1. С помощью программного сниффера проверить работу статической трансляции.

Команда **fixup** Cisco PIX предоставляет некоторые возмож- ности 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, содержа- щие 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 углуб- ленного 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.

### Настройка межсетевых экранов Cisco PIX

При выполнении работы осуществляется конфигурирование Cisco PIX Firewall для того, чтобы отделить и защитить корпора- тивную 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 за- крыт от внешних пользователей. Схема имитируемой сети показана на рис. 3.8. Адресация серверов внутренней сети выполнена следу- ющим 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.

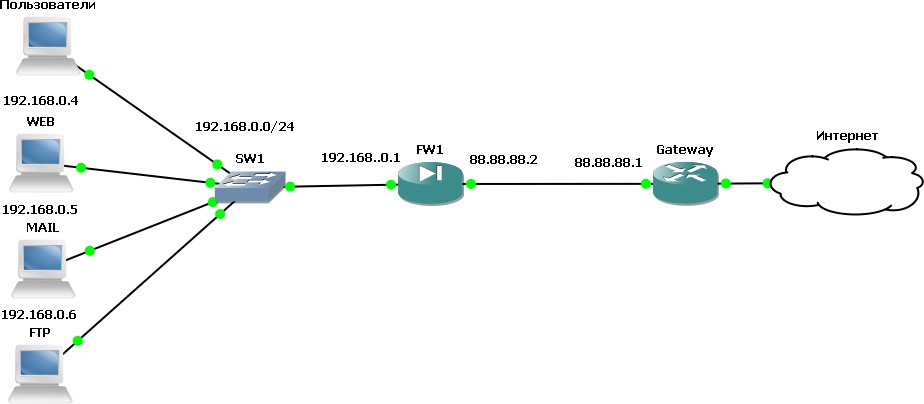


Рис. 3.8. Схема защиты сети

Всем пользователям внутренней сети разрешен неограничен- ный доступ в Интернет. Также пользователям разрешено выпол- нять команду ping до узлов в сети «Интернет», в то время как поль- зователям 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. рис. 3.8). 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 вы- полняется процедура трансляции адресов.

## ВЫПОЛНИТЬ!

1. Создать в GNS3 топологию сети, представленную на рис. 3.8.
2. Произвести настройку Cisco PIX Firewall, выполнив следующие команды в контексте глобального конфигури- рования:

# 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.**

1. 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.**

1. Добавить разрешения для пользователей Интернет подключаться к Web-, Mail-, и FTP-серверам: **PIX(config)#access-list 100 permit tcp any host**
   * + 1. **eq www**

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

* + - 1. **eq smtp**

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

* + - 1. **eq ftp.**

1. 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.** |

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

# PIX(config)#logging buffered errors.

1. Включить все интерфейсы (выключены по умолчанию): **PIX(config)#interface ethernet0 auto PIX(config)#interface ethernet1 auto.**
2. 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.**

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

# PIX(config)#global (outside) 1 88.88.88.15-

**88.88.88.253.**

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

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

1. 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.

1. 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**

* + - 1. **netmask 255.255.255.255 0 0**

**PIX(config)#static (inside,outside) 88.88.88.4**

* + - 1. **netmask 255.255.255.255 0 0**

**PIX(config)#static (inside,outside) 88.88.88.5**

* + - 1. **netmask 255.255.255.255 0 0.**

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

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

1. 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.**

Проверить работоспособность заданной конфигурации