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

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г.Локтионова
«__» _____ 2016 г.

# ДЕМИЛИТАРИЗОВАННЫЕ ЗОНЫ (DMZ)

Методические указания
по выполнению лабораторной работы
для студентов, обучающихся по направлению подготовки
11.03.02 «Инфокоммуникационные технологии и системы связи»
по курсу «Методы и средства моделирования
телекоммуникационных систем и устройств», а также для
студентов других направлений подготовки в области
информационных технологий

Курск 2016

УДК 654:004.7 (075.8)

Составители: преподаватель кафедры И.Г. Бабанин
преподаватель кафедры Н.П. Павлюченков
младший научный сотрудник Т.М. Петрияненко

Рецензент
Кандидат технических наук, старший научный сотрудник,
профессор кафедры А.М. Потапенко

Демилитаризованные зоны (DMZ): методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: И.Г.Бабанин, Н.П. Павлюченков, Т.М. Петрияненко. Курск, 2016. 11 с.

Методические указания по выполнению лабораторной работы содержат краткие теоретические сведения о функции Zone-Based Policy Firewall, задания по выполнению работы, а также перечень вопросов для самопроверки изучаемого материала.

Полученные знания в результате выполнения работы дадут возможность сформировать целостную картину информационного взаимодействия в современных сетях, что является фундаментом для изучения остальных дисциплин профессионального цикла учебного плана, а также могут быть использованы в будущей профессиональной деятельности выпускника, связанной с сетевыми технологиями.

Предназначены для студентов, обучающихся по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» по курсу «Методы и средства моделирования телекоммуникационных систем и устройств», а также для студентов других направлений подготовки в области информационных технологий в системе высшего образования.

Текст печатается в авторской редакции

Подписано печать . Формат 60x841/16.
Усл. печ. л.. Уч.-изд.л. 0,9 Тираж 100 экз. Заказ. 233 Бесплатно
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

## 1 Цель работы

- изучение способом построения демилитаризованных зон (DMZ) с использованием оборудования Cisco Systems.

## 2 Краткие теоретические сведения

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 [1].

## 3 Перечень ресурсов, необходимых для выполнения работы

- персональный компьютер с конфигурацией не ниже Pentium IV, ОЗУ 256 Мб;
- сетевой эмулятор Cisco Packet Tracer.

## 4 Задание на лабораторную работу

1) Создать в Cisco Packet Tracer топологию сети, представленную на рисунке 1.

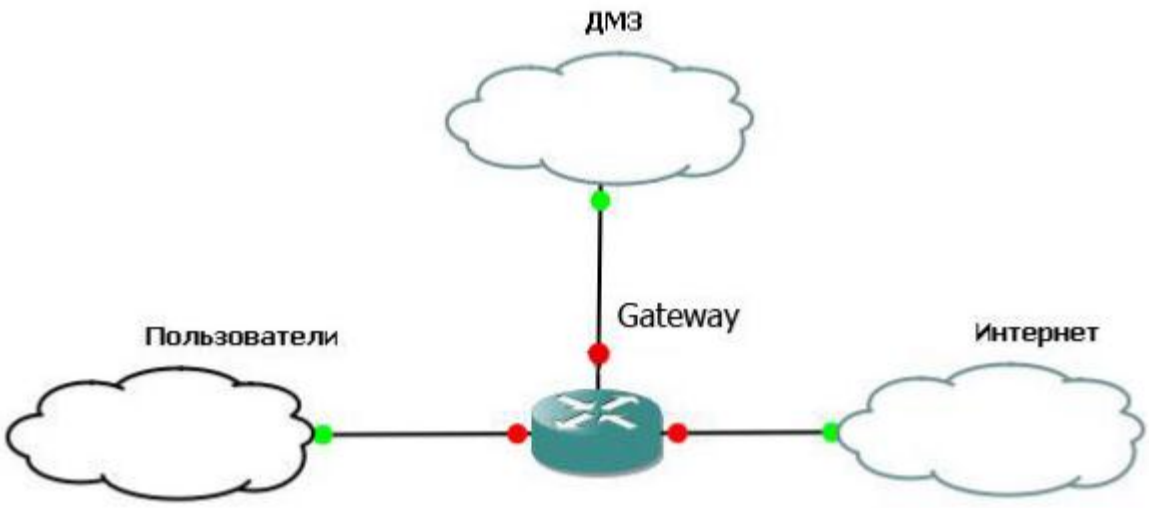


Рисунок 1 – Топология сети

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_http-ftp-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 inside-outside 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 web-server
Gateway(config)#access-list 101 permit ip any host 172.16.0.4
Gateway(config)#access-list 102 remark mail-server
Gateway(config)#access-list 102 permit ip any host 172.16.0.5
Gateway(config)#access-list 103 remark ftp-server

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 web-mail-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.

11) Проверить работоспособность созданной конфигурации.

*Примечание: каждая итерация должна сопровождаться скриншотом (-ами).*

## 5 Требования к оформлению отчёта по выполнению лабораторной работы

Отчёт должен быть оформлен с помощью редактора MS Word, версии 97 и выше (.doc, .rtf).

Параметры страницы:

- верхнее поле- 2 см;
- нижнее поле- 2 см;
- левое поле- 3 см;
- правое поле- 1 см;
- переплет- 0 см;
- размер бумаги А4;
- различать колонтитулы первой страницы.

Шрифт текста Times New Roman, 14 пунктов, через 1,5 интервала, выравнивание по ширине, первая строка с отступом 1,5 см. Номер страницы внизу, по центру, 14 пунктов.

Несложные формулы должны быть набраны с клавиатуры и с использованием команды «Вставка→Символ». Сложные формулы должны быть набраны в редакторе MathType 6.0 Equation.

Отчёт по лабораторной работе должен содержать:

- название предмета, номер и название лабораторной работы;
- фамилию и инициалы автора, номер группы;
- фамилию и инициалы преподавателя;
- цель работы;
- перечень используемого оборудования;
- последовательность действий проведения исследований;
- вывод о проделанной работе;
- ответы на вопросы п. 6;
- дату выполнения и личную подпись.

Результаты различных измерений необходимо представить в виде нескольких самостоятельных таблиц и графиков. Каждая таблица и каждый график должны иметь свой заголовок и исходные данные эксперимента.

При выполнении численных расчетов надо записать формулу определяемой величины, сделать соответственную численную подстановку и произвести вычисления.

Пример оформления отчёта представлен в приложении 1.

## 6 Примерный перечень вопросов для защиты лабораторной работы

1) Зачем необходимо построение демилитаризованных зон (DMZ)?
2) В выполнении каких шагов заключается конфигурирование Zone-Based Policy Firewall?
3) Какие существуют схемы построения сетей с использованием демилитаризованных зон?
4) С какой версии IOS появилась технология Zone-Based Policy Firewall?

## 7 Список использованных источников

1) Андрончик А.Н., Коллеров А.С., Синадский А.С., Щербаков М.Ю. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие; под общ. ред. Синадского Н.И.- Екатеринбург: изд-во Урал. ун-та, 2014. – 180 с.

Приложение 1
Пример оформления отчёта по лабораторной работе

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра космического приборостроения и систем связи

Отчёт по выполнению лабораторной работы
по курсу «Радиопередающие и радиоприёмные устройства»
на тему «Изучение принципа работы супергетеродинного приёмника»

Выполнил: студент группы ИТ-11б
Иванов И.И.
_____ «___»_____2012
(подпись)

Проверил: д.т.н., профессор кафедры
Петров П.П.
_____ «___»_____2012
(подпись)

Курск 2016

1 Цель работы

Ознакомиться …

2 Структурная схема макета и перечень используемого оборудования

Структурная схема лабораторного макета для проведения исследований спектров сигналов представлена на рисунке 2.1.

Рисунок 2.1 – Структурная схема лабораторного макета

Перечень используемого оборудования:

- лабораторный стенд «Радиоприёмные устройства» (1 к-т);
- сменный блок «Изучение принципа работы супергетеродинного радиоприёмника АМ сигналов» (1 к-т);
- осциллограф типа С1-96 (1 к-т);
- милливольтметр переменного напряжения типа DT-820B (1 к-т).

3 Последовательность проведения и результаты лабораторных исследований

3.1 Снятие амплитудно-частотной характеристики входной цепи

Результаты снятия зависимости напряжения на выходе входной цепи от частоты генератора, при фиксированном напряжении на входе, представлены в таблице 1.

Таблица 1 – АЧХ входной цепи

| | | | | |
|---|---|---|---|---|
| Частота генератора, кГц | | | | |
| Напряжение на выходе входной цепи $U_{ВЫХ}$, мВ при $U_{ВХ}$ = 500 мВ | | | | |

Продолжение таблицы 1

| | | | | |
|---|---|---|---|---|
| Нормированное напряжение на выходе входной цепи, $U_{ВЫХ}/ U_{ВЫХ.МАКС.}$ | | | | |

4 Ответы на контрольные вопросы

Вопрос №1. Какие основные функции радиоприёмных устройств?

Ответ:

Вопрос №2. Перечислите основные электрические характеристики радиоприемников.

Ответ:

5 Вывод о проделанной работе

В ходе выполнения лабораторной работы ознакомился с …