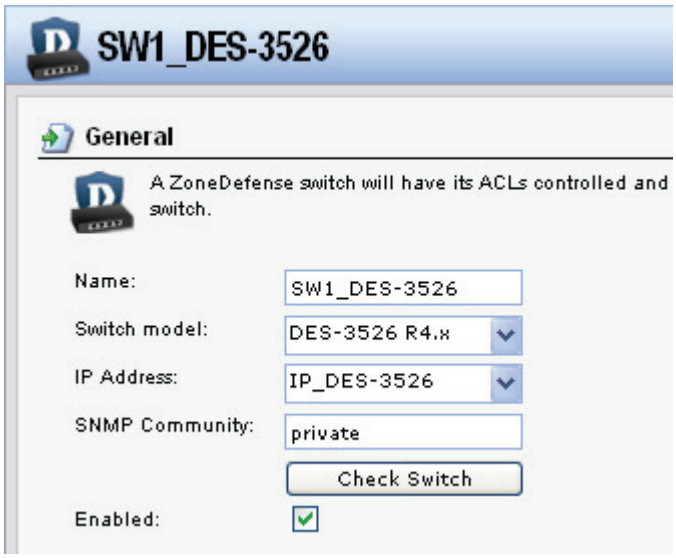


Click **OK**.

2. Switch setup for ZoneDefense feature

Go to ***ZoneDefense -> Switches***

Create one ZoneDefense Switch object:



Name: **SW1_DES-3526**
Switch model: **DES-3526 R4.x (R4.01-B19 or later)**
IP Address: **IP_DES-3526 (This is the IP of the port on the switch that is connected to the firewall)**
SNMP Community: **Private**
Check the Enabled box

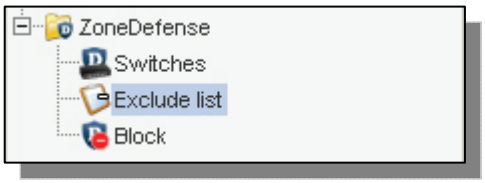
Clicking Check Switch can check the settings and connectivity.

Click OK.

3. Add the Firewall's management interface into exclude list

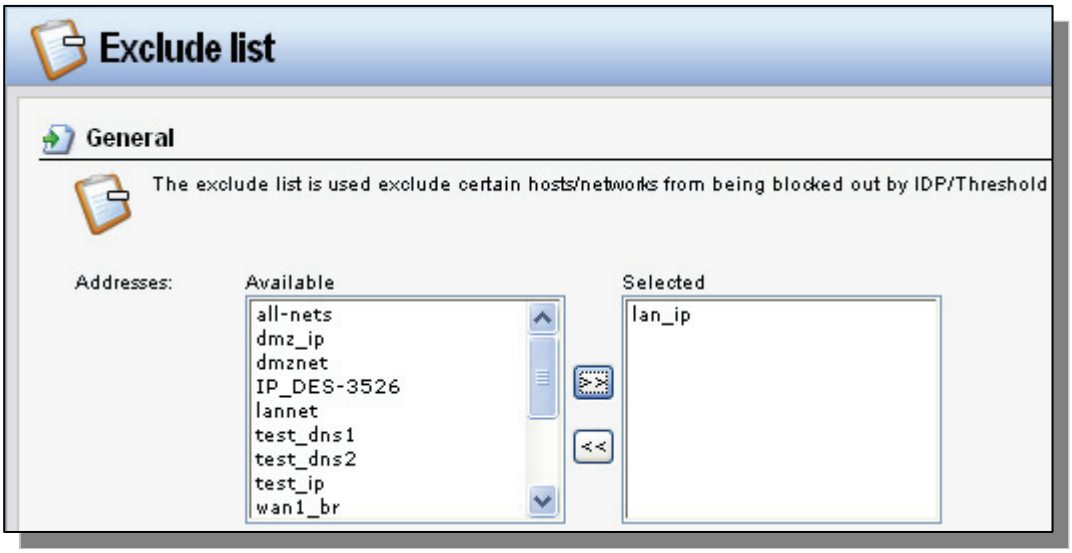
To prevent the firewall from accidentally being locked out from accessing the switch, add the firewall's interface for managing the switch into the exclude list.

Go to ***ZoneDefense -> Exclude list***



In the General tab:

General:



Select Lan_ip and add it to the selected list

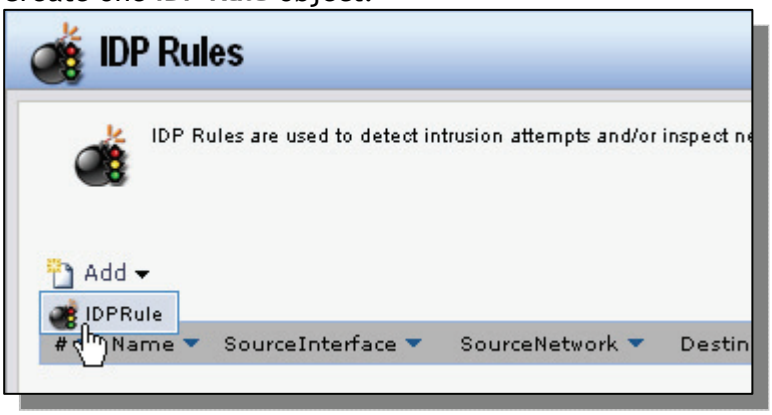
Click **OK**.

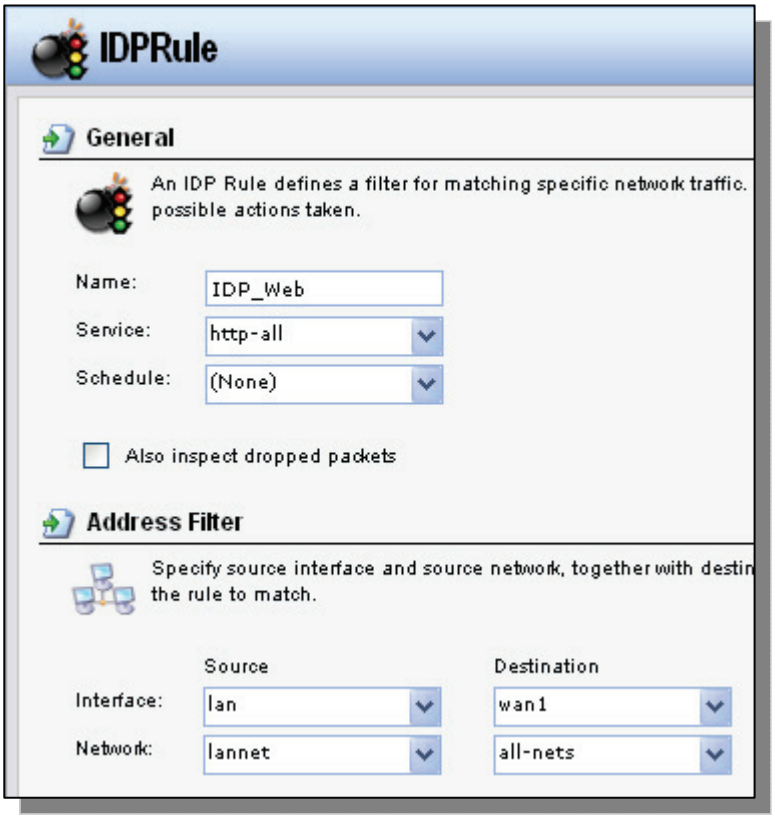
4. Create IDP rule

There are two major steps for IDP setting: first of all will make sure the protocol types and traffic address filter definition of IDP rule. Then assign IDP signature sets you want into IDP rule.

Go to ***IDP/IDS -> IDP Rules***

Create one IDP Rule object:





Name: **IDP_Web**
Service: **http-all**
Schedule: **None**
Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **wan1**
Destination Network: **all-nets**

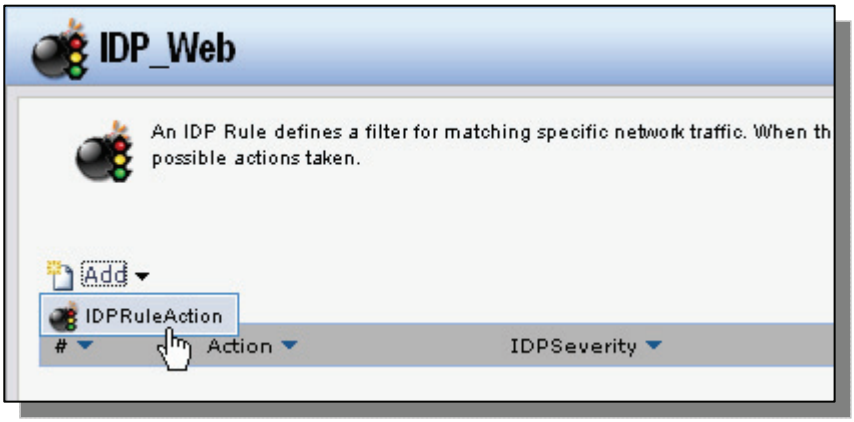
Click OK.

5. Configure IDP Rule Action to use ZoneDefense

After create IDP rule, the system will lead you to create IDP Rule Action as following screenshot.

5-1. Add signature set with WEB_CATTACK into IDP Rule Action

Create one **IDP Rule** object:



IDP database provide several HTTP attack signature set categories; each **IDP Rule Action** only can include one IDP signature set. You have to create several IDP Rule Action to cover more than one IDP signature sets.

In the **General** tab:

General:

Action: **`Protect`**
Severity: **`All`**
Signature(s): **`FROM_EXT_WEB_ATTACKS`**
`Check the Use ZoneDefense box`

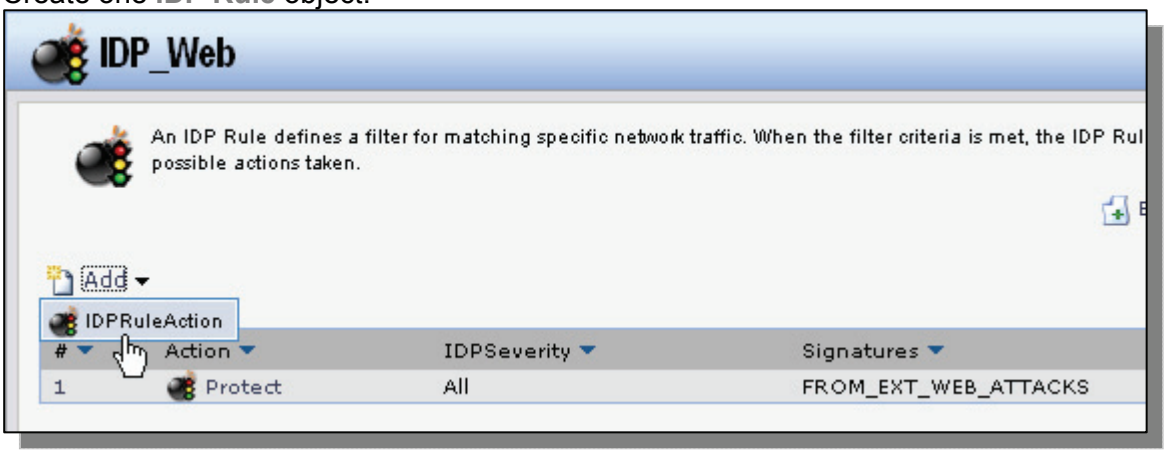
Click **OK**.

Note:
All signature sets could be used for any traffic direction and it depends on IDP rule setting.

5-2. Add signature set with WEB_COLDFUSION into IDP Rule Action

In this step, we will create additional **IDP Rule Action** based on same **IDP Rule** which could includes other IDP signature set to provide more high coverage and accuracy for HTTP type attack.

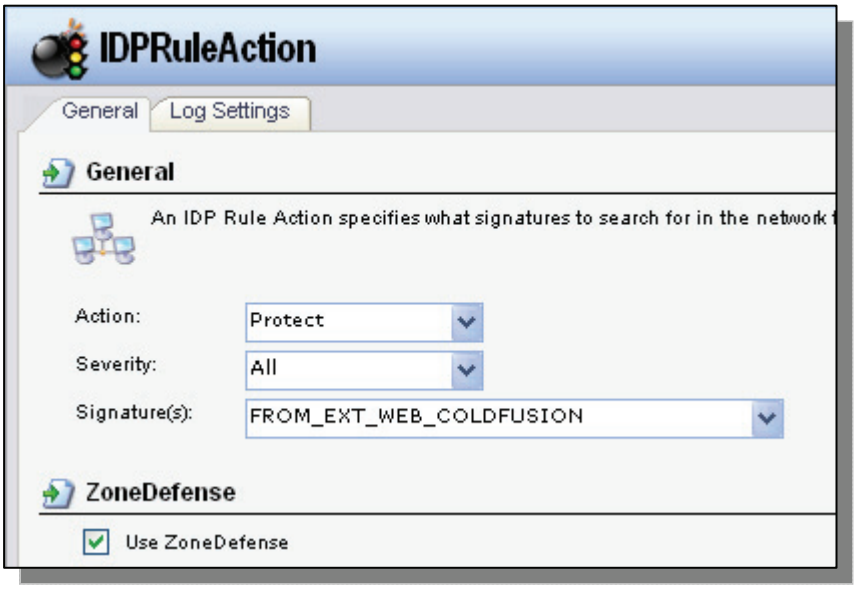
Create one IDP Rule object:



Now, we will add the signature set with **"FROM_EXT_WEB_COLDFUSION"** into IDP Rule Action.

In the General tab:

General:



Action: **Protect**
Severity: **All**
Signature(s): **FROM_EXT_WEB_COLDFUSION**
Check the Use ZoneDefense box

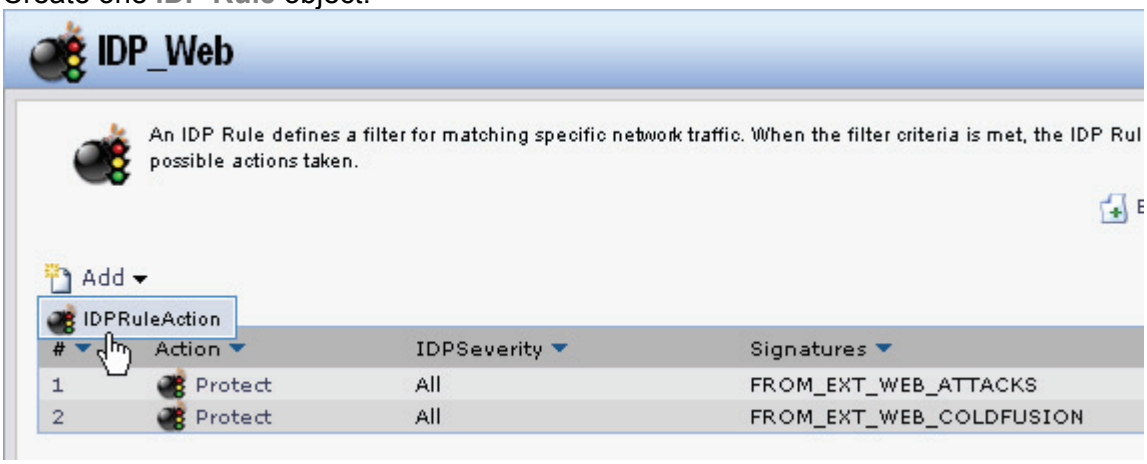
Click OK.

Note:
All signature sets could be used for any traffic direction and it depends on IDP rule setting.

5-3. Add signature set with WEB_FRONTPAGE into IDP Rule Action

In this step, we will create additional **IDP Rule Action** based on same **IDP Rule** which could includes other IDP signature set to provide more high coverage and accuracy for HTTP type attack.

Create one IDP Rule object:



Now, we will add the signature set with **"FROM_EXT_WEB_FRONTPAGE"** into IDP Rule Action.

In the General tab:

General:

Action: **Protect**
Severity: **All**
Signature(s): **FROM_EXT_WEB_FRONTPAGE**
Check the Use ZoneDefense box

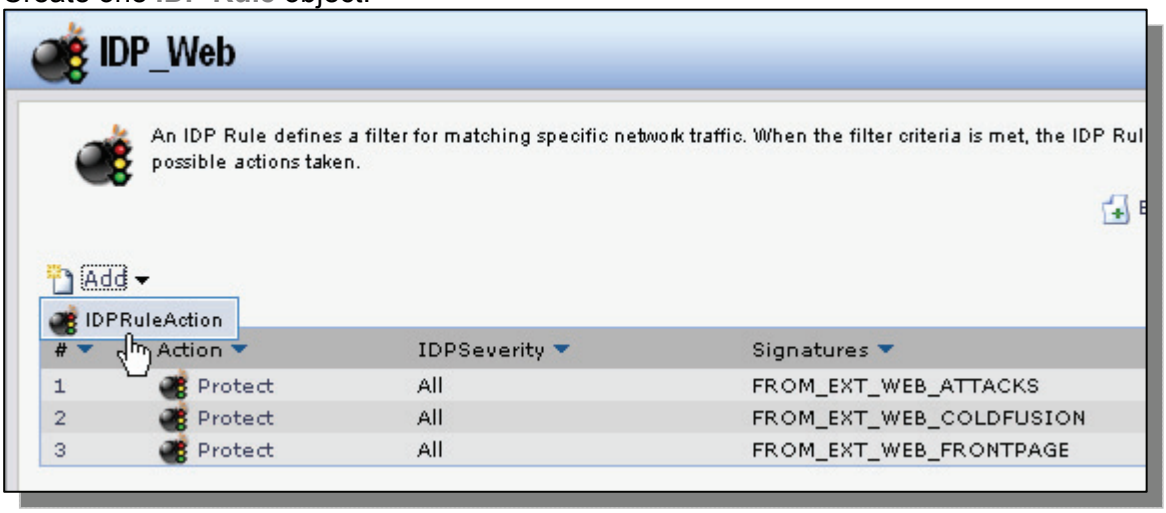
Click OK.

Note:
All signature sets could be used for any traffic direction and it depends on IDP rule setting.

5-4. Add signature set with WEB_IIS into IDP Rule Action

In this step, we will create additional **IDP Rule Action** based on same **IDP Rule** which could includes other IDP signature set to provide more high coverage and accuracy for HTTP type attack.

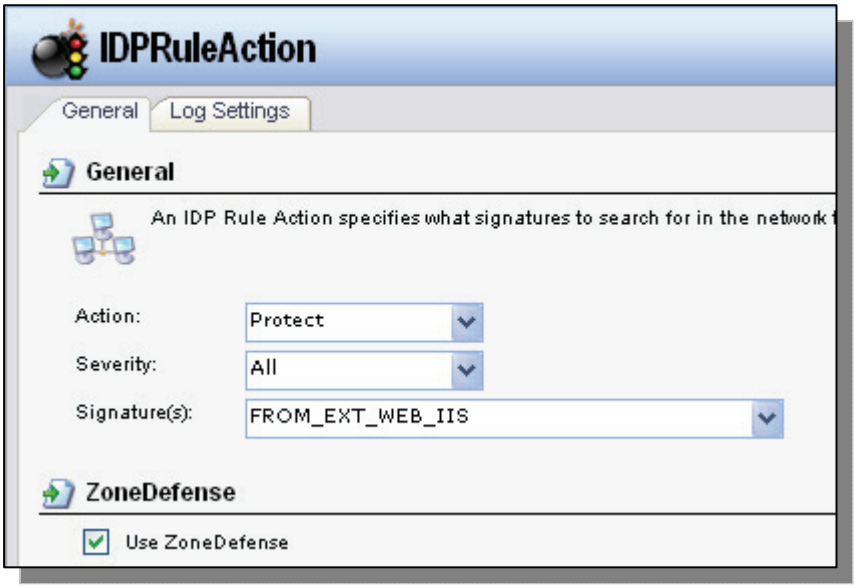
Create one IDP Rule object:



Now, we will add the signature set with **"FROM_EXT_WEB_IIS"** into IDP Rule Action.

In the General tab:

General:



Action: **Protect**
Severity: **All**
Signature(s): **FROM_EXT_WEB_IIS**
Check the Use ZoneDefense box

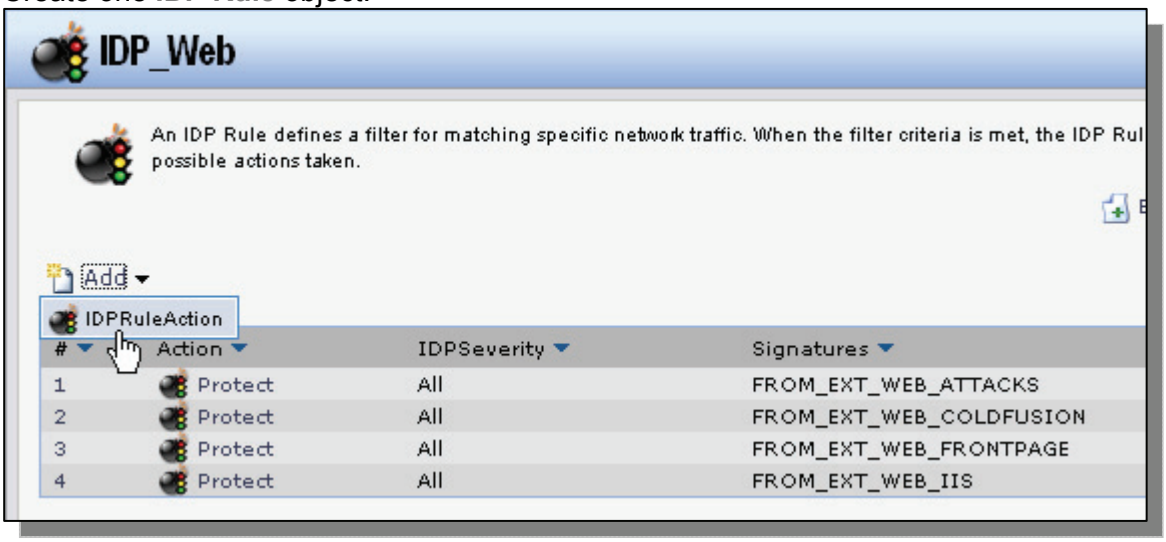
Click OK.

Note:
All signature sets could be used for any traffic direction and it depends on IDP rule setting.

5-5. Add signature set with WEB_MISC into IDP Rule Action

In this step, we will create additional **IDP Rule Action** based on same **IDP Rule** which could includes other IDP signature set to provide more high coverage and accuracy for HTTP type attack.

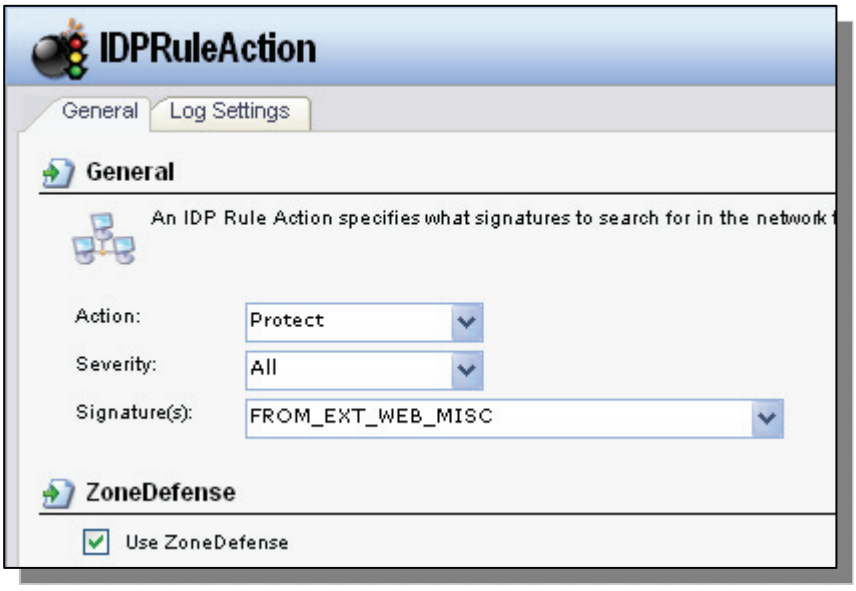
Create one IDP Rule object:



Now, we will add the signature set with **"FROM_EXT_WEB_MISC"** into IDP Rule Action.

In the General tab:

General:



Action: **Protect**
Severity: **All**
Signature(s): **FROM_EXT_WEB_MISC**
Check the Use ZoneDefense box

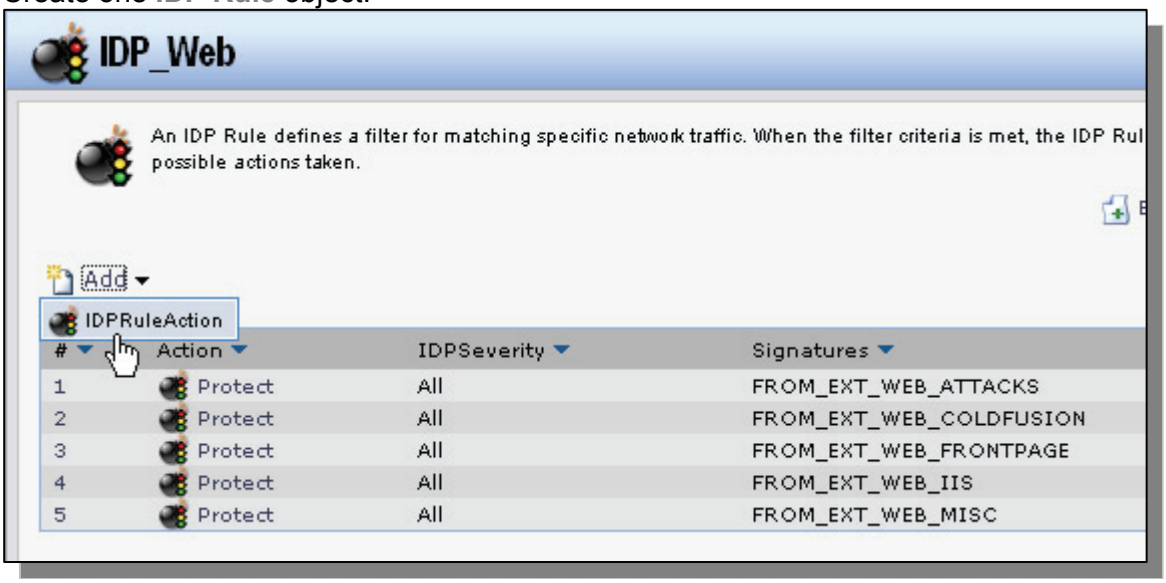
Click OK.

Note:
All signature sets could be used for any traffic direction and it depends on IDP rule setting.

5-6. Add signature set with WEB_PHP into IDP Rule Action

In this step, we will create additional **IDP Rule Action** based on same **IDP Rule** which could includes other IDP signature set to provide more high coverage and accuracy for HTTP type attack.

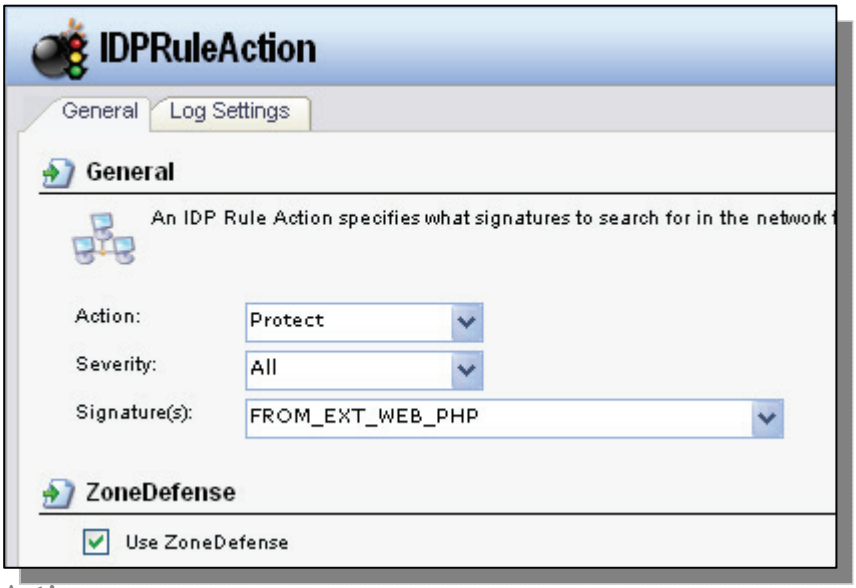
Create one IDP Rule object:



Now, we will add the signature set with **"FROM_EXT_WEB_PHP"** into IDP Rule Action.

In the General tab:

General:



Action: **Protect**
Severity: **All**
Signature(s): **FROM_EXT_WEB_PHP**
Check the Use ZoneDefense box

Click OK.

Save and activate the configuration