### Назначение межсетевых экранов Cisco PIX

Систему разграничения компьютерных сетей с различными политиками безопасности, реализующую правила информацион- ного обмена между ними, называют межсетевым экраном (МЭ). Межсетевой экран – это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программ- ное (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 межсе- тевые экраны: внутренняя, внешняя и демилитаризованная.

Внутренняя (inside) зона является так называемой довери- тельной зоной, к которой относятся устройства и конечные узлы закрытой сети. Обычно эти устройства и узлы подчиняются опре- деленной 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 кото- рой 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 внут- ренней и демилитаризованных зонах от воздействий с узлов, рас- положенных во внешней зоне.

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



Рис. 3.3. Вид устройства Cisco PIX 525

Общим компонентом данных устройств является применение адаптивного алгоритма безопасности ASA. Cisco PIX Firewall явля- ется 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 безопас- ности определяет степень доверия к тому или иному интерфейсу межсетевого экрана в зависимости от того, защищен он или нет от- носительно другого интерфейса. С помощью ASA осуществляется изоляция подключенных к межсетевому экрану сегментов сетей, поддерживаются так называемые периметры безопасности и кон- тролируется трафик, проходящий между этими сегментами сетей.

Каждому интерфейсу Cisco PIX Firewall присваивается уро- вень безопасности от 0 до 100. Значение уровня 100 означает самый высокий уровень безопасности устройства. Этот уровень назнача- ется 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 без- опасности. Назначается по умолчанию интерфейсу, связанному с внешней (outside) зоной. Так как 0 является самым низким значени- ем, 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 задействован- ным 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, находя- щихся в защищаемой сети, то есть соединения с интерфейса с большим уровнем безопасности на интерфейсы с меньшим уров- нем безопасности;
2. ASA запрещает соединения от узлов, находящихся в неза- щищенной сети, то есть соединения с интерфейса с меньшим уровнем безопасности на интерфейс с большим уровнем безопас- ности;
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 соблюда- ются 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, со- храняющий информацию о сессиях в таблице состояний (state table). Контроль трафика, проходящего через межсетевой экран, осуществляется путем применения политики безопасности и транс- ляции адресов к таблице состояний.

### Аппаратная часть межсетевых экранов Cisco PIX

Межсетевые экраны Cisco PIX являются аппаратными устрой- ствами, предназначенными для размещения как в серверной стойке, так и на стене (рис. 3.4).

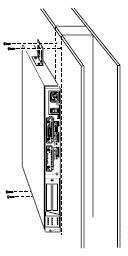


Рис. 3.4. Монтирование устройства Cisco PIX на стену

На лицевой панели устройства (рис. 3.5) расположены два ин- дикатора: POWER (наличие питания) и ACTIVE (индикатор режи- ма работоспособности устройства).

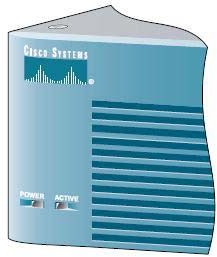


Рис. 3.5. Лицевая панель Cisco PIX 525

На задней панели устройства (рис. 3.6) расположены интер- фейсы (рис. 3.7):

* + - * 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.



Рис. 3.6. Задняя панель Cisco PIX 525

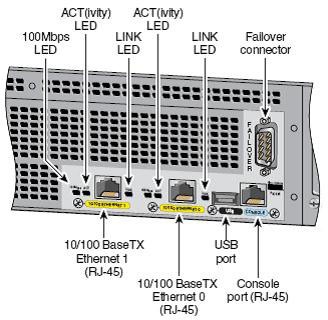


Рис. 3.7. Интерфейсы Cisco PIX 525

### 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 ко- манд вы уже познакомились в разделе, посвященном настройке маршрутизаторов. Ниже приводится описание команд, специфич- ных 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 сле- дующий 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 – внеш- нему. При задании имен другим интерфейсам автоматически будет назначаться уровень безопасности 0, который в дальнейшем можно изменить.Команда выполняется в глобальном контексте конфигу- рирования:

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

Команда **clear xlate** очищает таблицу трансляций, в ре- зультате чего происходит сброс всех существующих соединений, что позволяет изменить уровень безопасности интерфейса без ожи- дания 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 конфигури- рования выполнить команду interface. Синтаксис команды:

# interface <интерфейс> <скорость> <состояние>.

Пример:

# PIX(config)#interface ethernet0 auto shutdown.

1. 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.