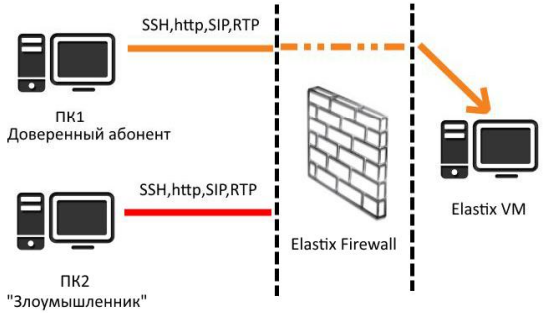
Лабораторная работа №2: Настройка встроенного Firewall'а.

Дата _____	Студенты
№ группы_____	_____
№ бригады_____	_____
	_____

Цель работы: Настройка встроенного в Elastix Firewall'а таким образом, чтобы исключить доступ к серверу по SSH и к веб-интерфейсу через http с незнакомых адресов. Установить допуск на совершение звонков только определённой группе абонентов

Подготовка к лабораторной работе: У каждой бригады должно быть 2 PC с установленными программами Phoner и Wireshark. Один из PC должен иметь предустановленную ОС Elastix, на которой зарегистрировано, как минимум, 2 пользователя.



ПК1 Ip адрес:_____ MAC адрес: Номер SIP:_____	ПК2 Ip адрес:_____ MAC адрес: Номер SIP:_____
IP адрес виртуальной машины _____	

Часть первая: Включение Firewall

1) Запустите виртуальную машину с установленной Elastix, зайдите на веб-интерфейс (логин – admin, пароль – задан вами при установке).
2) Зайдите в настройки Firewall, выбрав опцию security.
3) Включите firewall, нажав на кнопку "Activate Firewall".
4) Выберите в левом меню Define ports. Сделайте скриншот.

Часть вторая: настройка Firewall

1) Скачайте Putty на ПК1 и ПК2. С ПК2 зайдите на сервер Elastix, по его IP-адресу.
2) Введите логин и пароль для root, сделайте скриншот.
3) Теперь настройте firewall так, чтобы доступ к серверу по SHH был доступен только с ПК1. Отредактируйте правило для SSH в Firewall rules. Нужно изменить только поле "source address" прописав нужный ip адрес и маску (/32 в данном примере)
4) Запустите Wireshark и снимите дамп при доступе по SSH с одобренного и с запрещённого адреса. Сохраните данные дампы.
5) Ограничьте доступ по https, чтобы к веб-интерфейсу можно было подсоединиться только с ПК1. С помощью wireshark снимите дамп при удачном и неудачном и успешном подключении.
6) Запретите регистрацию абонентов с адреса ПК2. Отредактируйте правила файрвола для протокола SIP, чтобы происходил REJECT при попытке регистрации в phoner. Аналогично снимите дамп успешной и безуспешной регистрации.

Содержание отчёта:

1) Титульный лист;
2) Цель работы;
3) Скриншоты основного окна firewall'а и окна define ports;
4) Скриншоты wireshark успешного и неудачного подключения по SSH, https, SIP;
5) Блок-схема настроенного Firewall'а;
6) Выводы по проделанной работе.

Контрольные вопросы:

1) Действия ACCEPT,DROP,REJECT;
2) Соответствие адресов и масок;
3) Протоколы: SSH, https, SIP;
4) Протоколы: TCP, UDP, ICMP.