Примеры настройки межсетевых экранов D-Link серии NetDefend

DFL-210/800/1600/2500

Сценарий: Настройка ZoneDefense для модели коммутатора D-Link DES-3226S

Последнее обновление: 2005-10-20

Обзор:

В этом документе условное обозначение *Objects->Address book* означает, что в дереве на левой стороне экрана сначала нужно нажать (раскрыть) **Objects** и затем **Address Book**.

Большинство примеров в этом документе приведены для межсетевого экрана DFL-800. Те же самые настройки могут использоваться для всех других моделей этой серии. Единственное различие в названиях интерфейсов. Так как модели DFL-1600 и DFL-2500 имеют более одного сетевого интерфейса, lan -интерфейсы называются lan1, lan2 и lan3.

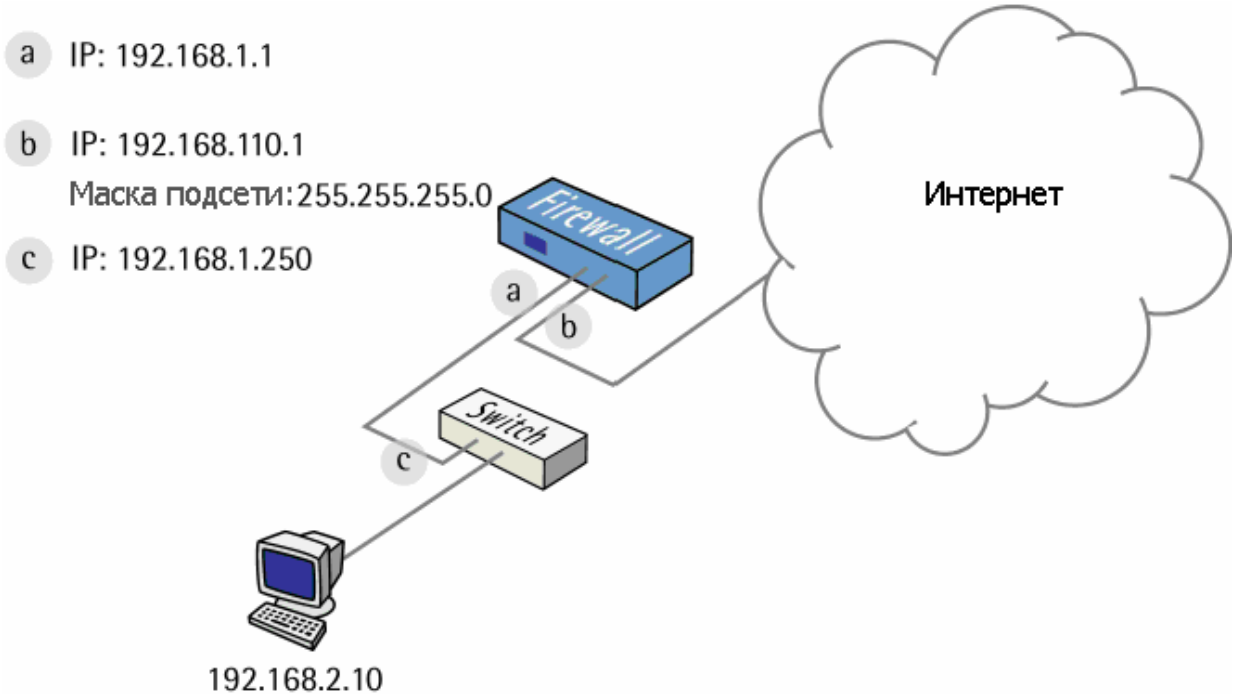
Скриншоты в этом документе приведены для программного обеспечения версии 2.04.00. Если используется более поздняя версия ПО, скриншоты могут отличаться от тех, которые появятся в браузере.

Для предотвращения влияния существующих настроек на настройки, описанные в этом руководстве, перед началом работы сбросьте межсетевой экран к заводским настройкам по умолчанию.

8 Настройка ZoneDefense для модели коммутатора D-Link DES-3226S

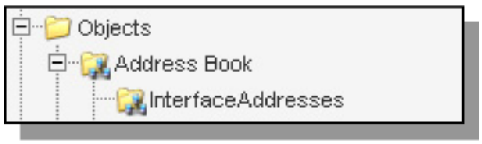
В этом примере будет показано, как настроить межсетевой экран для активизации фунгкции ZoneDefense.

Описание: В локальной сети находится коммутатор D-Link DES-3226S. Этот пример показывает, как задать **Microsoft-DS Threshold** (порт TCP 445) равным 10 соединений/в секунду (например, при работе SASSER.A будет отправлять большое количество TCP SYN на порт 445). Если количество соединений превышает этот лимит, межсетевой экран будет блокировать порт определенного сетевого узла на коммутаторе (в этом сценарии узел 192.168.2.10). Порт коммутатора, подключенный к межсетевому экрану, должен быть настроен на использование адреса 192.168.1.250 и идентификационной строки (community string) MyCompany.



1. Адреса

Перейти в *Objects -> Address book -> InterfaceAddresses.*



Изменить следующие пункты:

Заменить **lan_ip** на **192.168.1.1**
Заменить **lannet** на **192.168.1.0/24**

Заменить **wan1_ip** на **192.168.110.1**

Заменить **wan1net** на **192.168.110.0/24**

Перейти в *Objects -> Address book.*

Добавить новую папку **Address Folder** называемую **LocalHosts.**

В новой папке создать новый **IP4 Host/Network:**

Name: DES-3226S
IP Address: 192.168.1.250

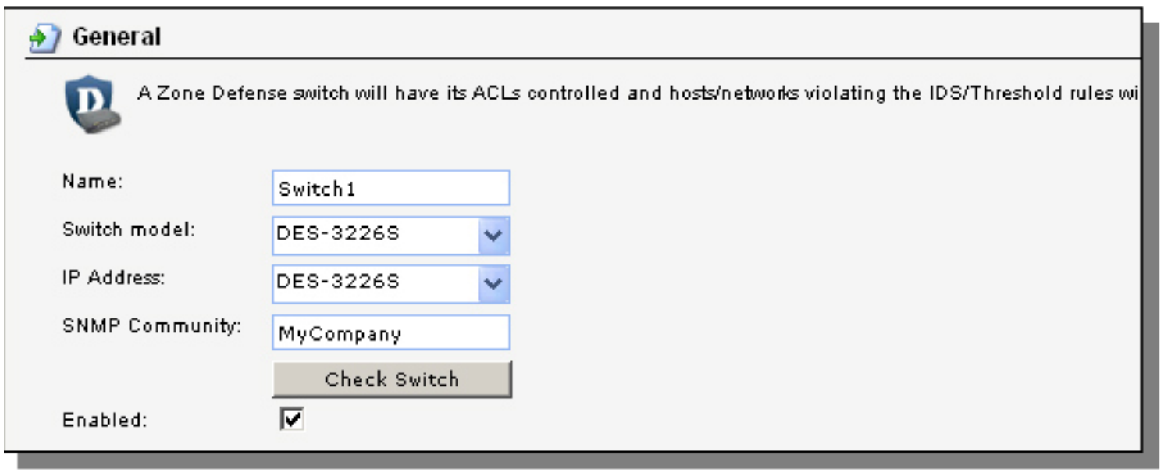
Нажать **Ok**

2. Настройка коммутатора

Перейти в *Zone Defence -> Switches.*

Добавить новый коммутатор **Switch:**

General:



Name: Switch1
Switch Model: DES-3226S
IP Address: DES-3226S (Это IP-адрес порта коммутатора, который подключен к межсетевому экрану)
SNMP Community: MyCompany

Взвести «флажок» **Enabled**
Нажатием на кнопку **Check Switch** можно проверить настройки и возможность соединения.

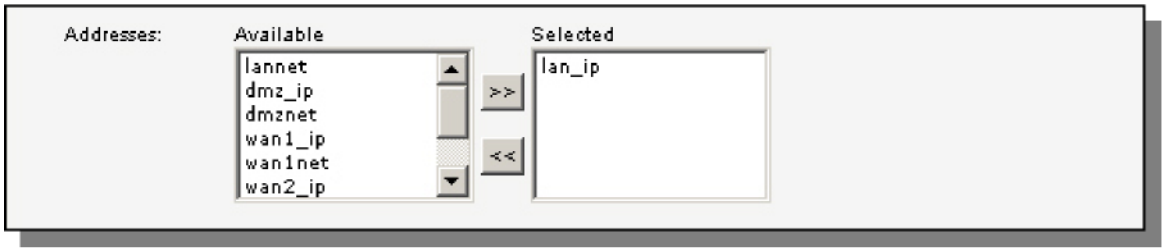
Нажать **Ok.**

3. Список исключений

Чтобы предотвратить межсетевой экран от случайной блокировки доступа к коммутатору, добавьте интерфейс межсетевого экрана для управления коммутатором в список исключений.

Перейти в *ZoneDefense -> Exclude.*

General:



Выбрать **lan_ip** и добавить в выбранный список.

Нажать **Ok.**

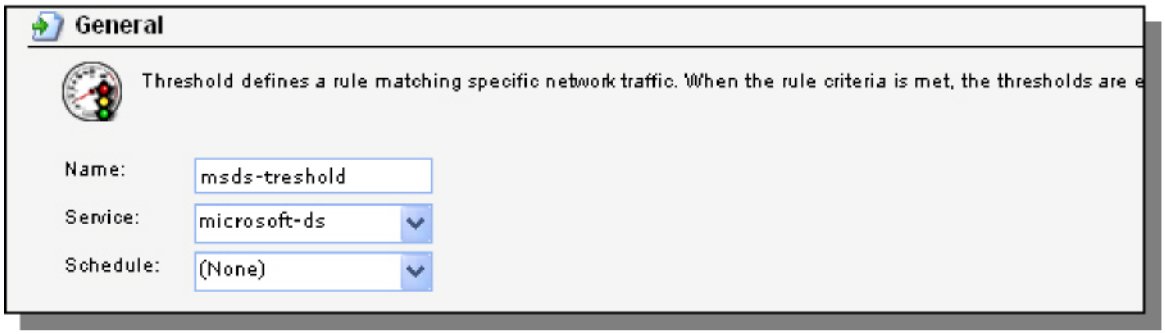
4. Пороговые правила

Перейти в *ZoneDefense -> Threshold.*

Добавить новый **Threshold.**

Вкладка **General**:

General:



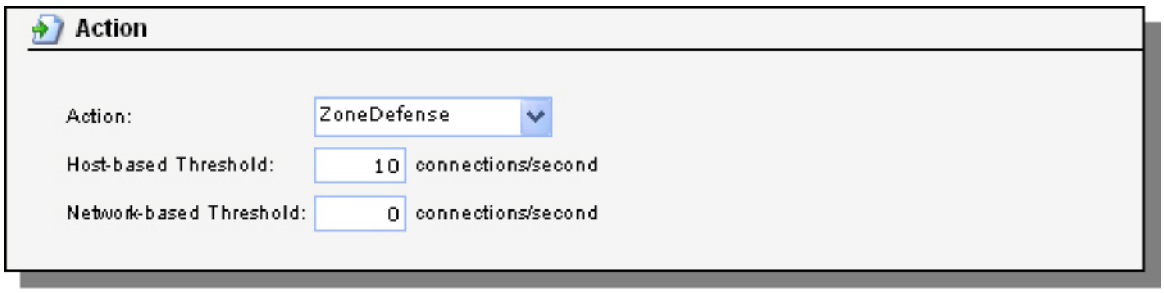
Name: msds- threshold
Service: microsoft-ds
Schedule: (None)

Address Filter:

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

Вкладка **Action**:

Action:



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

Нажать **Ok.**

Сохранить и активировать настройки.