МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

НАСТРОЙКА ZONE-BASED POLICY FIREWALL

Методические рекомендации по выполнению лабораторной работы №5
для студентов направления подготовки бакалавриата
10.03.01«Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Настройка Zone-Based Policy Firewall [Текст] : методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 8 с.: ил. 1. – Библиогр.: с. 8.

Содержат сведения по вопросам работы в программном продукте Cisco Packet Tracer. Указывается порядок выполнения лабораторной работы, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,47. Уч.-изд. л. 0,42. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

Начиная с версии IOS 12.4, в маршрутизаторах появилась функция Zone-Based Policy Firewall, позволяющая производить настройку правил межсетевого экрана. Эта функция позволяет назначить интерфейсам маршрутизатора зоны безопасности и установить правила взаимодействия между ними.

Конфигурирование Zone-Based Policy Firewall заключается в выполнение следующих шагов:

1) назначить зоны межсетевого экрана;
2) определить возможность прохождения сетевого трафика между зонами;
3) включить существующие сетевые интерфейсы в созданные зоны;
4) определить классы, к которым будут применяться политики для пересечения пары зон;
5) определить политики для пар зон, регламентирующие производимые действия над проходящим сетевым трафиком; 6) применить политики для выбранных пар зон.

Рассмотрим настройку Zone-Based Policy Firewall для случая, представленного на рисунке 30. В демилитаризованной зоне (ДМЗ) с адресом 172.16.0.0/16 расположены: Web-сервер (172.16.0.4); почтовый сервер (172.16.0.5); FTP-сервер (172.16.0.6). Адрес внутренней сети (пользователи) 192.168.20.0/24. Внешний IP-адрес маршрутизатора 10.0.0.2, маска сети 255.0.0.0, внутренний – 192.168.20.2.

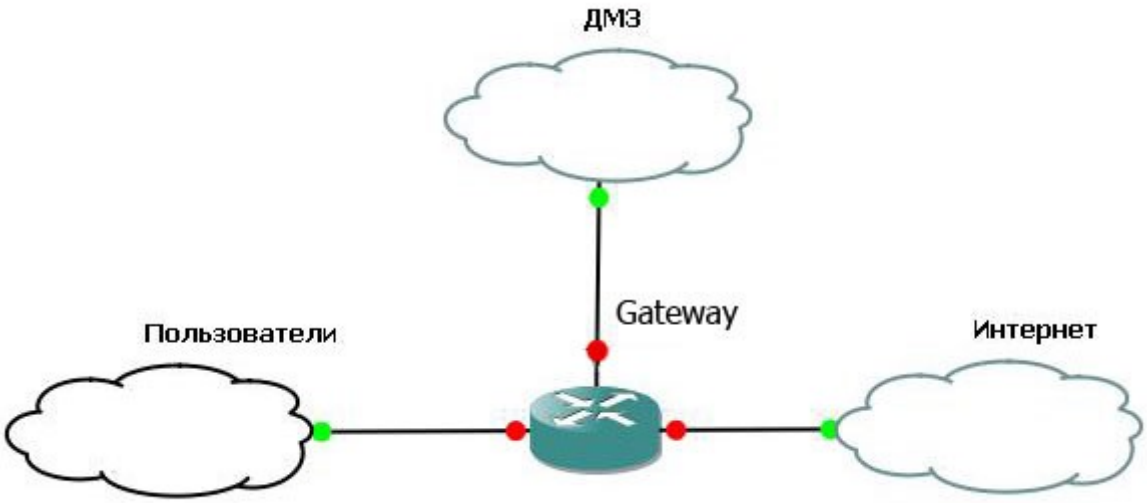

Рисунок 1 - Схема сети

ВЫПОЛНИТЬ!

1. Создать в GNS3 топологию сети, представленную выше (на рисунке 1).
2. В режиме глобального конфигурирования определить зоны безопасности. Для пользователей задать зону с именем inside, для Интернета – outside, для ДМЗ – DMZ.

```
Gateway(config)#zone security outside
Gateway(config-sec-zone)#description internet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security inside
Gateway(config-sec-zone)# description intranet
Gateway(config-sec-zone)#exit
Gateway(config)#zone security dmz
Gateway(config-sec-zone)#description DMZ
Gateway(config-sec-zone)#exit.
```

3. Назначить интерфейсы в зоны. По умолчанию прохождения трафика между зонами запрещено.

Для зоны outside:

```
Gateway(config)#interface FastEthernet0/0
Gateway(config-if)#ip address 10.0.0.2  255.0.0.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security outside
```

Gateway(config-if)#description outside
Gateway(config-if)#exit.
Для зоны inside:
Gateway(config)#interface FastEthernet0/1
Gateway(config-if)#ip address 192.168.20.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security inside
Gateway(config-if)#description inside
Gateway(config-if)#exit.
Для зоны DMZ:
Gateway(config)#interface FastEthernet1/0
Gateway(config-if)#ip address 172.16.0.2 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#zone-member security dmz
Gateway(config-if)#description DMZ
Gateway(config-if)#exit.

4. Определить протоколы, по которым пользователям разрешено выходить в Интернет (http, ftp, smtp, pop3, dns, icmp).

Gateway(config)#class-map type inspect match-any cm_http-ftp-dns-smtp-pop3-icmp
Gateway(config-cmap)#match protocol http
Gateway(config-cmap)#match protocol ftp Gateway(config-cmap)#match protocol pop3
Gateway(config-cmap)#match protocol smtp
Gateway(config-cmap)#match protocol dns
Gateway(config-cmap)#match protocol icmp
Gateway(config-cmap)#exit.

5. Определить политики:

Gateway(config)#policy-map type inspect in-out
Gateway(config-pmap)#class type inspect cm_httpftp-dns-smtp-pop3-icmp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

6. Создать цепочку из пары зон inside → outside:

Gateway(config)#zone-pair security insideoutside source inside destination outside

Gateway(config-sec-zone-pair)#service-policy type inspect in-out
Gateway(config-sec-zone-pair)#exit.

7. Создать списки доступа для публичных серверов:

Gateway(config)#access-list 101 remark webserver
Gateway(config)#access-list 101 permit ip any host 172.16.0.4
Gateway(config)#access-list 102 remark mailserver
Gateway(config)#access-list 102 permit ip any host 172.16.0.5
Gateway(config)#access-list 103 remark ftpserver
Gateway(config)#access-list 103 permit ip any host 172.16.0.6.

8. Определить протоколы для доступа к серверам из внешней сети:

Gateway(config)#class-map type inspect match-all web
Gateway(config-cmap)#match access-group 101 Gateway(config-cmap)#match protocol http
Gateway(config-cmap)#exit
Gateway(config)#class-map type inspect match-all mail
Gateway(config-cmap)#match access-group 102
Gateway(config-cmap)#match protocol smtp
Gateway(config-cmap)#match protocol pop3
Gateway(config-cmap)#exit
Gateway(config)#class-map type inspect match-all ftp
Gateway(config-cmap)#match access-group 103
Gateway(config-cmap)#match protocol ftp
Gateway(config-cmap)#exit.

9. Задать политики для ДМЗ:

Gateway(config)#policy-map type inspect webmail-ftp-dmz
Gateway(config-pmap)#class type inspect web
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect mail
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#class type inspect ftp
Gateway(config-pmap-c)#inspect
Gateway(config-pmap-c)#exit
Gateway(config-pmap)#exit.

10. Создать цепочку из пары зон outside → dmz:

Gateway(config)#zone-pair security out-dmz source outside destination dmz

Gateway(config-sec-zone-pair)#service-policy type inspect web-mail-ftp-dmz

Gateway(config-sec-zone-pair)#exit.

Проверить работоспособность созданной конфигурации.

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.