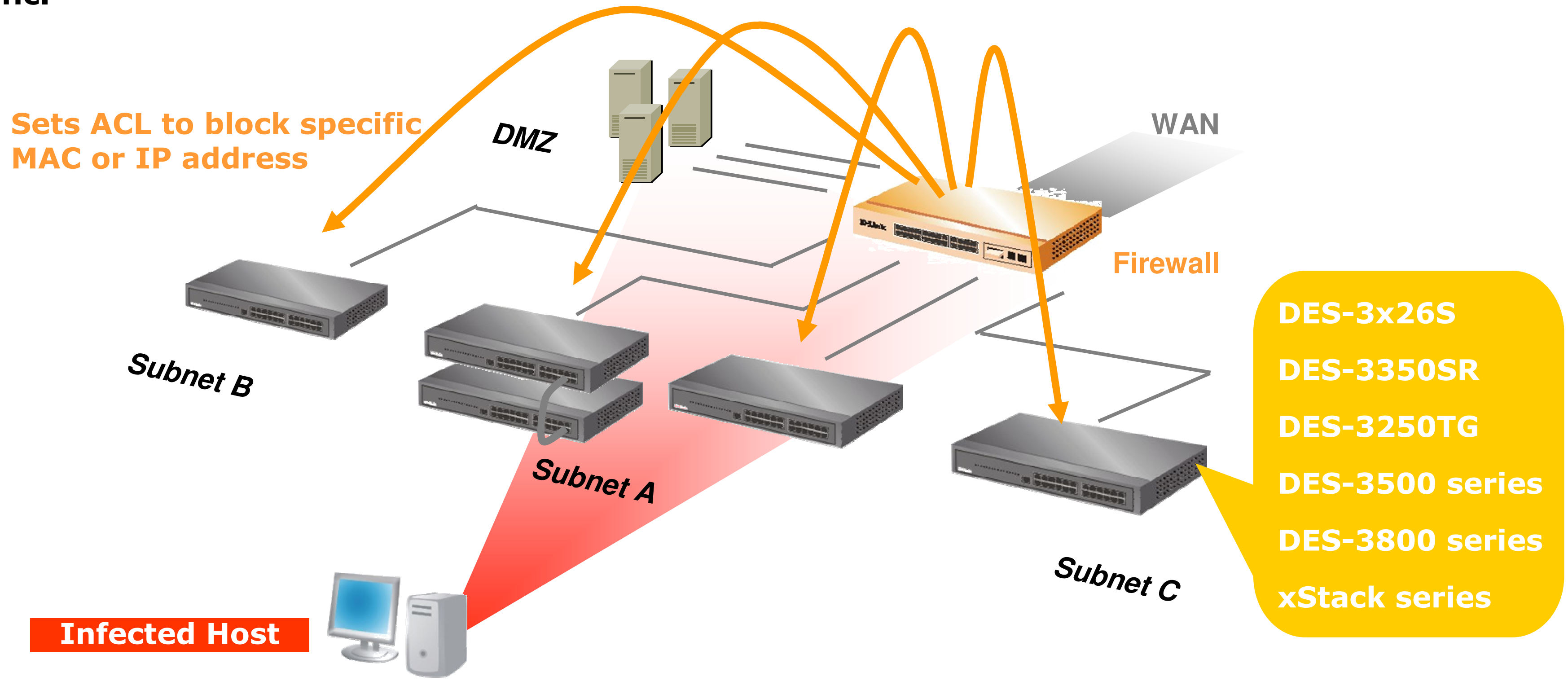
ZoneDefense

Setup Examples

ZoneDefense

- If there’s an infected host spreading worm into the network.
- Firewall can stop the malicious traffic flooding to other subnets but have no way to stop it infecting its network [Subnet A].
- The most effective solution will be: Firewall triggers the ACL in LAN switches to perform real time filtering on any malicious traffic.

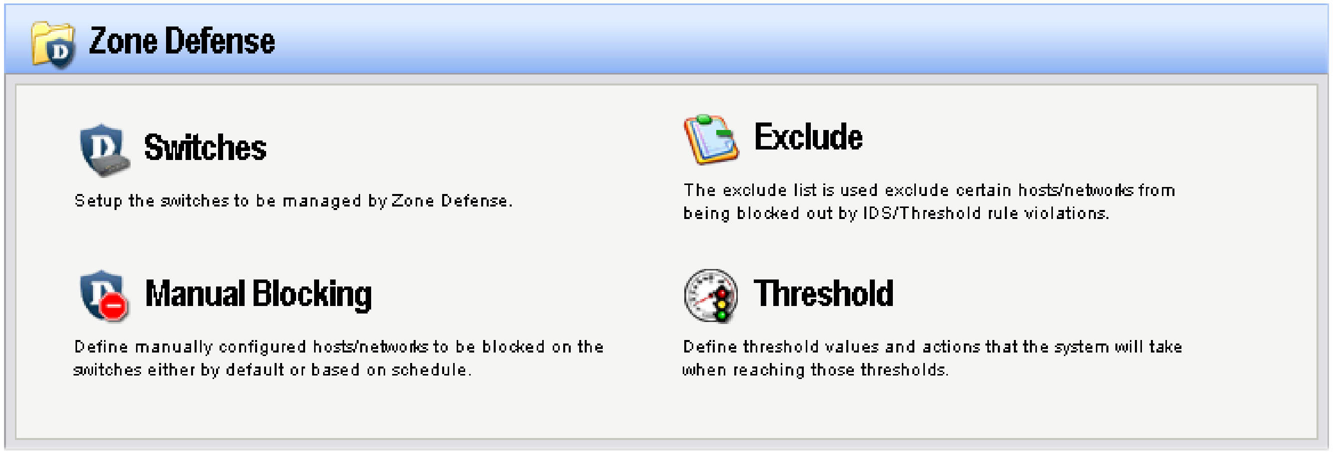
D-Link Firewalls implement ZoneDefense feature to perform proactive network security with D-Link switches



Setup Examples

ZoneDefense

- **ZoneDefense is a proprietary solution from D-Link. It operates with D-Link switches to isolate infected hosts that are generating unusual traffic on LAN.**
- **It uses Threshold rules to examine connections through the firewall and take actions upon them. The threshold rules monitor the number of connections per second.**
- **When a pre-defined limit is reached, the firewall sends block requests to the switches configured for ZoneDefense.**



Zone Defense

Switches

Setup the switches to be managed by Zone Defense.

Exclude

The exclude list is used exclude certain hosts/networks from being blocked out by IDS/Threshold rule violations.

Manual Blocking

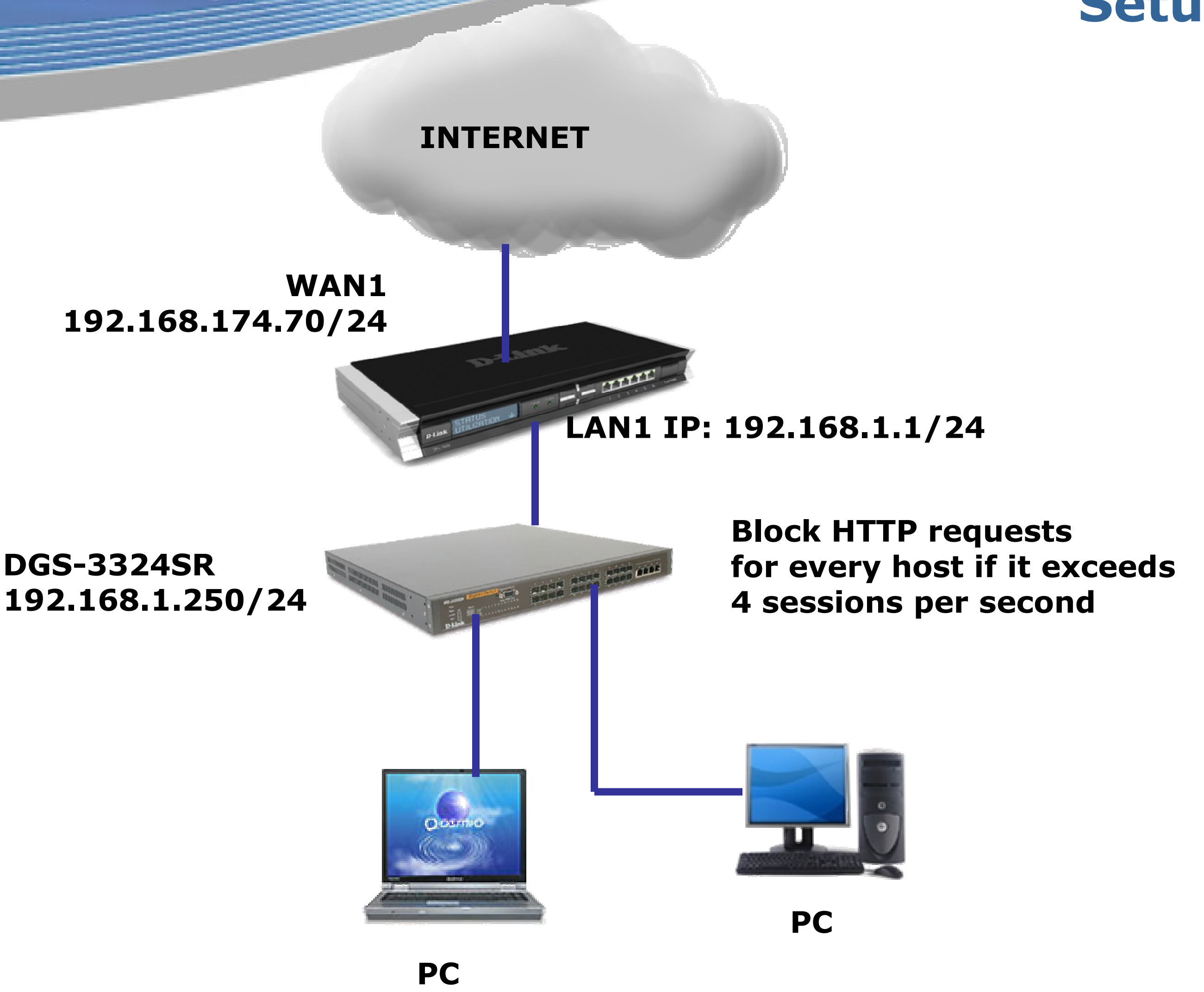
Define manually configured hosts/networks to be blocked on the switches either by default or based on schedule.

Threshold

Define threshold values and actions that the system will take when reaching those thresholds.

Setup Examples

ZoneDefense



INTERNET

WAN1
192.168.174.70/24

LAN1 IP: 192.168.1.1/24

DGS-3324SR
192.168.1.250/24

Block HTTP requests
for every host if it exceeds
4 sessions per second

PC

PC

Setup Examples

ZoneDefense

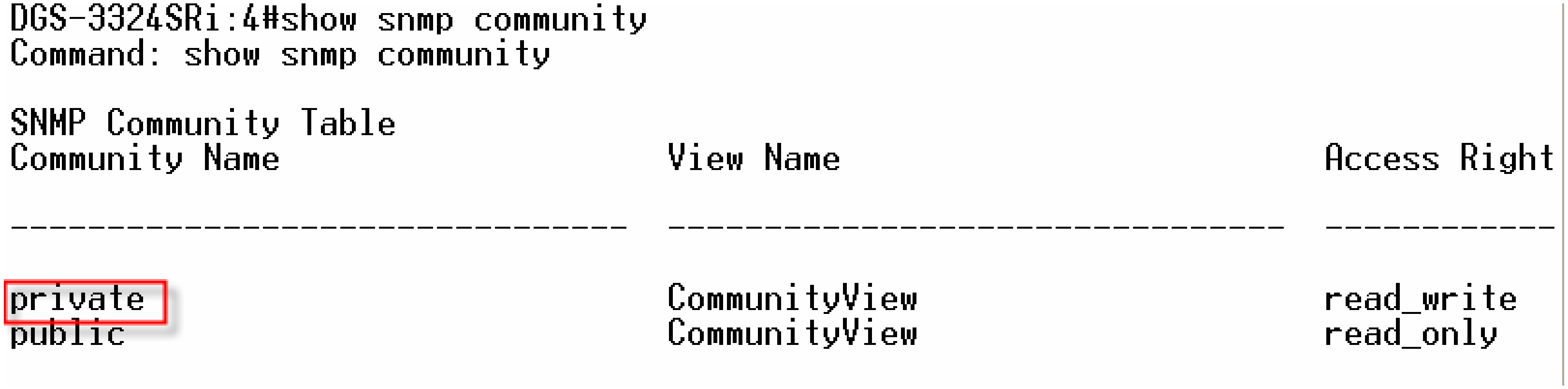
Setting up ZoneDefence in the firewall to control the ACL in a ZoneDefence aware switch.

Configuration Steps:

- **Configure the switch.**
- **Exclude the switch and Administrator's PC.**
- **Create and configure the Threshold rules.**

Setup Examples

ZoneDefense



```
DGS-3324SRi:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                    View Name                         Access Right

--------------------------------  --------------------------------  ------------

private                           CommunityView                     read_write
public                            CommunityView                     read_only
```

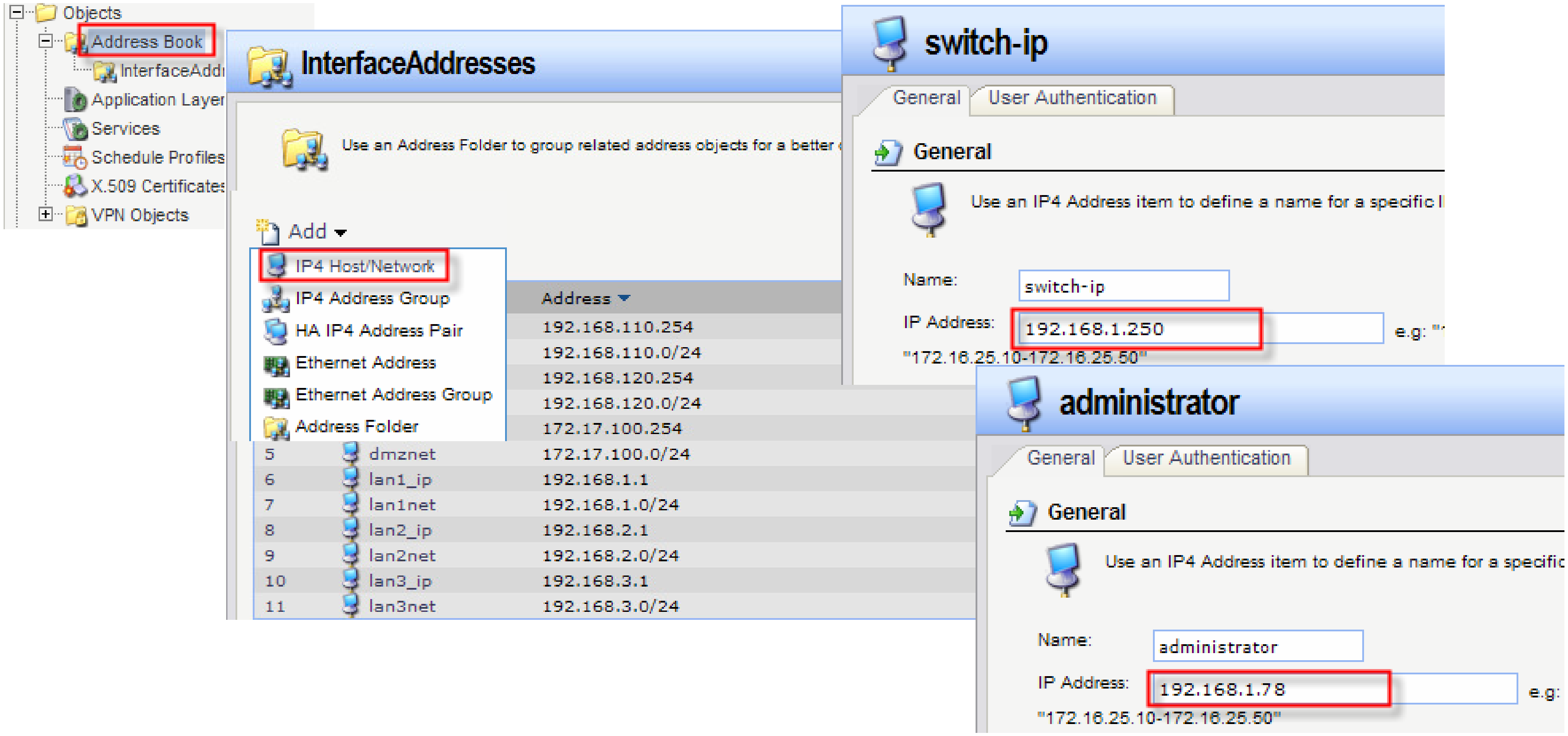
Verify communication between the firewall and the switch.
Check the SNMP community in the switch.
Command: "show snmp community"

D-Link
Building Networks for People

NetDefend

Setup Examples

ZoneDefense



InterfaceAddresses

Use an Address Folder to group related address objects for a better

		Address
		192.168.110.254
		192.168.110.0/24
		192.168.120.254
		192.168.120.0/24
		172.17.100.254
5	dmznet	172.17.100.0/24
6	lan1_ip	192.168.1.1
7	lan1net	192.168.1.0/24
8	lan2_ip	192.168.2.1
9	lan2net	192.168.2.0/24
10	lan3_ip	192.168.3.1
11	lan3net	192.168.3.0/24

switch-ip

General

Use an IP4 Address item to define a name for a specific I

Name: switch-ip

IP Address: 192.168.1.250 e.g: "

"172.16.25.10-172.16.25.50"

administrator

General

Use an IP4 Address item to define a name for a specific

Name: administrator

IP Address: 192.168.1.78 e.g:

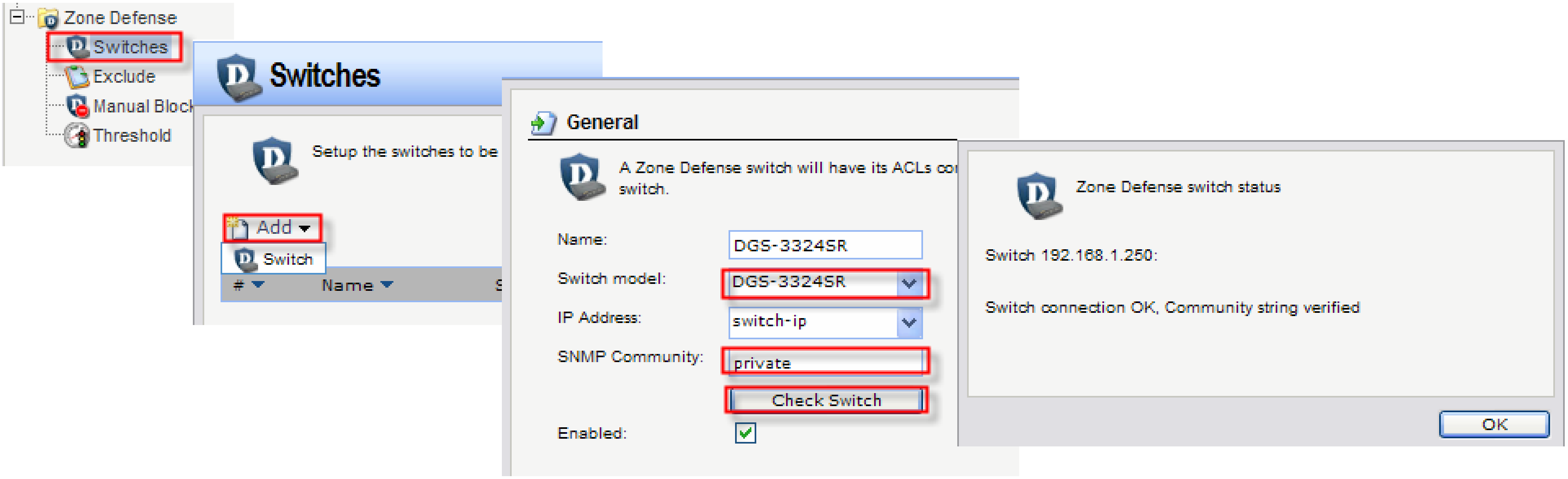
"172.16.25.10-172.16.25.50"

Go to Objects > Address Book > Interface Addresses.

Create two new objects for the switch and for the administrator's PC.

Setup Examples

ZoneDefense



Setup the switches to be

A Zone Defense switch will have its ACLs co switch.

Name: DGS-3324SR

Switch model: DGS-3324SR

IP Address: switch-ip

SNMP Community: private

Enabled: ☑

Zone Defense switch status

Switch 192.168.1.250:

Switch connection OK, Community string verified

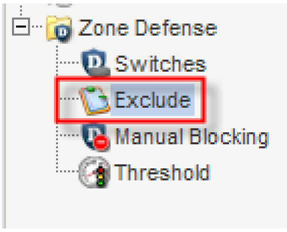
Go to Zone Defense > Switches.

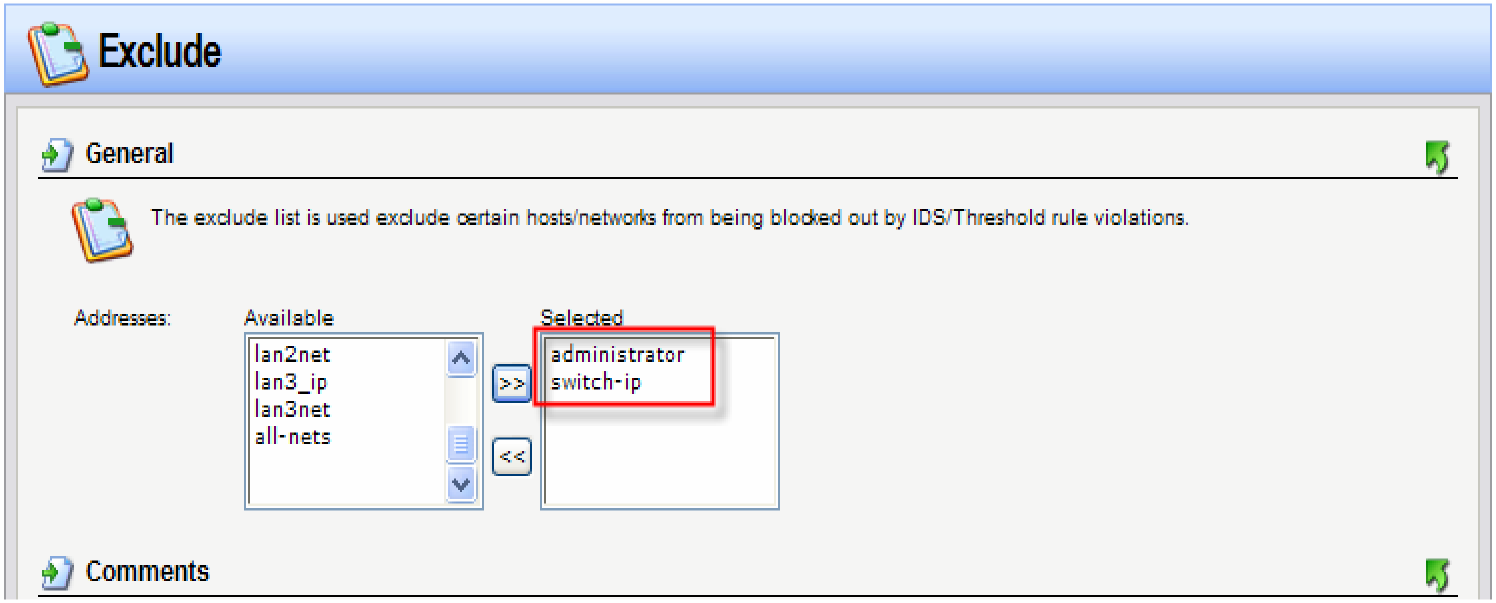
Add a new switch and specify the model of the switch.

Set the correct SNMP community string. Check connectivity with the switch.

Setup Examples

ZoneDefense





Exclude

General

The exclude list is used exclude certain hosts/networks from being blocked out by IDS/Threshold rule violations.

Addresses:

Available	Selected
lan2net lan3_ip lan3net all-nets	administrator switch-ip

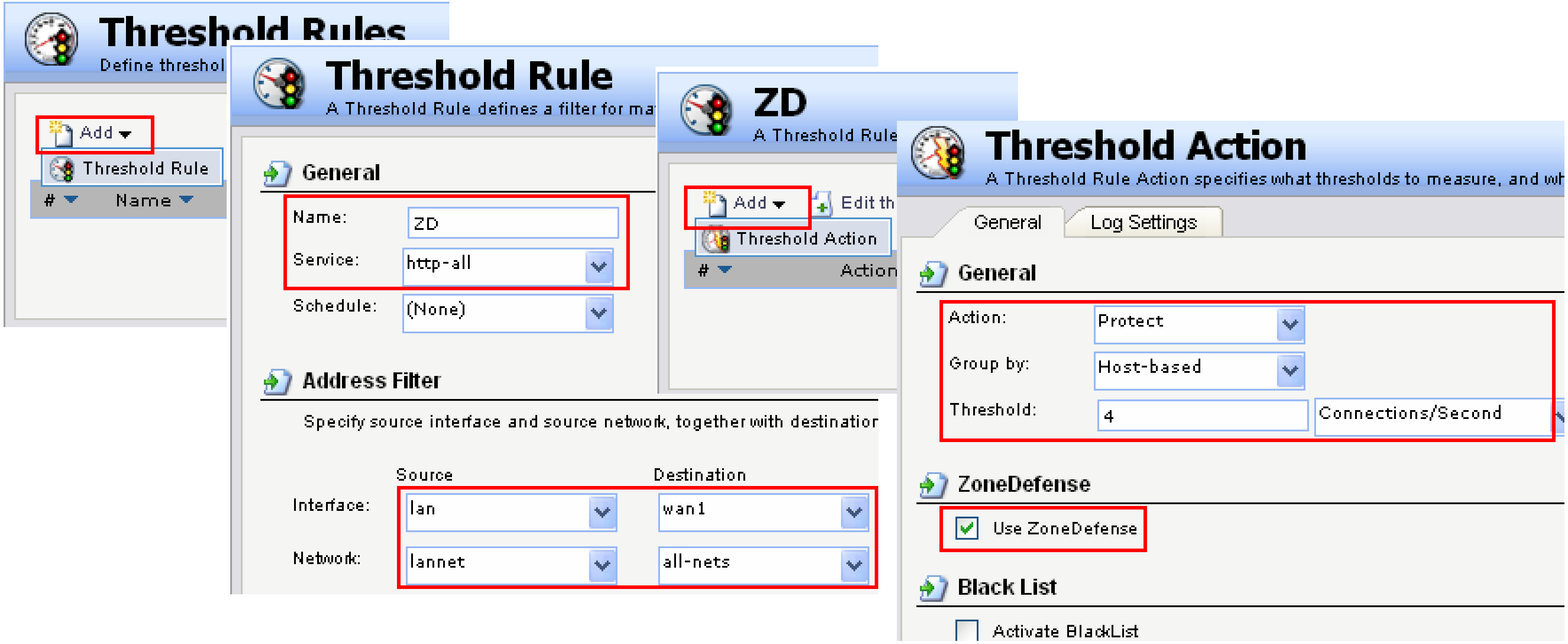
Comments

Go to Zone Defense > Exclude.

Add a new entry and select the Switch IP and the Administrator’s PC IP.

Setup Examples

ZoneDefense



Threshold Rule

A Threshold Rule defines a filter for ma

General

Name: ZD

Service: http-all

Schedule: (None)

Address Filter

Specify source interface and source network, together with destinatior

	Source	Destination
Interface:	lan	wan1
Network:	lannet	all-nets

Threshold Action

A Threshold Rule Action specifies what thresholds to measure, and wh

General

Action: Protect

Group by: Host-based

Threshold: 4 Connections/Second

ZoneDefense

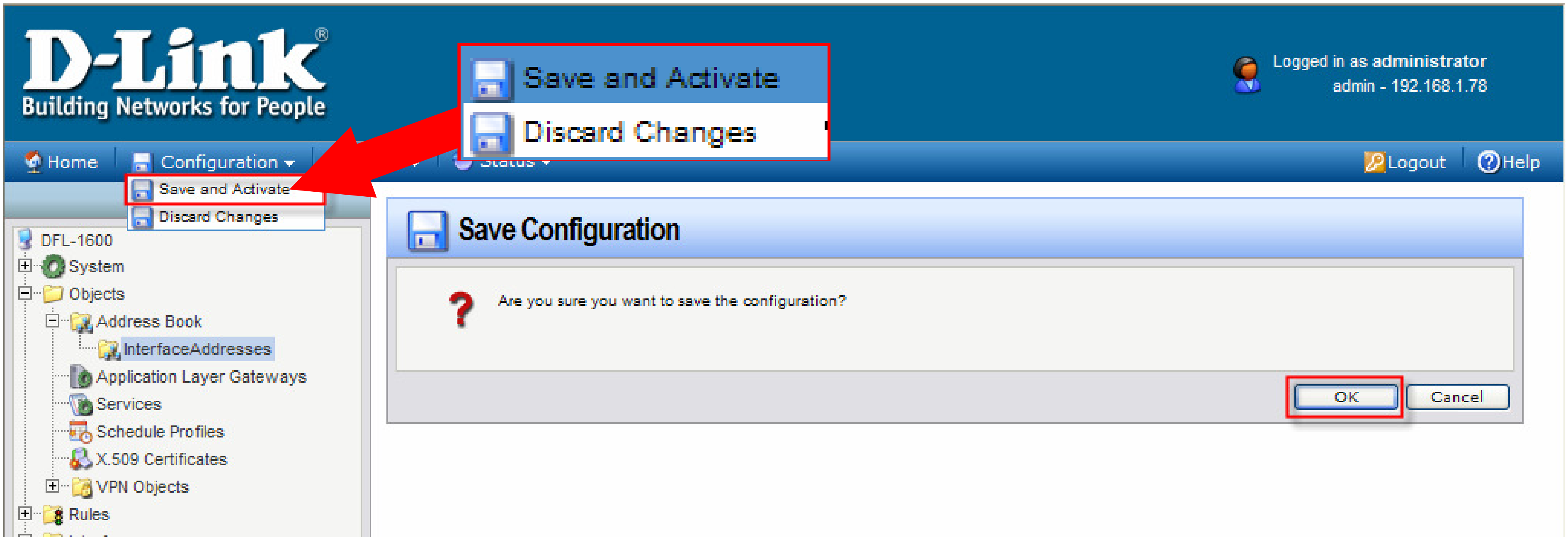
☑ Use ZoneDefense

Black List

□ Activate BlackList

Go to Traffic Management > Threshold Rules. Create a new threshold rule. Select the required service and interfaces then click OK button.

Create a threshold action required. Set the desired threshold (connections per second). Enable Use ZoneDefense and click OK button.



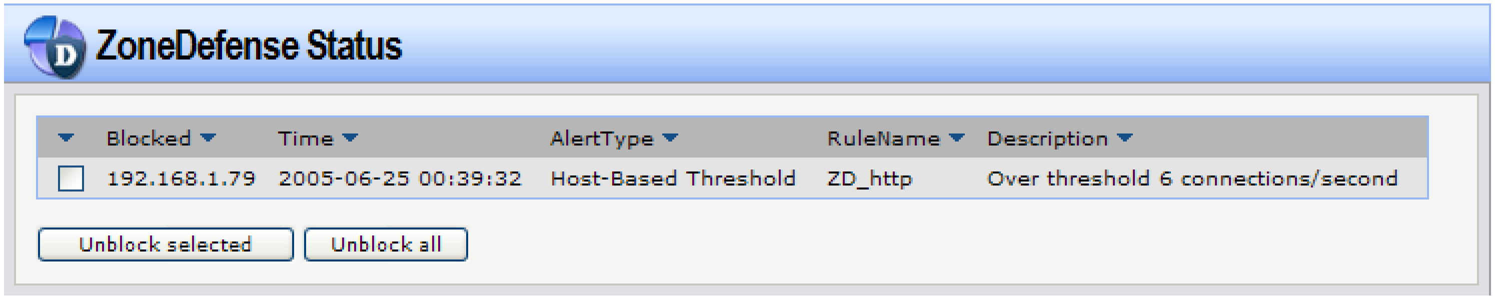
Are you sure you want to save the configuration?

Save and Activate the new configuration.

Setup Examples

ZoneDefense

Firewall ZoneDefense status:



ZoneDefense Status

	Blocked	Time	AlertType	RuleName	Description
□	192.168.1.79	2005-06-25 00:39:32	Host-Based Threshold	ZD_http	Over threshold 6 connections/second