МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

МЕЖСЕТЕВЫЕ ЭКРАНЫ CISCO PIX

Методические рекомендации по выполнению лабораторной работы №6
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

Межсетевые экраны Cisco PIX [Текст] : методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 17 с.: ил. 6. – Библиогр.: с. 17.

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. 0,99. Уч.-изд. л. 0,89. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1 Назначение межсетевых экранов Cisco PIX

Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (МЭ). Межсетевой экран – это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или исходящей из нее.

Существуют три сетевые зоны, с которыми работают межсетевые экраны: внутренняя, внешняя и демилитаризованная.

Внутренняя (inside) зона является так называемой доверительной зоной, к которой относятся устройства и конечные узлы закрытой сети. Обычно эти устройства и узлы подчиняются определенной политике безопасности при работе с другими сетями, относящимися к внешней зоне. Внешняя зона (outside) объединяет недоверенные (non-Trusted) сети. Демилитаризованная зона DMZ (De-Militarized Zone) является частью защищаемой сети, для которой устанавливаются особые правила безопасности. Обычно DMZ создается в случае необходимости размещения в сети серверов публичного доступа, например web-сервера. Основной функцией межсетевого экрана является защита узлов, находящихся во внутренней и демилитаризованных зонах от воздействий с узлов, расположенных во внешней зоне.

Линейкой устройств Cisco, предназначенных для решения задач межсетевого экранирования, является Cisco Secure PIX Firewall. В настоящее время пользователям предлагаются следующие модели аппаратно-программных межсетевых экранов Cisco Secure PIX Firewall – PIX 501, 506E, 515E, 525 и 535.

Рисунок 1 - Вид устройства Cisco PIX 525

Общим компонентом данных устройств является применение адаптивного алгоритма безопасности ASA. Cisco PIX Firewall является межсетевым экраном, использующим технологию пакетной фильтрации с запоминанием состояния (технология динамической фильтрации). Эта технология реализуется адаптивным алгоритмом безопасности (ASA – Adaptive Security Algorithm), основанным на концепции уровней безопасности (security levels). Уровень безопасности определяет степень доверия к тому или иному интерфейсу межсетевого экрана в зависимости от того, защищен он или нет относительно другого интерфейса. С помощью ASA осуществляется изоляция подключенных к межсетевому экрану сегментов сетей, поддерживаются так называемые периметры безопасности и контролируется трафик, проходящий между этими сегментами сетей.

Каждому интерфейсу Cisco PIX Firewall присваивается уровень безопасности от 0 до 100. Значение уровня 100 означает самый высокий уровень безопасности устройства. Этот уровень назначается по умолчанию интерфейсу, связанному с внутренней (inside) зоной. Без создания определенных разрешений узлы внешней зоны не получат доступ к внутренней зоне, тогда как узлы внутренней зоны имеют доступ к другим (внешним) зонам.

Значение уровня 0 устанавливает наименьший уровень безопасности. Назначается по умолчанию интерфейсу, связанному с внешней (outside) зоной. Так как 0 является самым низким значением, то за этим интерфейсом обычно находится самая незащищенная сеть, что позволяет ограничить доступ узлов этой сети к сетям, находящимся за другими интерфейсами без явного разрешения. Уровни безопасности от 1 до 99 назначаются другим

задействованным интерфейсам межсетевого экрана и определяют тип доступа, предоставляемый этим интерфейсам.

Уровни безопасности определяют поведение по умолчанию алгоритма следующим образом:

1) ASA разрешает соединения, исходящие от узлов, находящихся в защищаемой сети, то есть соединения с интерфейса с большим уровнем безопасности на интерфейсы с меньшим уровнем безопасности;

2) ASA запрещает соединения от узлов, находящихся в незащищенной сети, то есть соединения с интерфейса с меньшим уровнем безопасности на интерфейс с большим уровнем безопасности;

3) ASA запрещает соединения между узлами, находящимися в сетях, подключенных к интерфейсам с одинаковыми уровнями безопасности;

4) ASA разрешает соединения, идущие от узлов, находящихся в незащищенной сети, к узлам в защищенной сети (соединения с интерфейса с меньшим уровнем безопасности на интерфейс с большим уровнем безопасности) только в случае, если соблюдаются два условия:

- существует статическая трансляция для адреса назначения

(NAT static translation);

- задан список доступа (или conduit), разрешающий данное соединение.

Алгоритм ASA функционирует как динамический (stateful), ориентированный на соединение (connection-oriented) процесс, сохраняющий информацию о сессиях в таблице состояний (state table). Контроль трафика, проходящего через межсетевой экран, осуществляется путем применения политики безопасности и трансляции адресов к таблице состояний.

2 Аппаратная часть межсетевых экранов Cisco PIX

Межсетевые экраны Cisco PIX являются аппаратными устройствами, предназначенными для размещения как в серверной стойке, так и на стене (рисунок 2).

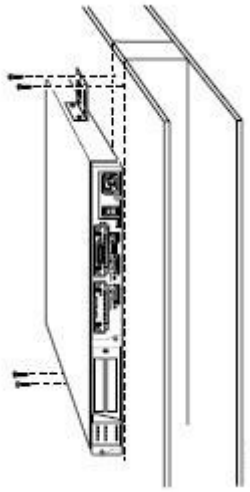

Рисунок 2 - Монтирование устройства Cisco PIX на стену

На лицевой панели устройства (рисунок 3) расположены два индикатора: POWER (наличие питания) и ACTIVE (индикатор режима работоспособности устройства).

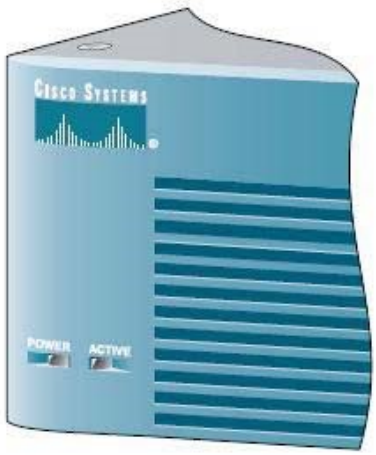

Рисунок 3 - Лицевая панель Cisco PIX 525

На задней панели устройства (рисунок 4) расположены интерфейсы (рисунок 5):

консольный порт для подключения к последовательному порту персонального компьютера с использованием коннектора RJ-45 и управления устройством в режиме командной строки; интерфейсы 100 BaseTX Ethernet0 и 100 BaseTX Ethernet1.

Рисунок 4 - Задняя панель Cisco PIX 525

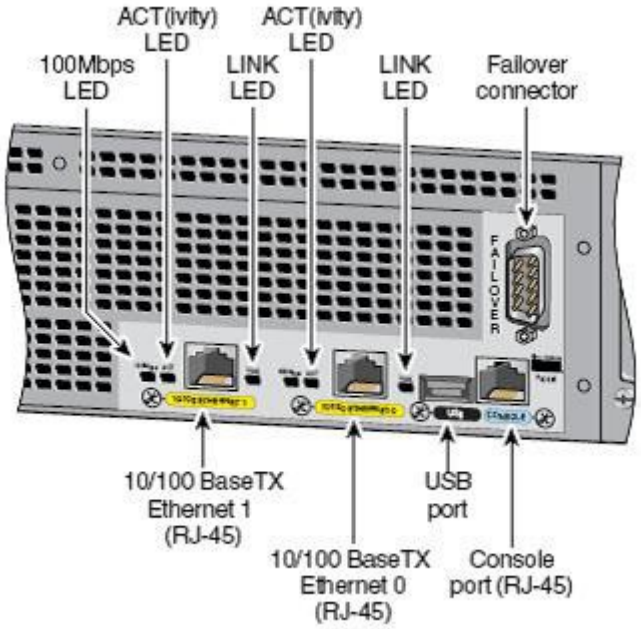

Рисунок 5 - Интерфейсы Cisco PIX 525

3 Базовые команды настройки Cisco PIX

Для начала работы с Cisco PIX определим минимальный набор команд для его настройки. К этим командам относятся: **hostname**, **interface**, **ip address**, **route**, **nameif**, **security-level**, **nat**, **nat-control**, **global**. С частью команд вы уже познакомились в разделе, посвященном настройке маршрутизаторов. Ниже приводится описание команд, специфичных для межсетевого экрана.

Nameif – эта команда предназначена для задания имени и уровня безопасности каждого интерфейса. По умолчанию первые два интерфейса имеют имена inside и outside. Команда имеет следующий синтаксис:

Nameif <интерфейс> <имя_интерфейса> <уровень_ безопасности>.

При первом включении Cisco PIX можно обратить внимание на то, что внутреннему (inside) и внешнему (outside) интерфейсам уже присвоены уровни безопасности: 100 – внутреннему, 0 – внешнему. При задании имен другим интерфейсам автоматически будет назначаться уровень безопасности 0, который в дальнейшем можно изменить.Команда выполняется в глобальном контексте конфигурирования:

PIX(config)#nameif ethernet0 outside security 0 PIX(config)#nameif ethernet1 inside security 100.

Команда **clear xlate** очищает таблицу трансляций, в результате чего происходит сброс всех существующих соединений, что позволяет изменить уровень безопасности интерфейса без ожидания закрытия существующих соединений.

ВЫПОЛНИТЬ!

1. Задать имена и уровни безопасности для интерфейсов межсетевого экрана.
2. Проверить возможность прохождения сетевых пакетов между интерфейсами межсетевого экрана.
3. Включить интерфейсы межсетевого экрана. По умолчанию все интерфейсы выключены, чтобы произвести их включение необходимо в контексте глобального конфигурирования выполнить команду interface. Синтаксис команды: **interface <интерфейс> <скорость> <состояние>.**

Пример:

PIX(config)#interface ethernet0 auto shutdown.

4. Назначить интерфейсам межсетевого экрана IP-адреса. В межсетевых экранах, в отличие от маршрутизаторов, назначение IP-адреса сетевым интерфейсам выполняется в режиме глобального конфигурирования командой:

ip address <имя_интерфейса> <ip_адрес> <маска_сети>.

Пример:

PIX(config)#ip address outside 88.88.88.2 255.255.255.0.

4 Технология NAT

NAT (Network Address Translation) – трансляция адресов, позволяющая скрывать адреса сети от узлов, находящихся за Cisco PIX. При прохождении пакетов через Cisco PIX внутренние адреса сети перед выходом с внешнего интерфейса транслируются в другие адреса. NAT конфигурируется с помощью команд **nat** и **global**.

Когда исходящий пакет от узла, находящегося во внутренней зоне, попадает на Cisco PIX, на котором сконфигурирована система NAT, адрес источника пакета сравнивается с таблицей существующих трансляций. Если этого адреса источника нет в таблице, он транслируется в один из адресов пула и в таблице трансляций появляется новая запись для этого адреса источника. Пул выдаваемых адресов конфигурируется командой **global**. В результате этого происходит обновление таблицы трансляций, а пакет перенаправляется дальше. По истечении определенного времени (значение по умолчанию равно трем часам) запись в таблице трансляций для адреса источника, не пославшего ни одного пакета, очищается и адрес, выданный из пула, освобождается для использования другими узлами внутренней зоны.

Задание правил трансляции адресов исходящих пакетов для одного либо нескольких узлов осуществляется с помощью команды **nat.**

Синтаксис команды можно представить следующим образом: **nat [(if_name)] nat_id address [netmask] [[tcp] tcp_max_conns [emb_limit] [norandomseq]]] [udp udp_max_conns]**, где:

- if_name – имя интерфейса, подключенного к сети, адреса которой необходимо транслировать;
- nat_id – число от 1 до 65535, соответствующее номеру пула глобальных адресов, в которые будут транслироваться внутренние адреса;
- address [netmask] – адрес, в который будет происходить трансляция;
- tcp_max_conns – максимальное число одновременных соединений, разрешенных узлам внутренней зоны. Соединения в

состоянии бездействия закрываются автоматически по истечении таймаута, задаваемого командой **timeout conn**;

- emb_limit – максимальное число незавершенных (embryonic) соединений. К незавершенным соединениям относятся те, которые еще не были до конца установлены между источником и назначением, например, при установке TCP-соединения между узлами;
- norandomseq – устанавливает необходимость при каждом новом соединении генерировать случайный initial sequence number (ISN). Связано это с тем, что TCP/IP стек некоторых ОС использует предсказуемые ISN, а это дает возможность злоумышленнику вклиниться в чужую сессию;
- udp_max_conns – максимальное число одновременных UDP-соединений, разрешенных каждому из узлов внутренней сети. UDP-соединения, находящиеся в состоянии бездействия, закрываются автоматически по истечении таймаута, задаваемого командой **timeout conn**.

Пример настройки службы NAT:

PIX(config)#nat (inside) 1 10.0.0.0 255.255.255.0.

ВЫПОЛНИТЬ!

5. Настроить службу NAT на внутреннем интерфейсе межсетевого экрана.

В команде **nat** параметром nat_id (в примере – 1) указывается номер пула глобальных адресов, которые можно сконфигурировать командой **global**. Синтаксис:

global [(if_name)] nat_id {mapped_ip
[-mapped_ip] [netmask mapped_mask]} | interface, где:

- if_name – имя интерфейса, на котором необходимо использовать задаваемый пул глобальных адресов;
- mapped_ip [-mapped_ip] – один адрес либо диапазон адресов;
- netmask mapped_mask – задание маски для пула адресов в случае, если используются подсети. Если диапазон адресов с заданной маской покрывает несколько подсетей, то адрес подсети и широковещательный адрес подсети не выдаются для трансляции. Например, если задан диапазон адресов 192.168.0.20-192.168.0.140

и маска 255.255.255.128, то адрес второй подсети 192.168.0.128 и широковещательный адрес первой подсети 192.168.0.127 выдаваться не будут;

- interface – определяет использование PAT (Port Address Translation) на интерфейсе. Пример:

PIX(config)#nat (inside) 1 10.0.0.0 255.255.255.0
PIX(config)#global (outside) 1 192.168.0.3-
192.168.0.100

В этом примере сконфигурирован пул из 98 адресов (192.168.0.3-192.168.0.100) под номером 1, в которые будут транслироваться внутренние адреса узлов из сети 10.0.0.0 при прохождении сетевых пакетов через межсетевой экран.

Выдача адресов осуществляется динамически, начиная с начала диапазона и до его конца. В примере первым выданным адресом будет 192.168.0.3.

ВЫПОЛНИТЬ!

6. Выполнить конфигурацию пула глобальных адресов для внутреннего интерфейса межсетевого экрана.

Командой **nat control** включается одноименный режим. При работе в этом режиме пакеты, идущие из внутреннего (inside) интерфейса на внешний (outside), должны иметь сконфигурированное для них правило трансляции. То есть, каждый узел сети внутренней зоны может обмениваться данными с узлами сети внешней зоны, если заданы правила трансляции для этих внутренних узлов. Если на Cisco PIX приходит пакет от внутреннего узла, для которого не сконфигурировано правило трансляции, то этот пакет им не обрабатывается.

Режим **nat control** является выключенным по умолчанию. Поэтому Cisco PIX транслирует адрес источника пакета в любом случае.

ВЫПОЛНИТЬ!

7. Включить nat control режим и проверить возможность прохождения сетевых пакетов между интерфейсами устройства.
8. Выключить nat control режим.

Кроме команды **nat** существует команда **static**, с помощью которой осуществляется конфигурирование статической трансляции. Синтаксис команды:

PIX(config)# static (real_ifc, global_ifc)

{global_ip | interface} {real_ip [netmask mask]}, где:

- real_ifc – интерфейс, на который приходят пакеты, подлежащие трансляции;
- global_ifc – интерфейс, с которого уходит для дальнейшей маршрутизации транслированный пакет;
- global_ip – адрес, в который будет осуществляться трансляция;
- real_ip – адрес, который будет транслироваться. Пример:

PIX(config)#static (inside,outside) 192.168.100.10 10.10.10.10 netmask

255.255.255.255

Все пакеты, приходящие на адрес 192.168.100.10 будут передаваться на узел с адресом 10.10.10.10.

ВЫПОЛНИТЬ!

9. Сконфигурировать статическую трансляцию на внешнем интерфейсе межсетевого экрана.
10. С помощью программного сниффера проверить работу статической трансляции.

Команда **fixup** Cisco PIX предоставляет некоторые возможности глубокого анализа пакетов в межсетевых экранах PIX. Например, команда **fixup protocol http** приводит к тому, что PIX выполняет ряд действий, к которым относятся:

- ведение журналов, фиксирующих URL-запросы, содержащие команды GET;
- мониторинг URL-запросов при помощи средств N2H2 или

Websense;

- фильтрация опасных сценариев Java и ActiveX.

Для последних двух функций межсетевой экран должен быть сконфигурирован с командой **filter**. Пример команд для углубленного анализа трафика по основным протоколам:

PIX(config)#fixup protocol ftp 21

PIX(config)#fixup protocol http 80

PIX(config)#fixup protocol h323 1720

PIX(config)#fixup protocol rsh 514

PIX(config)#fixup protocol smtp 25 PIX(config)# fixup protocol sqlnet 1521.

5 Настройка межсетевых экранов Cisco PIX

При выполнении работы осуществляется конфигурирование Cisco PIX Firewall для того, чтобы отделить и защитить корпоративную сеть от атак из сети «Интернет». Будем рассматривать внутреннюю сеть организации, содержащую Web-сервер, почтовый сервер и FTP-сервер, к которым имеют доступ пользователи сети «Интернет». Весь остальной доступ к узлам внутренней сети закрыт от внешних пользователей. Схема имитируемой сети показана на рисунок 3.8. Адресация серверов внутренней сети выполнена следующим образом:

- Web-сервер: внутренний адрес 192.168.0.4, Интернет-адрес 88.88.88.3;
- почтовый сервер: внутренний адрес 192.168.0.5, Интернет-адрес 88.88.88.4;
- FTP-сервер: внутренний адрес 192.168.0.6, Интернет-адрес 88.88.88.5.

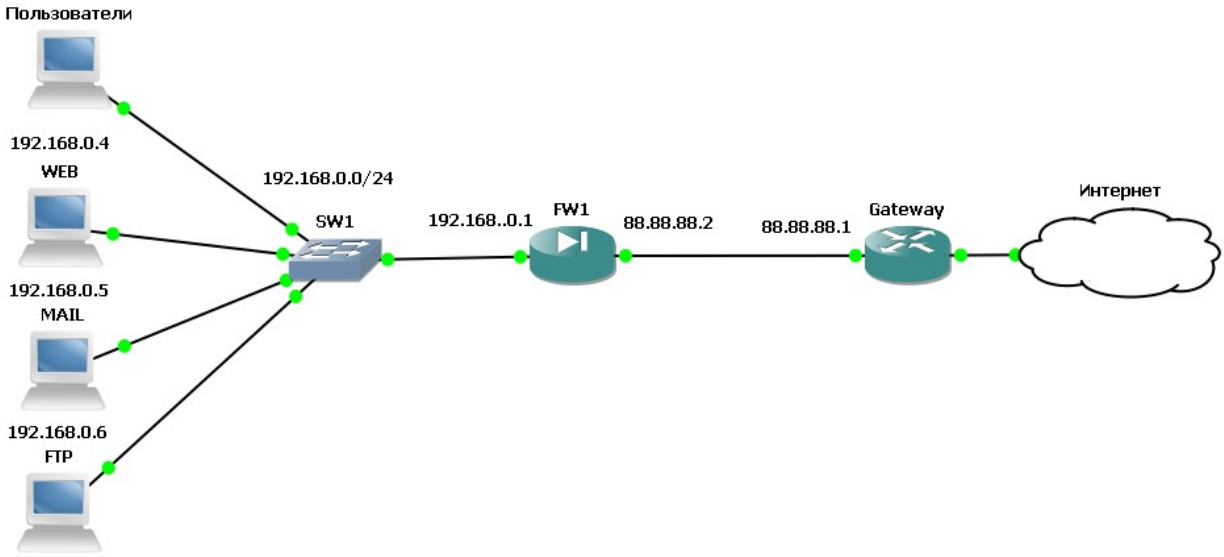

Рисунок 6 - Схема защиты сети

Всем пользователям внутренней сети разрешен неограниченный доступ в Интернет. Также пользователям разрешено выполнять команду ping до узлов в сети «Интернет», в то время как пользователям со стороны сети «Интернет» это запрещено. Провайдером выделен диапазон внешних адресов класса C: 88.88.88.0/24. Адреса 88.88.88.1 и 88.88.88.2 зарезервированы для внешнего маршрутизатора и внешнего интерфейса PIX (см. рисунок 6). Адреса диапазона 88.88.88.3 ÷ 88.88.88.5 отведены для серверов, а адреса 88.88.88.4 ÷ 88.88.88.14 зарезервированы для будущего использования, для пользователей внутренней сети выполняется процедура трансляции адресов.

ВЫПОЛНИТЬ!

11. Создать в GNS3 топологию сети, представленную на рисунок 36.

12. Произвести настройку Cisco PIX Firewall, выполнив следующие команды в контексте глобального конфигурирования:

PIX(config)#nameif ethernet0 outside security0
PIX(config)#nameif ethernet1 inside security100
PIX(config)#hostname pixfirewall
PIX(config)#fixup protocol ftp 21
PIX(config)#fixup protocol http 80

PIX(config)#fixup protocol h323 1720 PIX(config)#fixup protocol rsh 514

PIX(config)#fixup protocol smtp 25

PIX(config)#fixup protocol sqlnet 1521 PIX(config)#fixup protocol sip 5060 PIX(config)#names.

13. Создать ACL, разрешающий исходящие ICMP-запросы и ответы на них:

PIX(config)#access-list 100 permit icmp any any echo-reply

PIX(config)#access-list 100 permit icmp any any time-exceeded

PIX(config)#access-list 100 permit icmp any any unreachable.

14. Добавить разрешения для пользователей Интернет подключаться к Web-, Mail-, и FTP-серверам:

PIX(config)#access-list 100 permit tcp any host 88.88.88.3 eq www

PIX(config)#access-list 100 permit tcp any host 88.88.88.4 eq smtp

PIX(config)#access-list 100 permit tcp any host

88.88.88.5 eq ftp.

15. Включить режим ведения журналов:

PIX(config)#logging on

PIX(config)#no logging timestamp

PIX(config)#no logging standby

PIX(config)#no logging console PIX(config)#no logging monitor.

16. Установить режим сохранения сообщений об ошибках в локальном буфере:

PIX(config)#logging buffered errors.

17. Включить все интерфейсы (выключены по умолчанию):

PIX(config)#interface ethernet0 auto PIX(config)#interface ethernet1 auto.

18. Назначить IP-адреса сетевым интерфейсам:

PIX(config)#ip address outside 88.88.88.2 255.255.255.0

PIX(config)#ip address inside 192.168.0.1 255.255.255.0.

19. Определить пул трансляции адресов, которые используют внутренние узлы для выхода в Интернет:

PIX(config)#global (outside) 1 88.88.88.1588.88.88.253.

20. Определить адрес, который будет использоваться, когда выделенный пул адресов закончится:

PIX(config)#global (outside) 1 88.88.88.254.

21. Установить разрешение для всех внутренних узлов на использование NAT или PAT, определенные ранее:

PIX(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0.

22. Задать статическую трансляцию для внутренних Web-, почтового и FTP-серверов, чтобы они были доступны из Интернета:

PIX(config)#static (inside,outside) 88.88.88.3 192.168.0.4 netmask 255.255.255.255 0 0

PIX(config)#static (inside,outside) 88.88.88.4 192.168.0.5 netmask 255.255.255.255 0 0

PIX(config)#static (inside,outside) 88.88.88.5 192.168.0.6 netmask 255.255.255.255 0 0.

23. Применить разработанный ACL с номером 100 к внешнему интерфейсу, выполнив в его контексте конфигурирования команду:

PIX(config)#access-group 100 in interface outside.

24. Назначить маршрут по умолчанию на маршрутизатор провайдера услуг Интернет командой в глобальном контексте конфигурирования:

PIX(config)#route outside 0.0.0.0 0.0.0.0
88.88.88.1 1.

25. Проверить работоспособность заданной 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.