

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Построения защищённой сети IP-телефонии на
базе Elastix

Практическая часть

2015 г.

СОДЕРЖАНИЕ

5.1 Лабораторная работа №1. Установка Elastix в VMware player. Начальная конфигурация, связь между 2 абонентами.	3
5.2 Лабораторная работа №2. Использование встроенного Firewall'a.....	14
5.3 Лабораторная работа №3. Настройка протокола SRTP и TLS в ОС Elastix.....	23
5.4 Лабораторная работа №4. Использование программы Fail2Ban.....	33
5.5 Лабораторная работа №5. Подключение к Elastix через VPN туннель. 36	
Список использованной литературы:.....	45

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Основной целью лабораторного практикума является изучение построения защищённой сети ip-телефонии на базе Elastix.

5.1 Лабораторная работа №1. Установка Elastix в VMware player.
Начальная конфигурация, связь между 2 абонентами.

Цель работы: Ознакомление с принципами работы виртуальной машины, установка ОС Elastix на ВМ, настройка первоначальной конфигурации достаточной для совершения звонка между двумя абонентами внутренней сети, мониторинг проходящего звонка.

Подготовка к лабораторной работе:

На каждую машину должны быть установлены:

1. **Wireshark** - инструмент для захвата и анализа сетевого трафика.
Доступен бесплатно на сайте wireshark.org;
2. **Phoner** – софтвер для системы Windows, поддерживающий VoIP связь.

Порядок выполнения лабораторной работы:

Часть первая – Установка Elastix на виртуальную машину.

- 1) Если требуется, настройте IP адреса на ПК1 и ПК2, чтобы они могли взаимодействовать между собой и заполните часть следующей таблицы

Таблица 5.1

ПК1 IP адрес: _____ MAC адрес: _____ Номер SIP: _____	ПК2 IP адрес: _____ MAC адрес: _____ Номер SIP: _____
IP адрес сервера Elastix _____	

Для проверки соединения откройте командную строку Windows и воспользуйтесь утилитами *ipconfig*, для вывода информации о текущих соединениях, и *ping*, для проверки соединения между ПК1 и ПК2. Сделайте скриншот.

```
C:\Users >ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::e05d:c6bd:1ac9:1782%11
    IPv4-адрес. . . . . : 192.168.1.34
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::a1af:86b8:f4d3:28be%19
    IPv4-адрес. . . . . : 192.168.163.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::2dad:d3ca:809a:2d4b%20
    IPv4-адрес. . . . . : 192.168.6.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

Ethernet adapter VirtualBox Host-Only Network:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::2404:fa6b:3f3:9736%23
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . :
```

Рис. 5.1 Конфигурация адаптеров сети

- 2) Установите **VMware player** на ПК1.
- 3) Выберите *Create a new virtual machine*
В процессе создания выбирайте следующее
 - a) Установить операционную систему позже;
 - b) Система Линукс, Версия CentOS;
 - c) Введите имя своей виртуальной машины вида: StudXY, где X – номер группы, а Y – номер бригады;
 - d) Ёмкость диска – по умолчанию;
 - e) При настройке Hardware переведите network adapter в bridge mode и укажите путь к образу диска elastix в разделе CD\DVD.

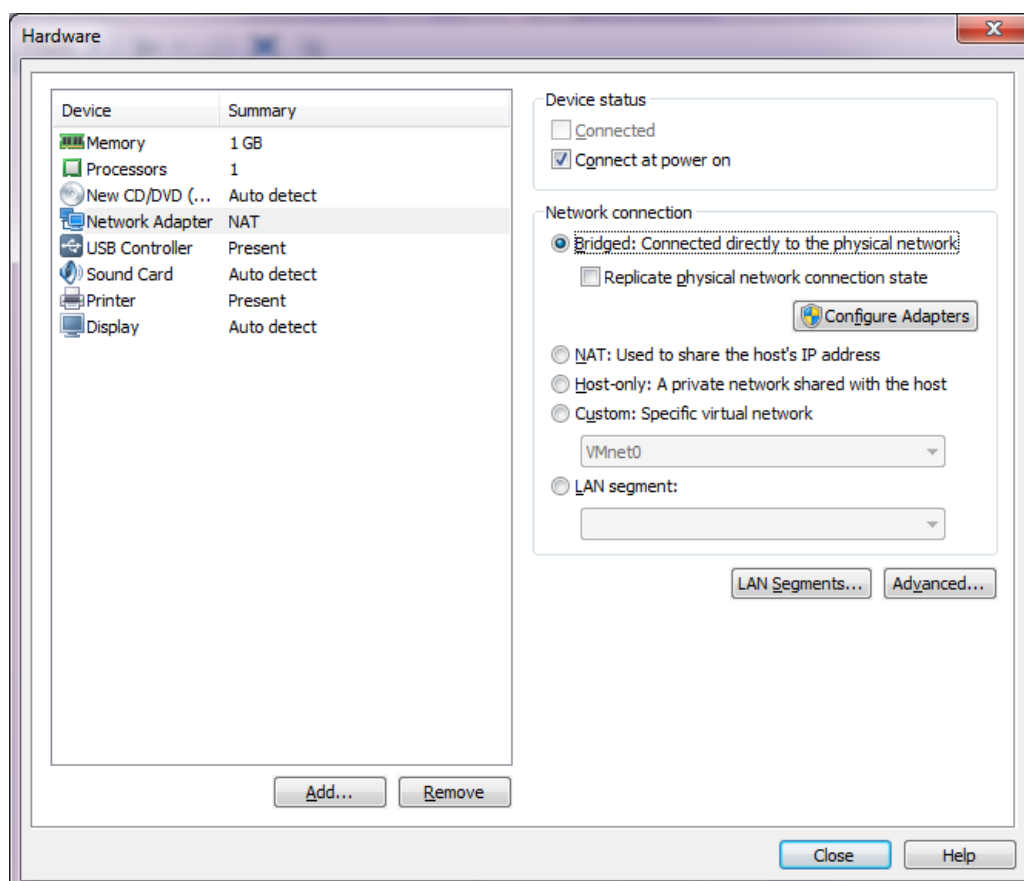


Рис. 5.2 Настройка Network Adapter

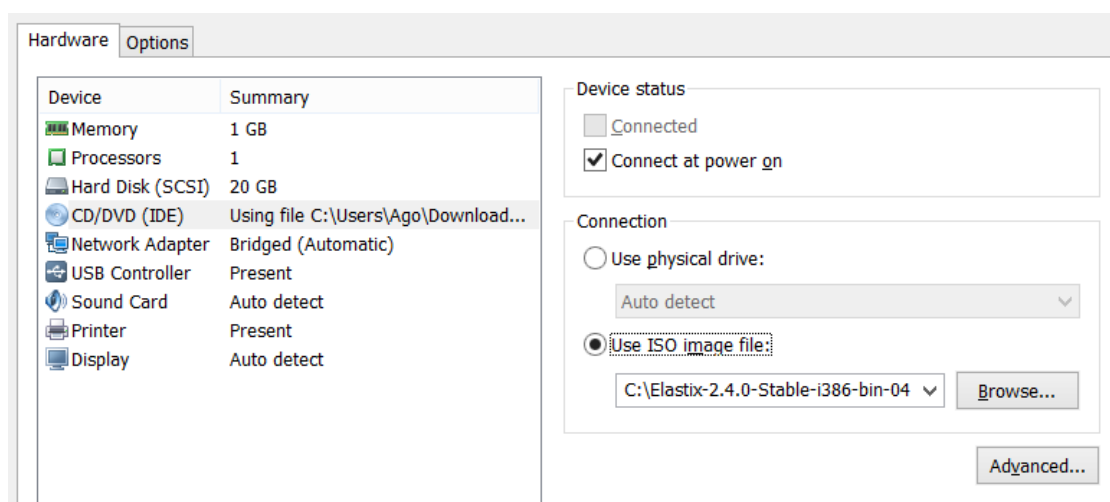


Рис. 5.3 Настройка CD\DVD

При запуске виртуальной машины появится следующий приветственный экран

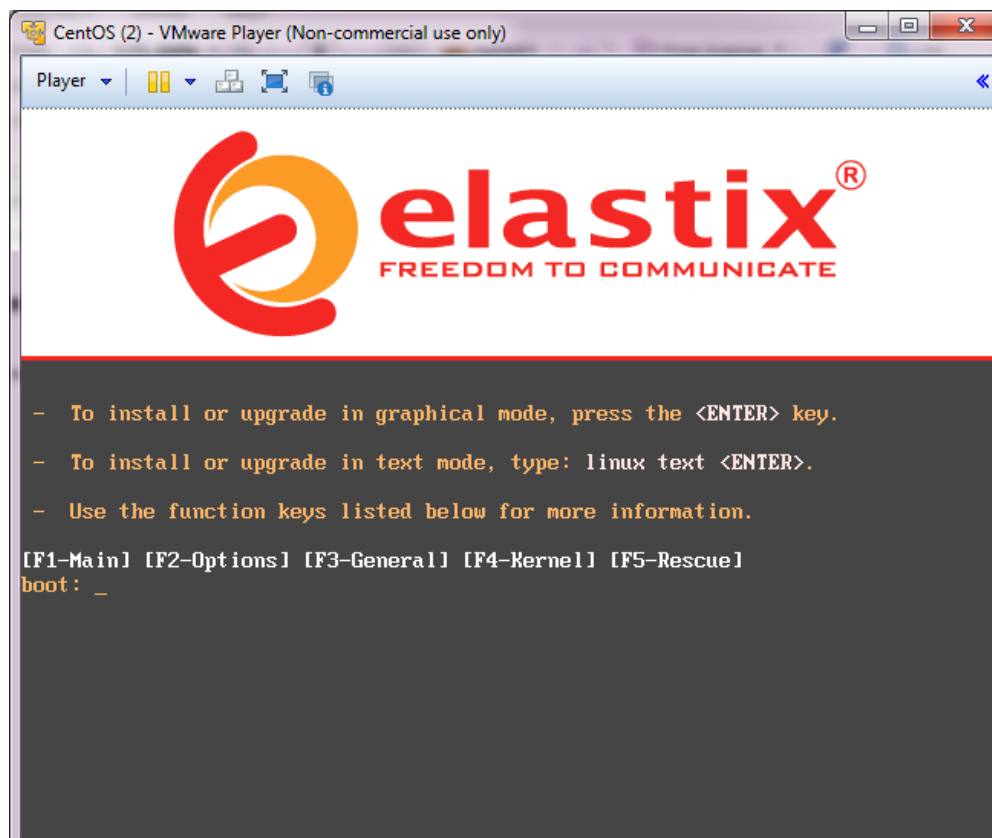


Рис. 5.4 Установка Elastix – Экран приветствия

- 4) Для продолжения установки нажмите клавишу Enter
- 5) Как только закончится анализ системы, начнётся процесс установки.
 - Выберите *English* в качестве языка по умолчанию;
 - Тип клавиатуры – us;
 - Partition type - remove all partitions on selected drives and create default layout;
 - Откажитесь от ручной конфигурации *eth0*;
 - Оставьте значения адреса шлюза и DNS пустыми;
 - В разделе Hostname configuration введите имя хоста в виде; StudXY, по аналогии с именем виртуальной машины;
 - В разделе Time Zone Configuration выбираем нужный нам часовой пояс;
 - При настройке Root Password – придумайте пароль администратора и запомните его;
 - В процессе установки придумайте пароль MySQL и пароль freePBX, который понадобится для входа в графический интерфейс Elastix.

- 6) По окончании установки, вы автоматически попадёте в консоль Elastix, войдите как администратор (user: root, password: задан в процессе установки). Сделайте скриншот.

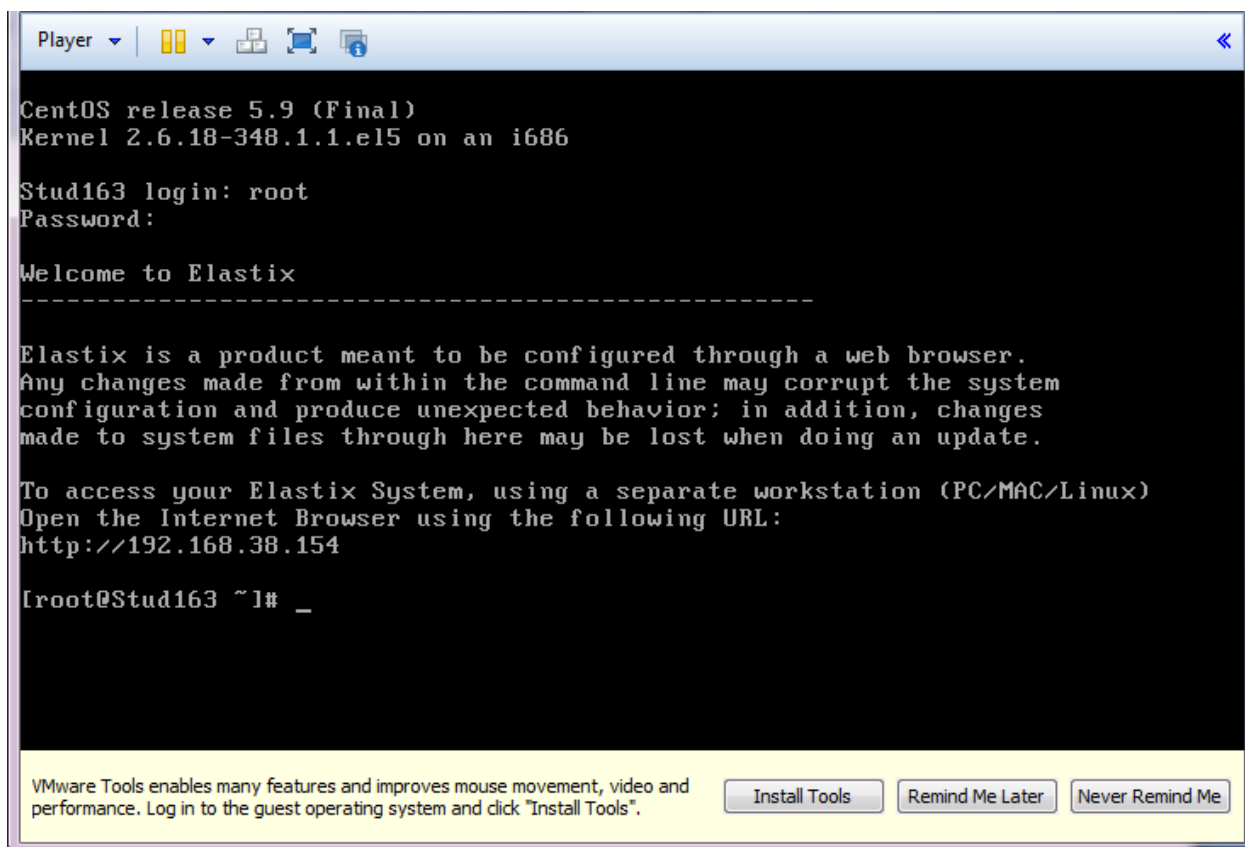


Рис. 5.5 Консоль Elastix

Часть вторая – настройка Elastix

- 1) Через браузер вы сможете зайти по адресу <https://ipaddress/> (например <http://192.168.38.154>) и попадёте на экран входа в веб-интерфейс. Когда вы введёте логин и пароль (user:admin, password: задан при установке), произойдёт вход в System centre Elastix. Сделайте скриншот.

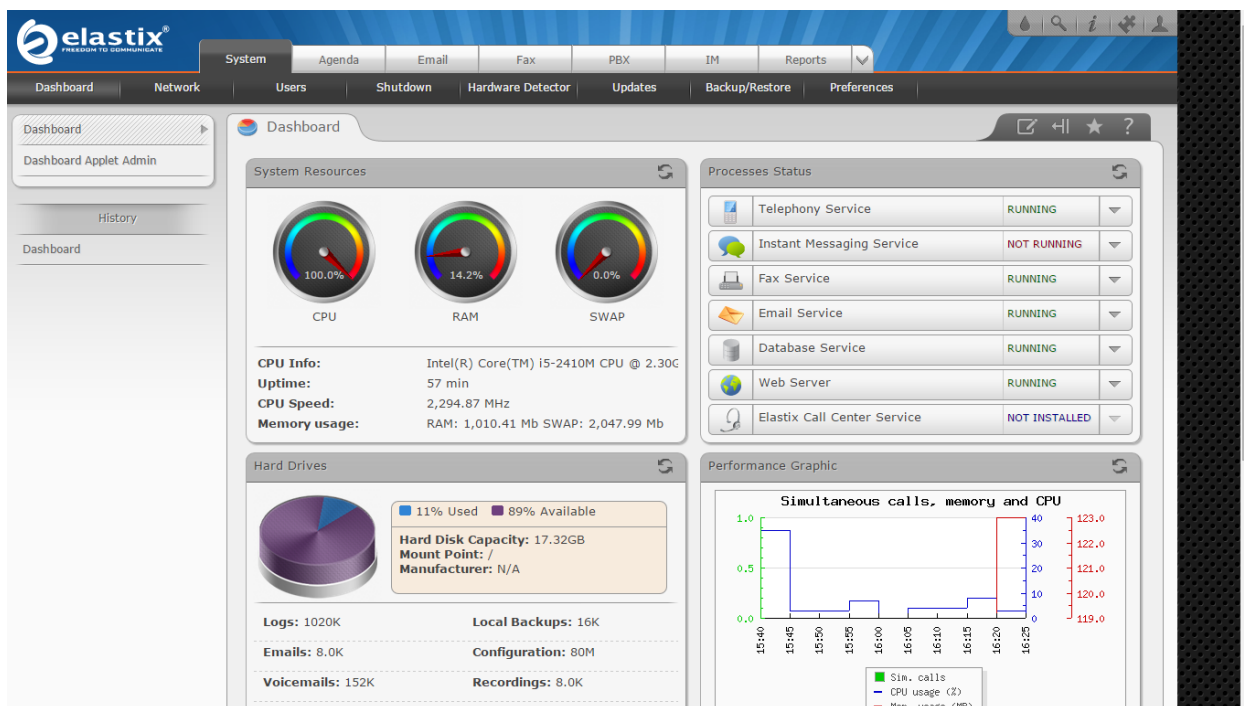


Рис. 5.6 Экран System Status

System status выводит информацию о используемых ресурсах и активности Elastix. Прежде чем пользоваться возможностями IP телефонии, нужно настроить Elastix. В данной лабораторной работе мы будем иметь дело только с базовыми настройками, которые потребуются для простого звонка между двумя абонентами.

2) Добавление пользователей

Перейдите во вкладку PBX. В этой вкладке происходит добавление новых пользователей и конфигурация PBX. Оставьте все настройки по умолчанию и сразу перейдем к настройке пользователей. Оставьте вид устройства “Generic SIP Device”. Нажмите Submit.

Вам предстоит заполнить следующие поля

- 1) User Extension – номер клиента. В нашем случае четырехзначный номер вида 1X0Y, где X – номер бригады, а Y – номер;
- 2) Display Name – имя клиента, которое будет выводиться при звонке;
- 3) Secret – пароль клиента.

Остальные поля оставить по умолчанию.

Add Extension

User Extension: 1311

Display Name: Andrei

CID Num Alias:

SIP Alias:

Extension Options

Outbound CID:

Ring Time: Default ▼

Call Waiting: Disable ▼

Call Screening: Disable ▼

Pinless Dialing: Disable ▼

Emergency CID:

Assigned DID/CID

DID Description:

Add Inbound DID:

Add Inbound CID:

Device Options

This device uses sip technology.

secret: password1311

dtmfmode: rfc2833

Рис. 5.7 Добавления абонента

Повторите операции, в зависимости от количества человек в бригаде. Сделайте скриншот настроек для одного пользователя.

Существует также быстрый способ добавления множества пользователей. Этот инструмент позволяет использовать электронные таблицы для настройки пользователей, а затем выгрузить их в Эластикс. Благодаря чему, они все появятся в системе.

Предполагается, что вы уже создали как минимум двух пользователей. Выберите вкладку PBX=>Batch configurations и нажмите на *Download the current extensions in CSV format*. На жёсткий диск загрузится файл с расширением .csv, который можно открыть любым редактором таблиц.

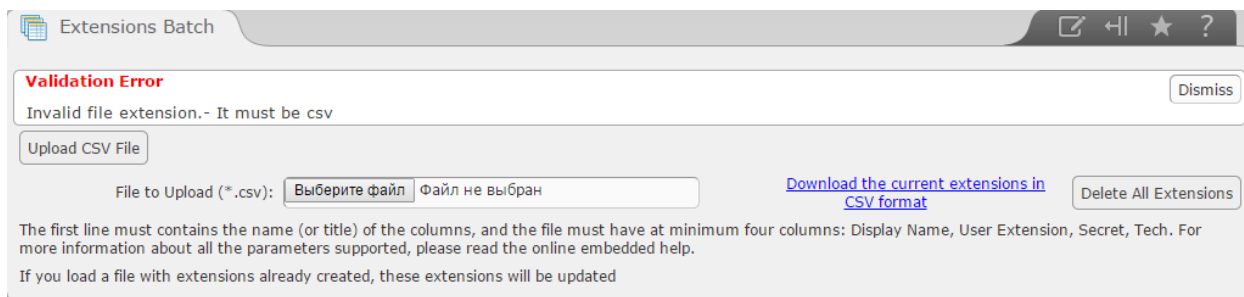


Рис. 5.8 Extensions Batch

В таблице вы должны увидеть созданные профили пользователей. Руководствуясь примером, вы можете добавить новых пользователей. Этот метод более эффективен при большом количестве пользователей, с приблизительно одинаковыми настройками и позволяет сэкономить много времени. Отредактированный файл сохраняется в формате .csv выбирается в поле “File to upload” и загружается в Elastix нажатием кнопки “Upload CSV File”.

После добавления трёх пользователей заполните следующую таблицу:

Таблица 5.2

Extension 1	Extension 2	Extension 3
Extension Number_____	Extension Number_____	Extension Number_____
Extension Password_____	Extension Password_____	Extension Password_____
Extension Name _____	Extension Name _____	Extension Name _____

Часть третья – настройка Phoner

- 1) Запустите программу Phoner и во вкладке Options выберите пункт Communications. На каждом компьютере настройте своего пользователя.

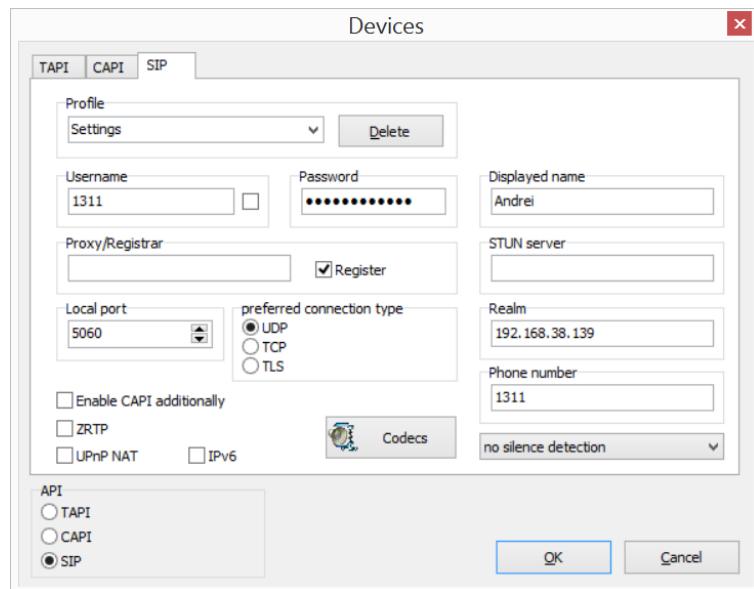


Рис. 5.9 Настройка Phoner

- 2) Сделайте скриншот настроек для любого пользователя. Если всё правильно, то в окне Phoner появится надпись вида (sip:1311@192.168.38.139 registered)

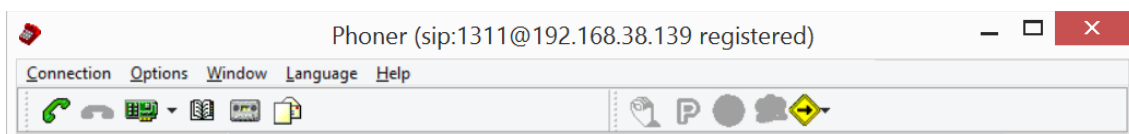


Рис. 5.10 Успешная регистрация

- 3) Запустите Wireshark, выберите основной интерфейс и начните захват пакетов с него.

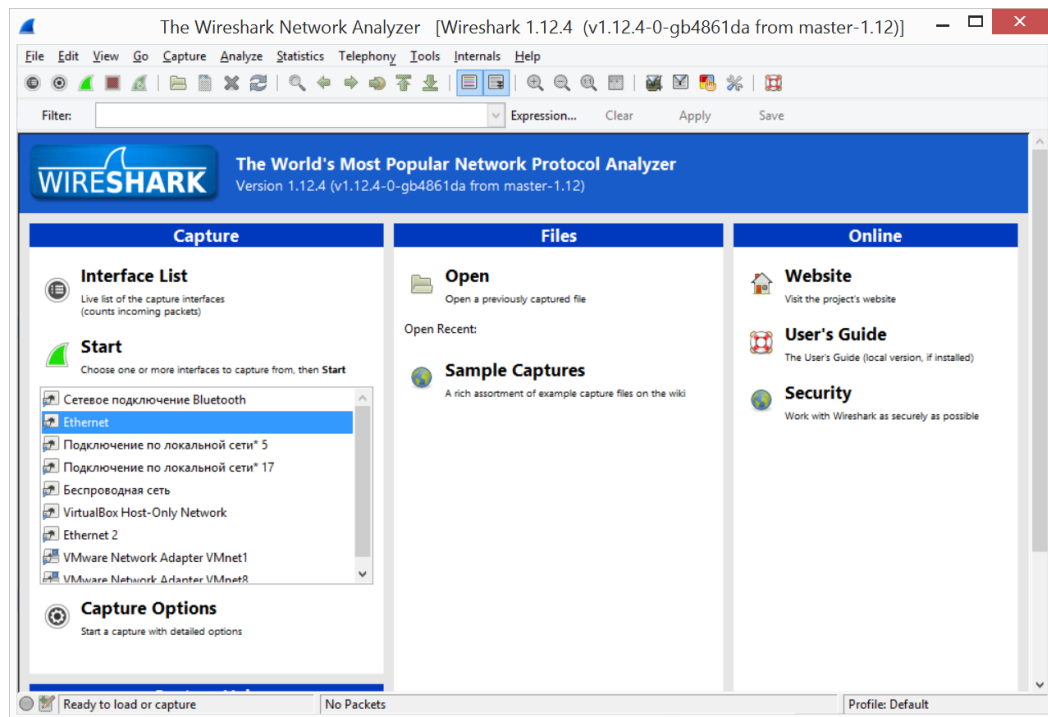


Рис. 5.11 Основное окно wireshark

- 4) Совершите звонок с ПК1 на ПК2 через phoner. По его окончании, остановите захват пакетов в wireshark. В поле “Filter” наберите SIP, чтобы отсортировать и вывести пакеты данного протокола. Сделайте скриншот и сохраните дамп (File-Save as)

*Ethernet [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

No.	Time	Source	Destination	Protocol	Length	Info
233	18.8413900	192.168.38.139	192.168.38.131	SIP	599	Request: OPTIONS sip:4001@192.168.38.131:5060
234	18.8440990	192.168.38.131	192.168.38.139	SIP	508	Status: 200 OK
272	24.4906520	192.168.38.161	192.168.38.131	SIP/SDF	1153	Request: INVITE sip:4001@192.168.38.139
275	24.5000670	192.168.38.131	192.168.38.161	SIP	445	Status: 100 Trying
276	24.5449490	192.168.38.131	192.168.38.161	SIP	519	Status: 180 Ringing
297	28.1527730	192.168.38.161	192.168.38.161	SIP/SDF	1061	Status: 200 OK
298	28.1557160	192.168.38.161	192.168.38.139	SIP	450	Request: ACK sip:4001@192.168.38.139
1568	40.1382950	192.168.38.139	192.168.38.161	SIP	599	Request: OPTIONS sip:1311@192.168.38.161:5060
1569	40.1390590	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK
1573	40.1712410	192.168.38.161	192.168.38.139	SIP	481	Request: BYE sip:4001@192.168.38.139
1574	40.1714850	192.168.38.139	192.168.38.161	SIP	573	Status: 481 call leg/transaction does not exist
2361	53.0247720	192.168.38.131	192.168.38.161	SIP	481	Request: BYE sip:1311@192.168.38.161:5060
2362	53.0253920	192.168.38.161	192.168.38.131	SIP	443	Status: 200 OK

Рис. 5.12 Скриншот пакетов SIP

- 5) Используя меню Wireshark, проверьте VoIP запись звонка в дампе.

Для этого в разделе Telephony выбираем пункт VoIP Calls. Используя кнопку “Flow” – проверить обмен SIP message пакетами. Сделайте скриншот. Используя “Player” – прослушать записанный звонок. Сделайте скриншот записи прослушанного звонка.

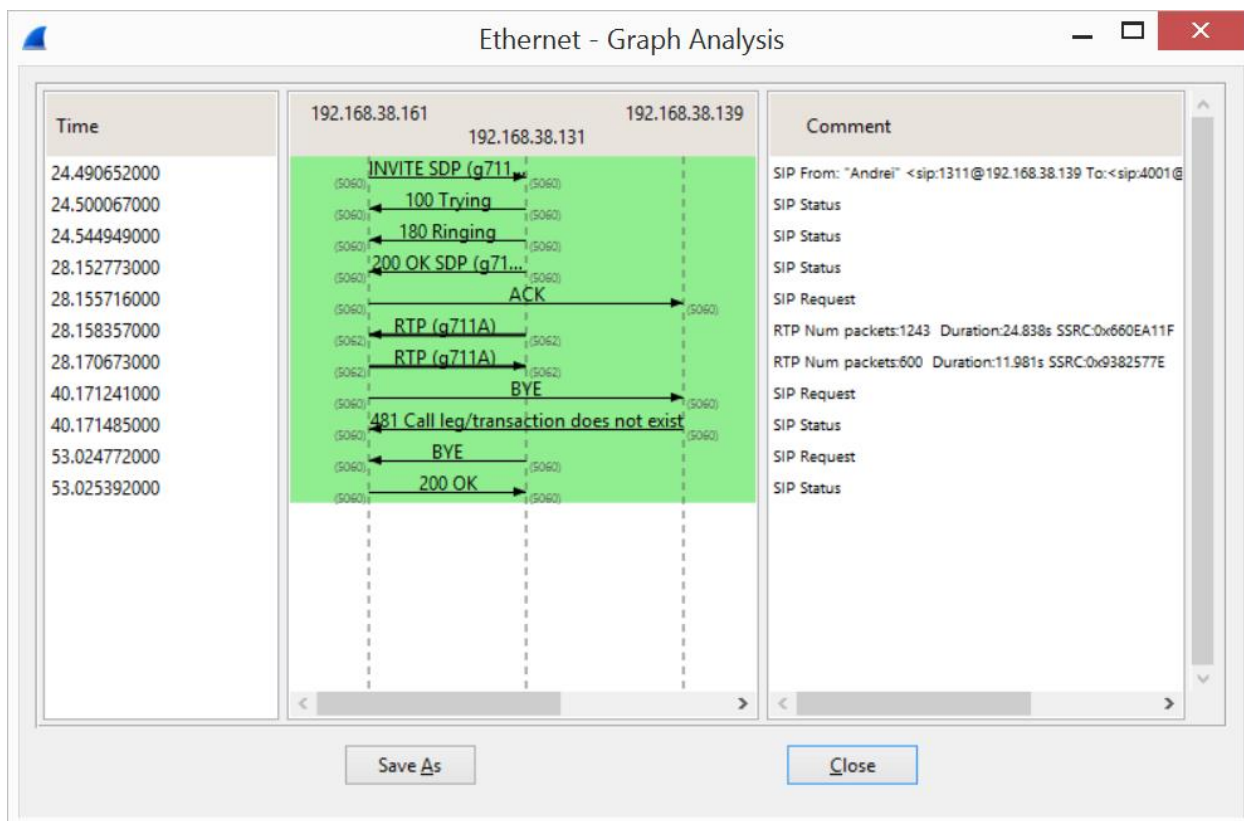


Рис. 5.13 Анализ Flow

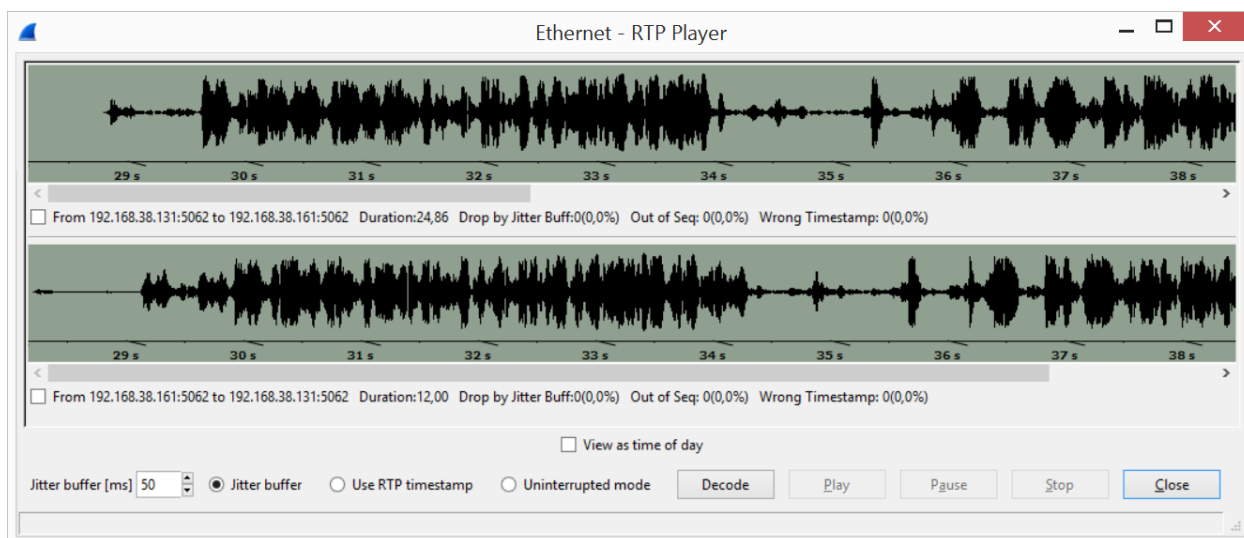


Рис. 5.14 RTP player

Содержание отчёта:

- 1) Титульный лист;
- 2) Цель работы;

- 3) Скриншоты: Установка Elastix, добавление пользователей, настройка phoner, дампы Wireshark.
- 4) Выводы о проделанной работе

Контрольные вопросы:

- 1) Установка Elastix
- 2) Протоколы: SIP, RTP.
- 3) Анализ дампа Wireshark

5.2 Лабораторная работа №2. Использование встроенного Firewall'a

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

Подготовка к лабораторной работе: У каждой бригады должно быть 2 ПК с установленными программами Phoner и Wireshark. Один из ПК должен иметь предустановленный Elastix PBX, на котором зарегистрировано, как минимум, 2 пользователя.

Таблица 5.3

ПК1 IP адрес: _____ MAC адрес: _____ Номер SIP: _____	ПК2 IP адрес: _____ MAC адрес: _____ Номер SIP: _____
IP адрес сервера Elastix: _____	

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

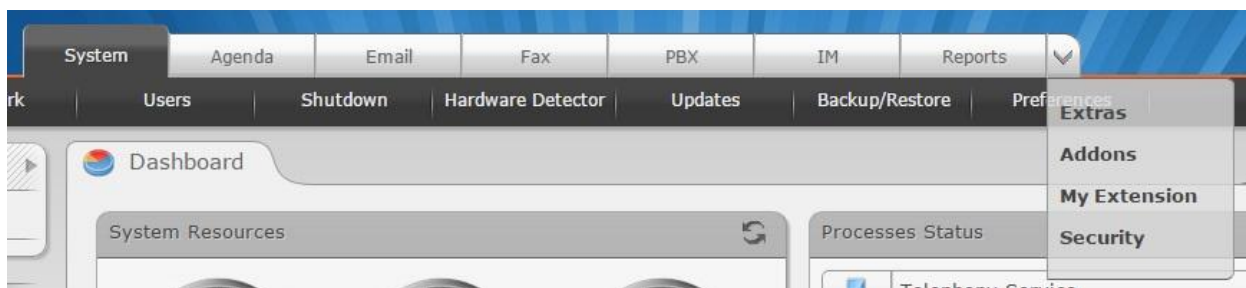


Рис. 5.15 Опция Security

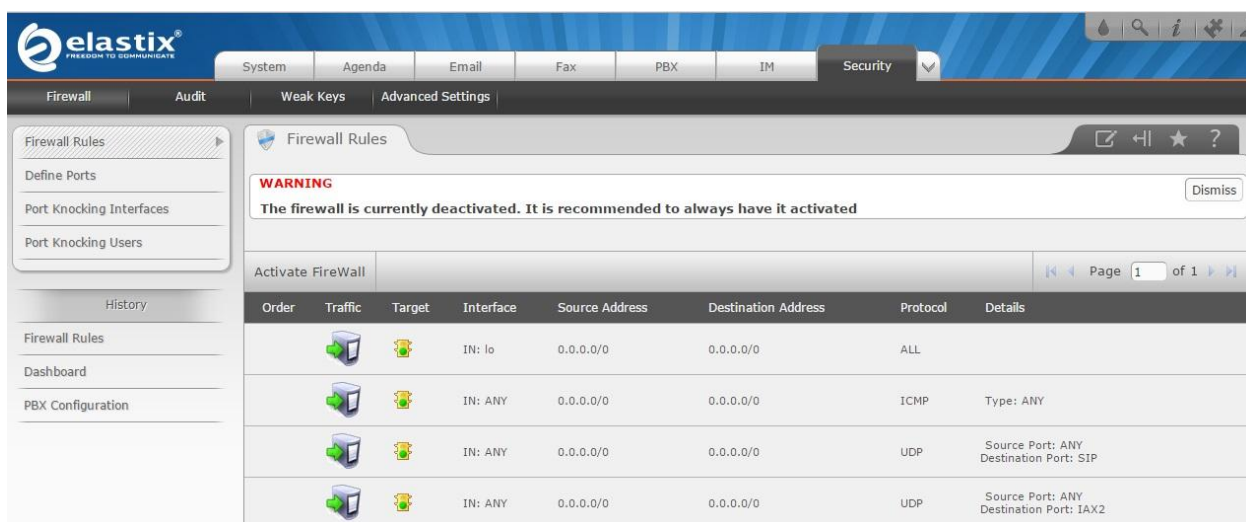


Рис. 5.16 Включение Firewall

- 3) Включите firewall, нажав на кнопку “Activate Firewall”.
- 4) Перед вами начальная установка firewall. Elastix уже имеет набор правил по умолчанию, которые охватывают все установленные компоненты системы. Сами по себе они не предоставляют защиты, так как принимают трафик к элементам данного списка из любой сети. Тем не менее, любой трафик, не представленный в данном списке, будет остановлен.

Order	Traffic	Target	Interface	Source Address	Destination Address	Protocol	Details
1			IN: In	0.0.0.0/0	0.0.0.0/0	ALL	
2			IN: ANY	0.0.0.0/0	0.0.0.0/0	ICMP	Type: ANY
3			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: SIP
4			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: JAX2
5			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: JAX3
6			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: RTP
7			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: MGCP
8			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: DNS Destination Port: ANY
9			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: TFTP
10			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: SSH
11			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: SMTP
12			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: HTTP
13			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: POP3
14			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: IMAP
15			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: HTTPS
16			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: IMAPS
17			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: POP3S
18			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: JABBER/KNIP
19			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: OpenFire
20			IN: ANY	0.0.0.0/0	0.0.0.0/0	STATE	Established,Related
21			IN: ANY	0.0.0.0/0	0.0.0.0/0	ALL	
22			IN: ANY OUT: ANY	0.0.0.0/0	0.0.0.0/0	ALL	

Рис. 5.17 Default Firewall

Данные правила являются стандартным набором для Elastix. Сделайте скриншот всех правил. Когда вы захотите удалить лишние правила, вернуться к настройкам по умолчанию – данный скриншот будет служить вам примером.

- Синие стрелки позволяют менять очерёдность правил;
- Зелёная стрелка на компьютере показывает, что трафик является входящим. Т.е. он установлен как трафик INPUT, пакеты идут в систему;
- Также может быть тип FORWARD – пакеты проходят через систему Elastix, или OUTPUT – исходящие пакеты;
- Зелёный цвет светофора, означает что для данного правила происходит действие АССЕРТ;
- Interface – к какому интерфейсу применяется правило. По умолчанию, ANY, т.е к любому;
- Source address – адрес источника. Изначально, любой IP адрес может получить доступ к системе Elastix;
- Destination address – обычно применяется для исходящих правил;
- Информация о протоколе и используемом порте;
- Лампочка показывает, активно ли данное правило.

5) Выберите в левом меню Define ports.

Как видно, номера портов настроены по умолчанию, при установке Elastix. Нажав на *view* в строке нужного порта, вы сможете узнать более подробную информацию. Если понадобится, номера портов можно изменить именно в этом меню. Сделайте скриншот со списком портов.

	Name	Protocol	Details
<input type="checkbox"/>	HTTP	TCP	Port 80
<input type="checkbox"/>	HTTPS	TCP	Port 443
<input type="checkbox"/>	POP3	TCP	Port 110
<input type="checkbox"/>	IMAPS	TCP	Port 993
<input type="checkbox"/>	SSH	TCP	Port 22
<input type="checkbox"/>	SMTP	TCP	Port 25
<input type="checkbox"/>	POP3S	TCP	Port 995
<input type="checkbox"/>	JABBER/XMPP	TCP	Port 5222
<input type="checkbox"/>	OpenFire	TCP	Port 9090
<input type="checkbox"/>	IMAP	TCP	Port 143
<input type="checkbox"/>	SIP	UDP	Ports 5004:5082
<input type="checkbox"/>	RTP	UDP	Ports 10000:20000
<input type="checkbox"/>	MGCP	UDP	Port 2727
<input type="checkbox"/>	IAX2	UDP	Port 4569
<input type="checkbox"/>	IAX1	UDP	Port 5036
<input type="checkbox"/>	DNS	UDP	Port 53
<input type="checkbox"/>	TFTP	UDP	Port 69

Рис. 5.18 Define ports

The screenshot shows the 'Edit Port' window. The 'Name' field is 'RTP'. The 'Protocol' dropdown is open with 'UDP' selected. The 'Port' field is '20000'. The 'Comment' field is empty. Buttons for 'Save' and 'Cancel' are at the top.

Рис. 5.19 Редактирование порта

Протокол для данного порта установлен на прохождение только UDP трафика, поэтому если кто-то попытается подсоединиться по TCP к портам от 10000 до 20000, Firewall этого не позволит.

Имеются четыре опции:

- TCP – прохождение только TCP трафика через данный порт. Обычно используется для HTTP, HTTPS;
- UDP – прохождение только UDP трафика через данный порт. В основном используется протоколами SIP, RTP;
- ICMP – прохождение пакетов вида Internet Control Message Protocol. К таким относятся ping, TraceRoute и т.д. То есть данные пакеты переносят не полезную нагрузку, а информацию о статусе сети;
- IP – применяется крайне редко, в случае когда приходится использовать номер протокола, а не номер порта.

Часть вторая: настройка Firewall

1) Ограничьте доступ по SSH

Скачайте Putty на ПК2 и зайдите на сервер Elastix, по его ip адресу. Введите логин и пароль для root, сделайте скриншот.

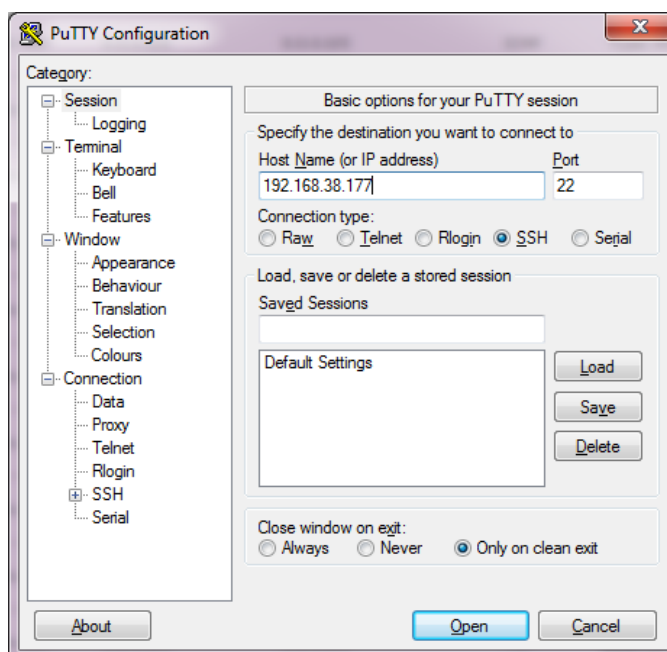


Рис. 5.20 Putty

- 2) Теперь настройте firewall так, чтобы доступ к серверу по SSH был доступен только с ПК1.

Отредактируйте 10 правило в Firewall rules. Нажмите на кнопку EDIT.

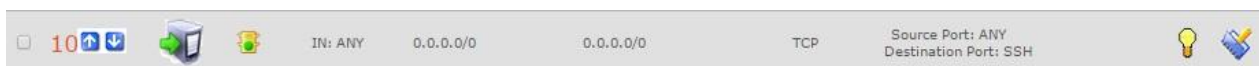


Рис. 5.21 Строка порта SSH

Предоставьте доступ по SSH только ПК1, только с его ip адреса. Нужно изменить поле “source address” прописав нужный ip адрес и маску.

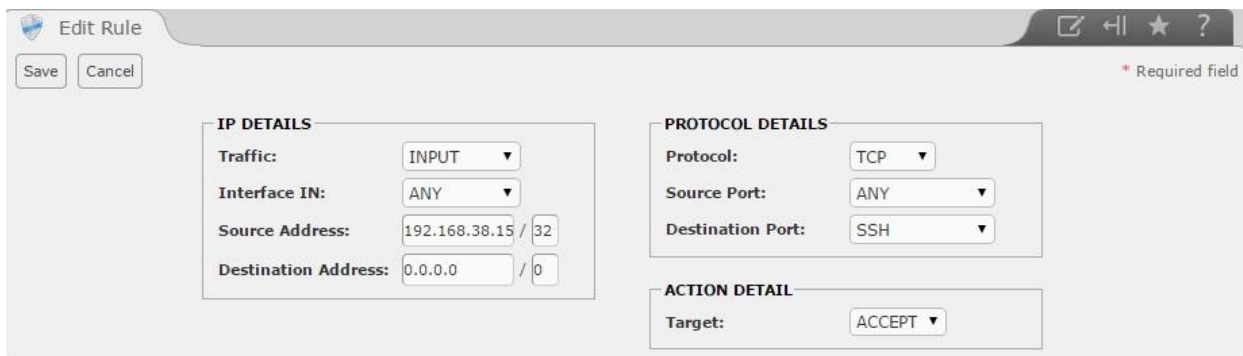


Рис. 5.22 Изменение правила

Заметьте, что в конце адреса маска /32. Источником может являться один единственный IP адрес. Такая запись аналогична 192.168.38.155/255.255.255.255. Если же вы хотите разрешить доступ только из определённой подсети, то следует записать 192.168.38.155/24, что аналогично 192.168.38.155/255.255.255.0. Тогда любой адрес вида 192.168.38.XX может осуществить доступ по SSH. Не забудьте нажать на save changes, когда измените правило и попадёте в окно “Firewall rules”

3) Запустите Wireshark и снимите дамп при доступе по SSH с одобренного и с запрещённого адреса. Сохраните данные дампы.

Filter:		ip.dst == 192.168.38.139 or ip.src == 192.168.38.139		Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
5	0.51798800	192.168.38.139	94.100.207.29	NTP	90	NTP Version 4, client	
8	2.79747200	192.168.38.161	192.168.38.139	TCP	66	58950->22 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK	
9	2.79822300	192.168.38.139	192.168.38.161	ICMP	94	Destination unreachable (Port unreachable)	
12	3.51868200	192.168.38.139	195.3.254.2	NTP	90	NTP Version 4, client	
16	4.51861900	192.168.38.139	93.180.6.3	NTP	90	NTP Version 4, client	
30	5.79170700	192.168.38.161	192.168.38.139	TCP	66	[TCP Retransmission] 58950->22 [SYN] Seq=0 win=8192 Len=0	
31	5.79209600	192.168.38.139	192.168.38.161	ICMP	94	Destination unreachable (Port unreachable)	
55	11.79746900	192.168.38.161	192.168.38.139	TCP	62	[TCP Retransmission] 58950->22 [SYN] Seq=0 win=8192 Len=0	
56	11.79782300	192.168.38.139	192.168.38.161	ICMP	90	Destination unreachable (Port unreachable)	

Рис. 5.23 Попытка доступа по SSH с запрещённого адреса

Filter:	ip.dst == 192.168.38.139 or ip.src == 192.168.38.139	Expression...	Clear	Apply	Save
Time	Source	Destination	Protocol	Length	Info
33	5.64619400	192.168.38.161	TCP	66	58922->22 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
34	5.64654600	192.168.38.139	TCP	66	22->58922 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1
35	5.64660700	192.168.38.161	TCP	54	58922->22 [ACK] Seq=1 Ack=1 win=65536 Len=0
36	5.65075900	192.168.38.161	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.64)
37	5.65125100	192.168.38.139	TCP	54	22->58922 [ACK] Seq=1 Ack=29 win=5888 Len=0
38	5.65836200	192.168.38.139	SSHv2	74	Server: Protocol (SSH-2.0-OpenSSH_4.3)
39	5.65855500	192.168.38.161	SSHv2	726	Client: Key Exchange Init
40	5.65959300	192.168.38.139	SSHv2	758	Server: Key Exchange Init
41	5.65972500	192.168.38.161	SSHv2	70	Client: Diffie-Hellman Group Exchange Request (old)
42	5.66200700	192.168.38.139	SSHv2	334	Server: Diffie-Hellman Group Exchange Group
43	5.68658900	192.168.38.161	SSHv2	326	Client: Diffie-Hellman Group Exchange Init
44	5.72626100	192.168.38.139	TCP	54	22->58922 [ACK] Seq=1005 Ack=989 win=8576 Len=0
45	5.73014600	192.168.38.139	SSHv2	902	Server: Diffie-Hellman Group Exchange Reply, New Keys
46	5.75632400	192.168.38.161	SSHv2	70	Client: New Keys
47	5.75644600	192.168.38.139	TCP	54	22->58922 [ACK] Seq=1853 Ack=1005 win=8576 Len=0
48	5.75651600	192.168.38.161	SSHv2	106	Client: Encrypted packet (len=52)
49	5.75657100	192.168.38.139	TCP	54	22->58922 [ACK] Seq=1853 Ack=1057 win=8576 Len=0
50	5.75669900	192.168.38.139	SSHv2	106	Server: Encrypted packet (len=52)
51	5.80028400	192.168.38.161	TCP	54	58922->22 [ACK] Seq=1057 Ack=1905 win=65536 Len=0
58	7.94854600	192.168.38.161	SSHv2	122	Client: Encrypted packet (len=68)
59	7.94918000	192.168.38.139	SSHv2	138	Server: Encrypted packet (len=84)
60	7.94940800	192.168.38.161	SSHv2	154	Client: Encrypted packet (len=100)
61	7.98898500	192.168.38.139	TCP	54	22->58922 [ACK] Seq=1989 Ack=1225 win=8576 Len=0
62	7.99536600	192.168.38.139	DNS	87	Standard query 0xfdd3 PTR 161.38.168.192.in-addr.arpa
63	7.99626500	192.168.38.161	DNS	132	Standard query response 0xfdd3 No such name
64	7.99759900	192.168.38.139	SSHv2	138	Server: Encrypted packet (len=84)
65	8.04908500	192.168.38.161	TCP	54	58922->22 [ACK] Seq=1225 Ack=2073 win=65280 Len=0
69	9.75764400	192.168.38.161	SSHv2	350	Client: Encrypted packet (len=296)
70	9.75779700	192.168.38.139	TCP	54	22->58922 [ACK] Seq=2073 Ack=1521 win=9984 Len=0
71	9.75872500	192.168.38.139	SSHv2	90	Server: Encrypted packet (len=36)
72	9.75883500	192.168.38.161	SSHv2	122	Client: Encrypted packet (len=68)
73	9.76226800	192.168.38.139	SSHv2	106	Server: Encrypted packet (len=52)
74	9.76245700	192.168.38.161	SSHv2	154	Client: Encrypted packet (len=100)
75	9.76258600	192.168.38.161	SSHv2	106	Client: Encrypted packet (len=52)
76	9.76301500	192.168.38.139	TCP	54	22->58922 [ACK] Seq=2161 Ack=1741 win=9984 Len=0
77	9.76309200	192.168.38.161	SSHv2	90	Server: Encrypted packet (len=36)
78	9.76993800	192.168.38.139	SSHv2	142	Server: Encrypted packet (len=88)
79	9.76998000	192.168.38.161	TCP	54	58922->22 [ACK] Seq=1741 Ack=2285 win=65024 Len=0
80	9.77013800	192.168.38.139	SSHv2	650	Server: Encrypted packet (len=596)
81	9.80438500	192.168.38.161	SSHv2	122	Server: Encrypted packet (len=68)
82	9.80442700	192.168.38.139	TCP	54	58922->22 [ACK] Seq=1741 Ack=2949 win=64512 Len=0
83	9.80739600	192.168.38.139	SSHv2	122	Server: Encrypted packet (len=68)
84	9.85724000	192.168.38.161	TCP	54	58922->22 [ACK] Seq=1741 Ack=3017 win=64512 Len=0

Рис. 5.24 Доступ по SSH с разрешённого адреса

- 4) Настройте протокол Https аналогично, чтобы доступ имел только ПК2. Сделайте скриншоты настроек и дампа в wireshark при правоммерном и запрещённом доступе.

Filter:	ip.dst == 192.168.38.139	Expression...	Clear	Apply	Save	
No.	Time	Source	Destination	Protocol	Length	Info
18	5.16220400	192.168.38.155	192.168.38.139	TCP	66	62849->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	5.16305200	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
25	5.41265600	192.168.38.155	192.168.38.139	TCP	66	62851->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	5.41332700	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
32	8.15927000	192.168.38.155	192.168.38.139	TCP	66	[TCP Retransmission] 62849->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
33	8.15974700	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
37	8.41216800	192.168.38.155	192.168.38.139	TCP	66	[TCP Retransmission] 62851->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
38	8.41267000	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
60	14.15940600	192.168.38.155	192.168.38.139	TCP	62	[TCP Retransmission] 62849->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61	14.15990500	192.168.38.139	192.168.38.155	ICMP	90	Destination unreachable (Port unreachable)
67	14.41045700	192.168.38.155	192.168.38.139	TCP	62	[TCP Retransmission] 62851->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
68	14.41091400	192.168.38.139	192.168.38.155	ICMP	90	Destination unreachable (Port unreachable)
128	26.33666500	192.168.38.155	192.168.38.139	TCP	66	62862->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
129	26.33714100	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
150	29.35742500	192.168.38.155	192.168.38.139	TCP	66	[TCP Retransmission] 62862->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
152	29.35800600	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
160	31.42163500	192.168.38.155	192.168.38.139	TCP	66	62864->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
161	31.42214200	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
176	34.42400000	192.168.38.155	192.168.38.139	TCP	66	[TCP Retransmission] 62864->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
177	34.42469700	192.168.38.139	192.168.38.155	ICMP	94	Destination unreachable (Port unreachable)
188	35.36095600	192.168.38.155	192.168.38.139	TCP	62	[TCP Retransmission] 62862->443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
189	35.36141500	192.168.38.139	192.168.38.155	ICMP	90	Destination unreachable (Port unreachable)

Рис. 5.26 Доступ по https с запрещённого адреса

59	3.60400400	Dell_df:9c:1c	Broadcast	ARP	42	Who has 192.168.38.139? Tell 192.168.38.155
60	3.60437800	Vmware_de:d6:86	Dell_df:9c:1c	ARP	60	192.168.38.139 is at 00:0c:29:de:d6:86
61	3.60440800	192.168.38.155	192.168.38.139	TCP	66	62322->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
62	3.60528200	192.168.38.139	192.168.38.155	TCP	66	80->62322 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
63	3.60545700	192.168.38.155	192.168.38.139	TCP	54	62322->80 [ACK] Seq=1 Ack=1 win=65536 Len=0
64	3.60573500	192.168.38.155	192.168.38.139	TCP	66	62323->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
65	3.60614000	192.168.38.139	192.168.38.155	TCP	66	443->62323 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
66	3.60630000	192.168.38.155	192.168.38.139	TCP	54	62323->443 [ACK] Seq=1 Ack=1 win=65536 Len=0
67	3.60631200	192.168.38.155	192.168.38.139	TCP	66	62324->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
68	3.60694400	192.168.38.155	192.168.38.139	TCP	66	62325->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
69	3.60699700	192.168.38.139	192.168.38.155	TCP	66	443->62324 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
70	3.60713700	192.168.38.155	192.168.38.139	TCP	54	62324->443 [ACK] Seq=1 Ack=1 win=65536 Len=0
71	3.60775300	192.168.38.155	192.168.38.139	TCP	66	62326->443 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	3.60804300	192.168.38.139	192.168.38.155	TCP	66	443->62325 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
73	3.60818700	192.168.38.155	192.168.38.139	TCP	54	62325->443 [ACK] Seq=1 Ack=1 win=65536 Len=0
74	3.60873500	192.168.38.139	192.168.38.155	TCP	66	443->62326 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
75	3.60889300	192.168.38.155	192.168.38.139	TCP	54	62326->443 [ACK] Seq=1 Ack=1 win=65536 Len=0
76	3.61491500	192.168.38.155	192.168.38.139	TLsv1	255	Client Hello
77	3.61533200	192.168.38.139	192.168.38.155	TCP	60	443->62324 [ACK] Seq=1 Ack=202 win=6912 Len=0
78	3.61654400	192.168.38.155	192.168.38.139	TLsv1	255	Client Hello
79	3.61716900	192.168.38.139	192.168.38.155	TCP	60	443->62326 [ACK] Seq=1 Ack=202 win=6912 Len=0
80	3.61966900	192.168.38.155	192.168.38.139	TLsv1	255	Client Hello
81	3.61980900	192.168.38.155	192.168.38.139	TLsv1	255	Client Hello

Рис. 5.27 Доступ по https с разрешённого адреса.

- 5) Запретите регистрацию абонентов с определённого адреса. Отредактируйте правила для протокола SIP, чтобы происходил REJECT при попытке регистрации в phoner. Аналогично снимите дампы успешной и безуспешной регистрации.

Filter: ip.dst == 192.168.38.139							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
7	1.30119500	192.168.38.161	192.168.38.139	ICMP	590	Destination unreachable (Port unreachable)				
22	2.90799000	192.168.38.161	192.168.38.139	SIP	645	Request: REGISTER sip:192.168.38.139 (1 binding)				
25	2.90973700	192.168.38.161	192.168.38.139	SIP	806	Request: REGISTER sip:192.168.38.139 (1 binding)				
28	2.91040900	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
30	2.91070800	192.168.38.161	192.168.38.139	SIP	507	Status: 200 OK				
36	3.71401900	192.168.38.161	192.168.38.139	SIP	602	Request: SUBSCRIBE sip:1311@192.168.38.139				
38	3.71465200	192.168.38.161	192.168.38.139	SIP	768	Request: SUBSCRIBE sip:1311@192.168.38.139				
41	3.71531700	192.168.38.161	192.168.38.139	SIP	483	Status: 200 OK				

Рис. 5.28 Успешная регистрация по SIP

Filter: ip.dst == 192.168.38.139							Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info				
27	6.44122700	192.168.38.161	192.168.38.139	ICMP	590	Destination unreachable (Port unreachable)				
29	7.07754600	192.168.38.161	192.168.38.139	SIP	645	Request: REGISTER sip:192.168.38.139 (1 binding)				
30	7.07771500	192.168.38.139	192.168.38.161	ICMP	590	Destination unreachable (Port unreachable)				
33	7.44104700	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
34	7.44117000	192.168.38.139	192.168.38.161	ICMP	536	Destination unreachable (Port unreachable)				
35	7.79268400	192.168.38.161	192.168.38.139	SIP	603	Request: SUBSCRIBE sip:1311@192.168.38.139				
36	7.79289600	192.168.38.139	192.168.38.161	ICMP	590	Destination unreachable (Port unreachable)				
46	8.44121100	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
47	8.44255100	192.168.38.139	192.168.38.161	ICMP	536	Destination unreachable (Port unreachable)				
50	9.44066700	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
51	9.44096000	192.168.38.139	192.168.38.161	ICMP	536	Destination unreachable (Port unreachable)				
54	10.44247200	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
55	10.44292400	192.168.38.139	192.168.38.161	ICMP	536	Destination unreachable (Port unreachable)				
89	17.11518300	192.168.38.155	192.168.38.139	SIP	508	Status: 200 OK				
116	20.44261300	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
117	20.44281800	192.168.38.139	192.168.38.161	ICMP	536	Destination unreachable (Port unreachable)				
122	21.44243200	192.168.38.161	192.168.38.139	SIP	508	Status: 200 OK				
123	21.44272400	192.168.38.139	192.168.38.161	ICMP	536	Destination unreachable (Port unreachable)				

Рис. 5.29 Неудачная попытка регистрации

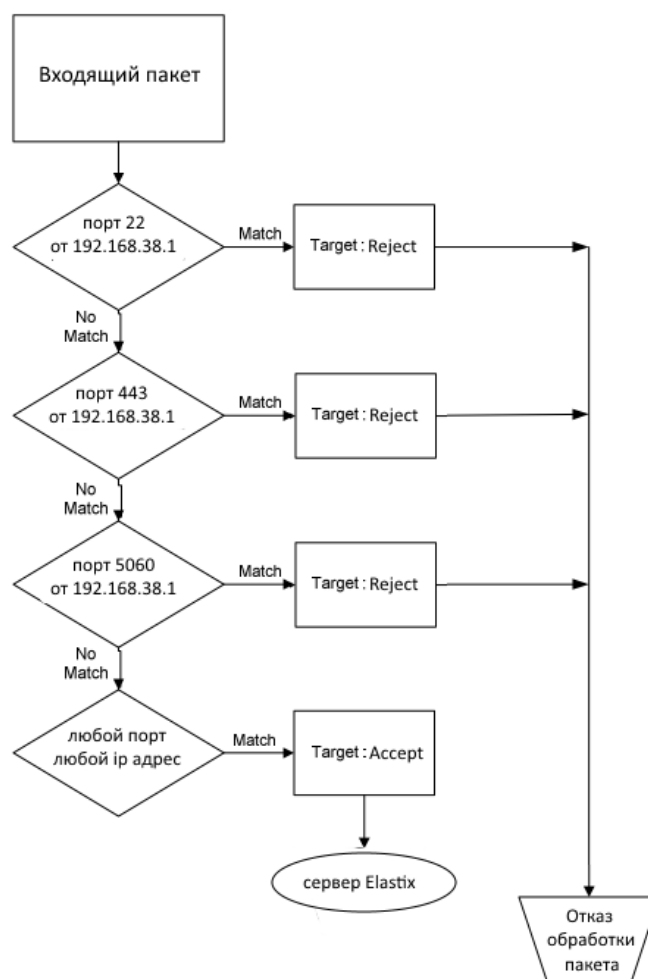


Рис. 5.30 Блок схема работы firewall'a

Содержание отчёта:

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

5.3 Лабораторная работа №3. Настройка протокола SRTP и TLS в ОС Elastix.

Цель работы: Настроить защищённое соединение между двумя абонентами с применением протоколов SRTP и TLS. Убедиться в том, что данный вид связи шифрует как сессию, так и непосредственно голос.

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

Таблица 5.4

ПК1 Ip адрес: _____ MAC адрес: _____ Номер SIP: _____	ПК2 Ip адрес: _____ MAC адрес: _____ Номер SIP: _____
IP адрес сервера Elastix: _____	

Порядок выполнения лабораторной работы:

Часть первая: Создание сертификатов.

- 1) Включите виртуальную машину с Elastix и зайдите как root.
- 2) Создайте директорию для хранения ключей и сертификатов с помощью команды:

```
mkdir /etc/asterisk/keys
```

- 3) Создайте само-подписанный сертификат сервера при помощи скрипта "ast_tls_cert". Для этого перейдите в директорию, где находится этот скрипт командой:

```
cd /usr/share/doc/asterisk-1.8.20.0/contrib./scripts/
```

Запустите скрипт для формирования сертификата:

```
./ast_tls_cert -C xxx.xxx.xxx.xxx -O "Group" -d  
/etc/asterisk/keys
```

, где C – ip адрес сервера, O – название группы, d – директория для файлов

В процессе формирования сертификата необходимо установить пароль для ca.key, а затем подтвердить его.

```
[root@Stud163 scripts]# ./ast_tls_cert -C 192.168.38.154 -O "IKTZXX" -d /etc/asterisk/keys

No config file specified, creating '/etc/asterisk/keys/tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating CA key /etc/asterisk/keys/ca.key
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for /etc/asterisk/keys/ca.key:
Verifying - Enter pass phrase for /etc/asterisk/keys/ca.key:
Creating CA certificate /etc/asterisk/keys/ca.crt
Enter pass phrase for /etc/asterisk/keys/ca.key:
Creating certificate /etc/asterisk/keys/asterisk.key
```

Рис. 5.31 Формирование сертификата сервера.

4) Сформируйте сертификат для клиента командой:

```
./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k /etc/asterisk/keys/ca.key -C yyy.yyy.yyy.yyy -O "Group" -d /etc/asterisk/keys -o clientXXXX
```

Где вместо XXXX введите SIP номер, а С - ip адрес ПК на который установлен phoner. Данную операцию следует повторить для формирования ключа на ПК2. Убедитесь, что вводите верные IP адреса машин. Сделайте скриншот формирования сертификата.

В процессе формирования сертификата будет запрошен пароль для ca.key:

```
[root@Stud163 scripts]# ./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k /etc/asterisk/keys/ca.key -C 192.168.38.155 -O "IKTZXX" -d /etc/asterisk/keys -o client1111

No config file specified, creating '/etc/asterisk/keys/tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating certificate /etc/asterisk/keys/client1111.key
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Creating signing request /etc/asterisk/keys/client1111.csr
Creating certificate /etc/asterisk/keys/client1111.crt
Signature ok
subject=/CN=192.168.38.155/O=IKTZXX
Getting CA Private Key
Enter pass phrase for /etc/asterisk/keys/ca.key:
Combining key and crt into /etc/asterisk/keys/client1111.pem
```

Рис. 5.32 Формирование клиентского сертификата

- 5) Перейдите в папку keys командой “Cd /etc/asterisk/keys” и командой ls выведите список всех файлов в папке. Сделайте скриншот.

```
[root@Stud163 scripts]# cd /etc/asterisk/keys
[root@Stud163 keys]# ls
asterisk.crt      ca.cfg           client1111.csr   client2222.csr
asterisk.csr      ca.crt           client1111.key   client2222.key
asterisk.key       ca.key           client1111.pem   client2222.pem
asterisk.pem       client1111.crt   client2222.crt   tmp.cfg
```

Рис. 5.33 Директория keys

Часть вторая: Настройка Elastix для работы с TLS и SRTP

- 1) Запустите файловый менеджер Midnight Commander с помощью команды mc, перейдите в директорию /etc/asterisk, выберите нужный файл sip_general_custom.conf и нажмите "F4"(редактировать):



Рис. 5.34 Midnight Commander

- 2) Добавьте в этот файл следующие строки:

tlsenable=yes (включение tls)

tlsbindaddr=0.0.0.0 (адрес привязки)

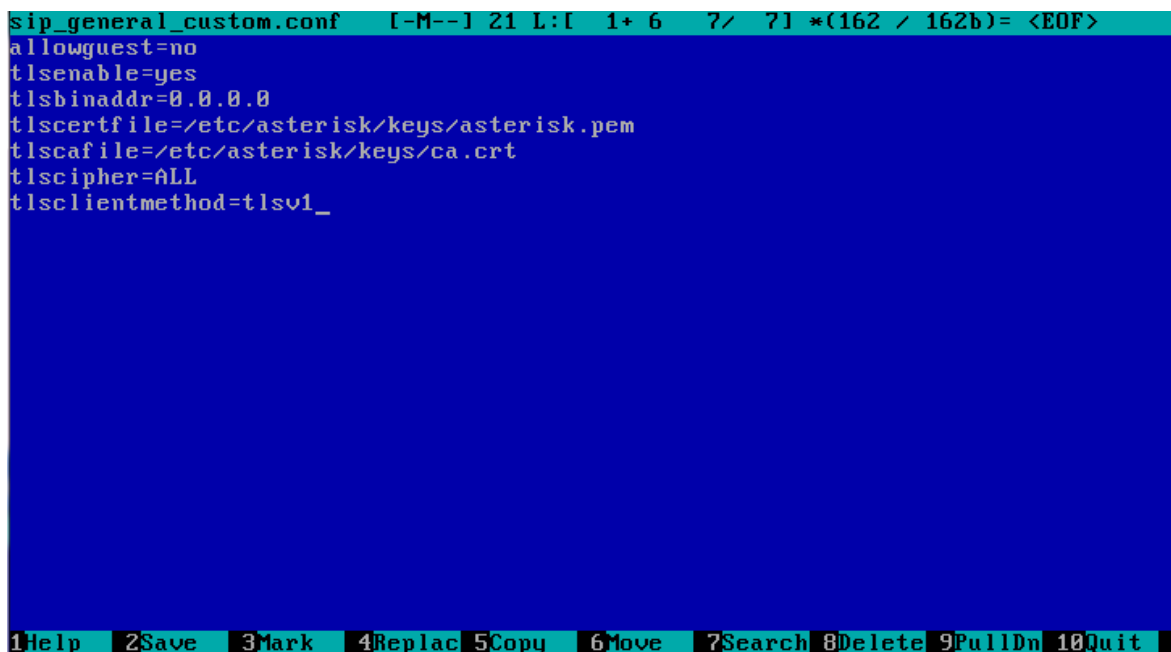
tlscertfile=/etc/asterisk/keys/asterisk.pem (путь к сертификату)

tlscasfile=/etc/asterisk/keys/ca.crt (путь к частному ключу)

```
tlscipher=ALL
```

```
tlsclientmethod=tlsv1 (метод шифрования)
```

Сохраните изменения клавишей "F2".



```
sip_general_custom.conf [-M--] 21 L:l 1+ 6 7/ 71 *(162 / 162b)= <EOF>
allowguest=no
tlsenable=yes
tlsbinaddr=0.0.0.0
tlscertfile=/etc/asterisk/keys/asterisk.pem
tlscacfile=/etc/asterisk/keys/ca.crt
tlscipher=ALL
tlsclientmethod=tlsv1_
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис. 5.35 Sip_general_custom.conf

3) Измените файл sip_custom_post.conf , прописав для номеров абонентов:

```
[XXXX] (+)
transport = tls
encryption=yes
[YYYY] (+)
transport = tls
encryption=yes
```

Сделайте скриншот.

4) Перейдите в директорию keys, введя в консоли:

```
cd /etc/asterisk/keys
```

выполните команду:

```
chmod 777 *
```

```

sip_custom_post.conf [----] 14 L:
[1111](+)
transport=tls
encryption=yes
[2222](+)
transport=tls
encryption=yes_

```

Рис. 5.36 sip_custom_post.conf

- 5) Необходимо загрузить сертификаты с сервера на ПК1 и ПК2. Для этого воспользуемся web-оболочкой Webmin.

Введите в консоли:

```
wget http://www.webmin.com/download/rpm/webmin-current.rpm
```

Установите Webmin, для этого в командной строке введите:

```
rpm - ivh webmin-XXXX.noarch.rpm
```

, где XXXX загруженная версия Webmin.

```

Saving to: 'webmin-1.740-1.noarch.rpm'
100%[=====>] 25,030,571  192K/s  in 1m 56s
2015-03-18 10:32:01 (210 KB/s) - 'webmin-1.740-1.noarch.rpm' saved [25030571/25030571]

[root@Stud163 ~]# rpm -ivh webmin-1.740-1.noarch.rpm
warning: webmin-1.740-1.noarch.rpm: Header U3 DSA signature: NOKEY, key ID 11f63c51
Preparing...
Operating system is CentOS Linux
 1:webmin
ip_tables: (C) 2000-2006 Netfilter Core Team
Webmin install complete. You can now login to https://Stud163:10000/
as root with your root password.

```

Рис. 5.37 Установка Webmin

- 6) Через браузер зайдите в Webmin по адресу https://ip_address:10000, где вместо ip_address подставьте адрес сервера Elastix (например, <https://192.168.38.177:10000/>). Введите логин, пароль (пользователь root, пароль - который указали при установке Elastix)

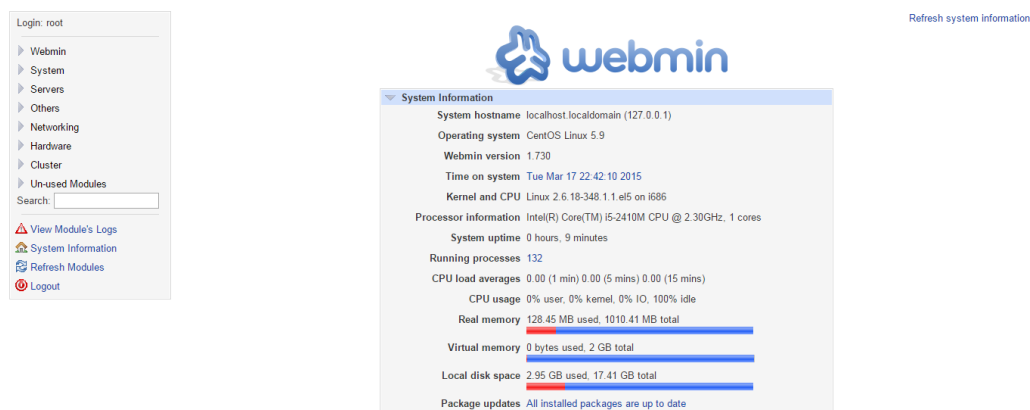


Рис. 5.38 Webmin – главный экран

- 7) Пройдя по пути Others->Upload and Download->download from server попадём на страницу загрузки файлов с сервера. Нас интересуют три файла: ca.crt, clientXXXX.crt и clientYYYYY.crt. Выберите нужный файл в поле "File to Download" по адресу /etc/asterisk/keys и нажмите на кнопку download, чтобы загрузить файл на компьютер.

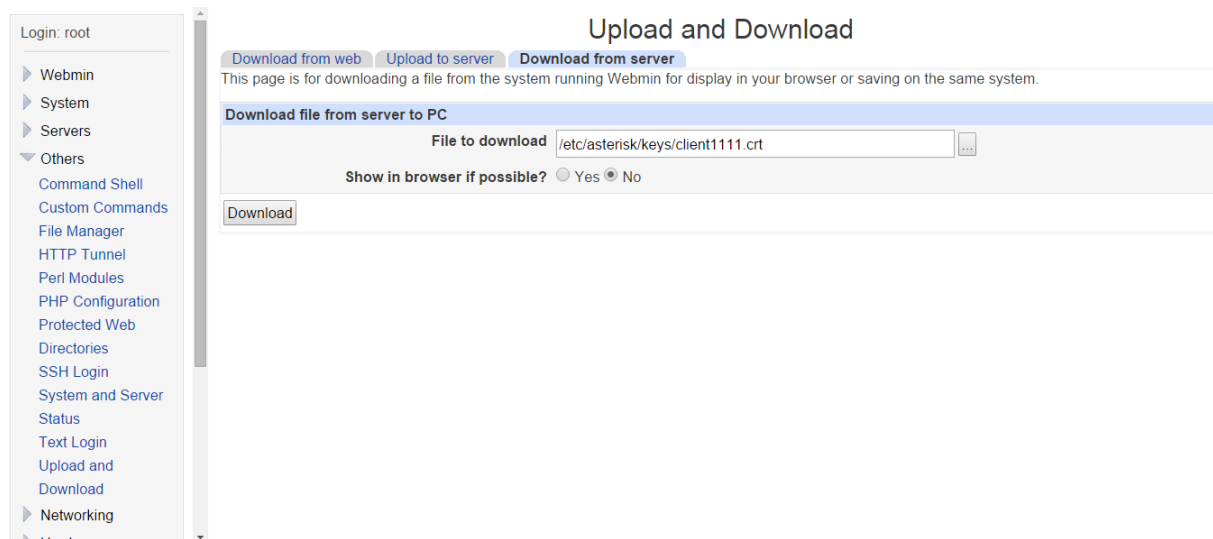


Рис. 5.39 Окно Webmin – Upload and Download

- 8) Установите оба сертификата на ПК1 и ПК2 (соответственно номерам клиентов) с помощью стандартного менеджера сертификатов. Для этого кликните по сертификату правой кнопкой мыши и выберите «Установить сертификат». Все опции оставить по умолчанию.

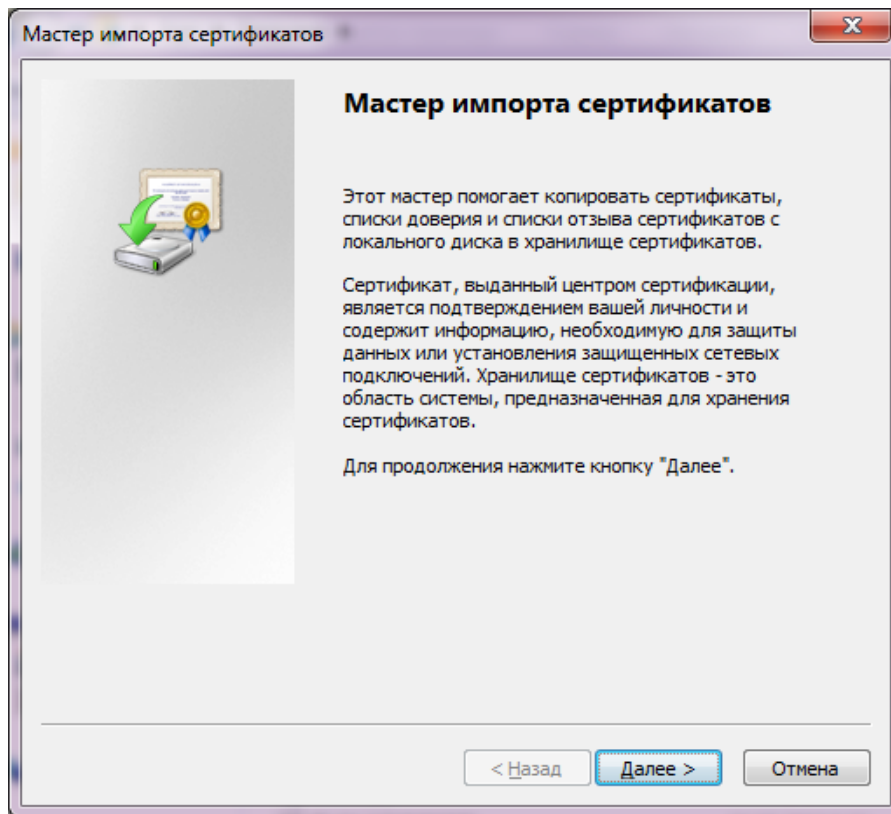


Рис. 5.40 Окно «Мастер импорта сертификатов»

- 9) Войдите к Asterisk, для этого в консоли Elastix введите
`asterisk -vr`

В консоли Asterisk выполните команду, для сохранения изменений:

```
XXXXCLI> reload
```

Введите команду `SIP SHOW PEER XXXX`, где XXXX-номер пользователя. Убедитесь, что значения `Prim.transp` и `Allowed.Trsp` равны TLS, а `encryption=yes`. Сделайте скриншот.

```
Addr->IP      : 192.168.38.155:60160
Defaddr->IP    : (null)
Prim.Transp.  : TLS
Allowed.Trsp  : TLS
Def. Username : 1111
SIP Options   : (none)
Codecs        : 0xe (gsmiulawialaw)
Codec Order   : (ulaw:20,alaw:20,gsm:20)
Auto-Framing  : No
Status        : OK (6 ms)
Useragent     : SIPPER for phoner
Reg. Contact  : sip:1111@192.168.38.155:5062;transport=tls
Qualify Freq  : 60000 ms
Sess-Timers   : Accept
Sess-Refresh  : uas
Sess-Expires  : 1800 secs
Min-Sess      : 90 secs
RTP Engine    : asterisk
Parkinglot    :
Use Reason    : No
Encryption    : Yes
```

Рис. 5.41 Данные о пользователе

Часть третья: Настройка Phoner и проверка Wireshark

1) Настройте Phoner на ПК1 и на ПК2, согласно вашим пользователям.

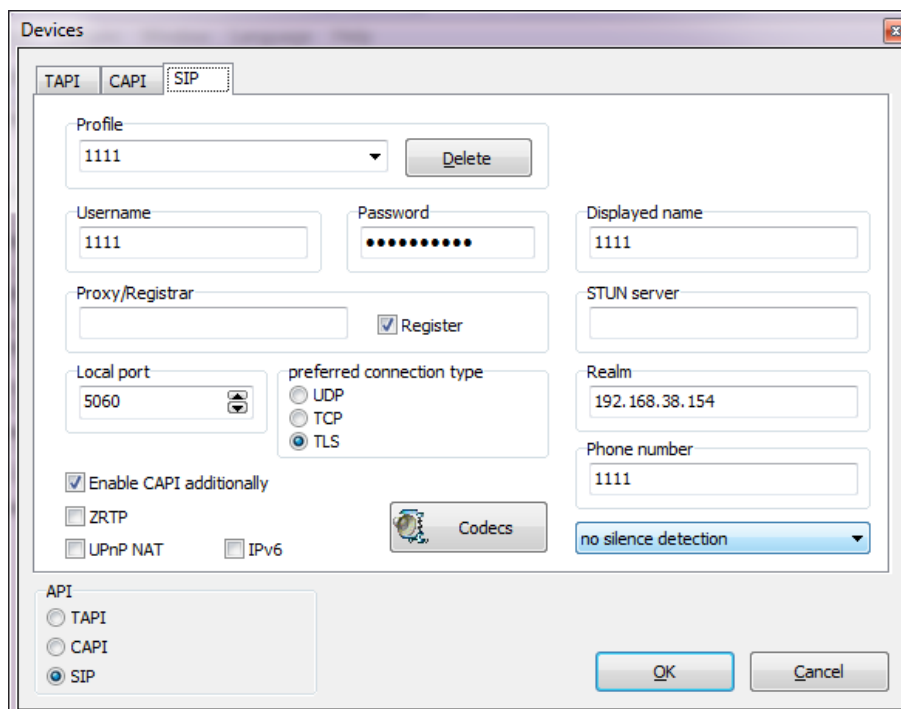


Рис. 5.42 Настройка Phoner

Нажмите на кнопку “Codecs” и установите галочку рядом с SRTP, чтобы задействовать шифрование аудио.

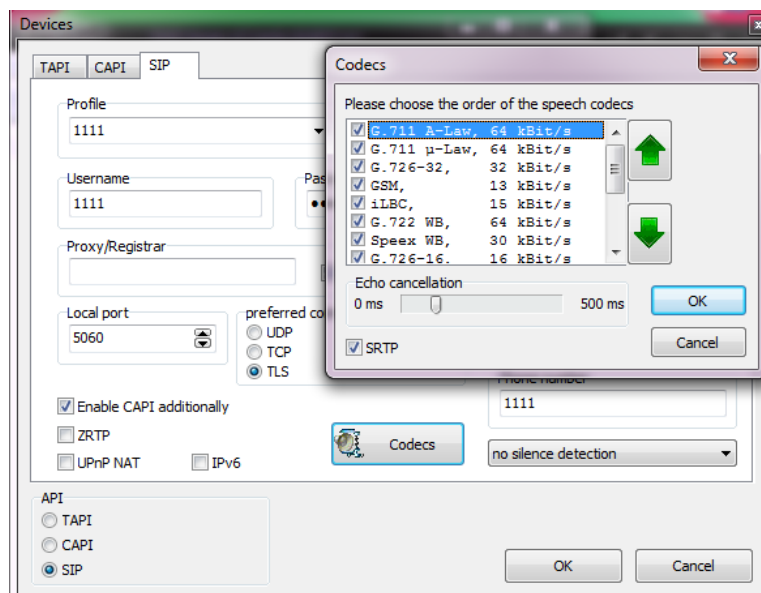


Рис. 5.43 Включение SRTP

Убедитесь в том, что регистрация прошла успешно.

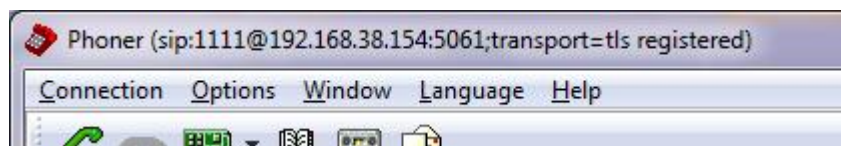


Рис. 5.44 Успешная регистрация

- 2) Откройте Wireshark и снимите дамп звонка с одного ПК на другой.

По умолчанию wireshark RTP пакеты не распознает и показывает простой UDP трафик.

2854	8.900175000	192.168.38.155	192.168.38.150	UDP	102	Source port: 5063	Destination port: 5063
2855	8.900248000	192.168.38.155	192.168.38.150	UDP	214	Source port: 5062	Destination port: 5062
2859	8.910349000	192.168.38.150	192.168.38.155	UDP	102	Source port: 5063	Destination port: 5063
2860	8.910826000	192.168.38.150	192.168.38.155	UDP	214	Source port: 5062	Destination port: 5062
2863	8.919925000	192.168.38.155	192.168.38.150	UDP	214	Source port: 5062	Destination port: 5062

Рис. 5.45 UDP пакеты

- 3) Зайдите в «Edit->Preferences->Protocols->RTP» и поставьте галочку «try to decode rtp outside of conversations».

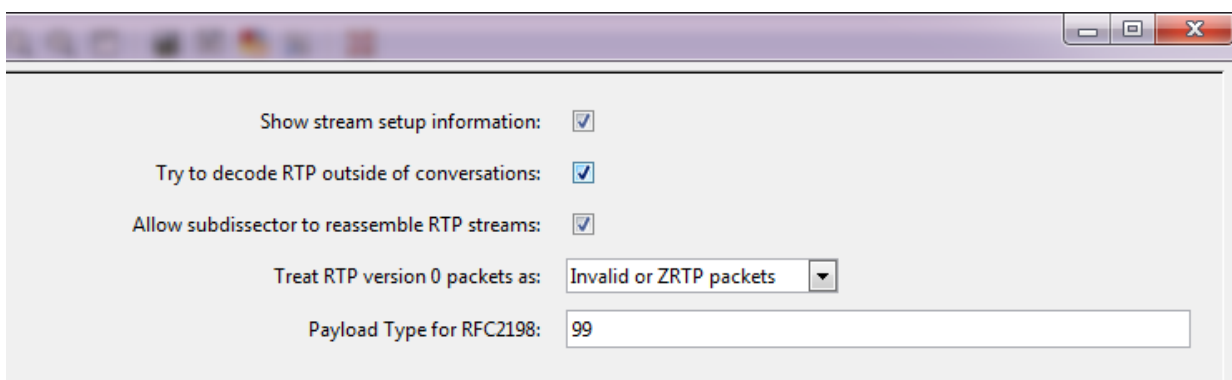


Рис. 5.46 Настройка протокола RTP

- 4) Сделайте скриншот дампа, когда происходит обмен ключами.

2097	6.643859000	192.168.38.150	192.168.38.155	TCP	60	1057-5061 [ACK] Seq=1 Ack=1 win=65535 Len=0
2098	6.644874000	192.168.38.150	192.168.38.155	TLSv1.2	420	Client Hello
2100	6.645451000	192.168.38.155	192.168.38.150	TLSv1.2	1514	Server Hello
2101	6.645463000	192.168.38.155	192.168.38.150	TCP	1514	[TCP segment of a reassembled PDU]
2102	6.646121000	192.168.38.150	192.168.38.155	TCP	60	1057-5061 [ACK] Seq=367 Ack=2921 win=65535 Len=0
2103	6.646163000	192.168.38.155	192.168.38.150	TCP	1514	[TCP segment of a reassembled PDU]
2104	6.646170000	192.168.38.155	192.168.38.150	TLSv1.2	751	Certificate
2105	6.647041000	192.168.38.150	192.168.38.155	TCP	60	1057-5061 [ACK] Seq=367 Ack=4381 win=65535 Len=0
2118	6.665763000	192.168.38.150	192.168.38.155	TLSv1.2	381	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2122	6.697517000	192.168.38.155	192.168.38.150	TLSv1.2	305	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2125	6.699326000	192.168.38.150	192.168.38.155	TLSv1.2	697	Application Data
2127	6.701777000	192.168.38.155	192.168.38.150	TLSv1.2	389	Application Data
2193	6.881971000	192.168.38.150	192.168.38.155	TCP	60	1057-5061 [ACK] Seq=1337 Ack=5664 win=64252 Len=0
2194	6.882053000	192.168.38.155	192.168.38.150	TLSv1.2	143	Application Data
2258	7.083056000	192.168.38.150	192.168.38.155	TCP	60	1057-5061 [ACK] Seq=1337 Ack=5753 win=64163 Len=0

Рис. 5.47 Обмен ключами

- 5) Убедитесь, что ваш звонок был зашифрован и при перехвате злоумышленник не смог бы его повторно воспроизвести.

В wireshark пройдите по пути Telephony-RTP-Show all streams. В открывшемся окне выберите два потока и нажмите на кнопку “Analyze”.

Затем выберите опцию “Player” и декодируйте сообщение с помощью кнопки “Decode”. Сделайте скриншот.

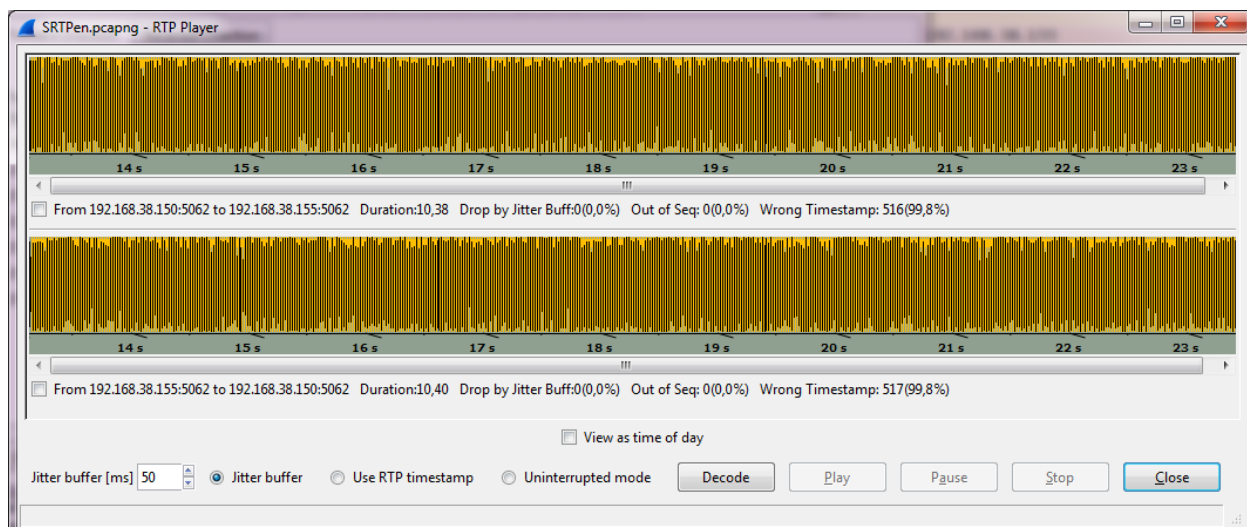


Рис. 5.48 Зашифрованная передача аудио

- б) Отключите SRTP в Phoner и снова сделайте звонок. Декодируйте RTP, как было указано ранее. Переговоры не были зашифрованы, злоумышленник мог прослушать ваш разговор. Сделайте скриншот, не забудьте сохранить дамп.

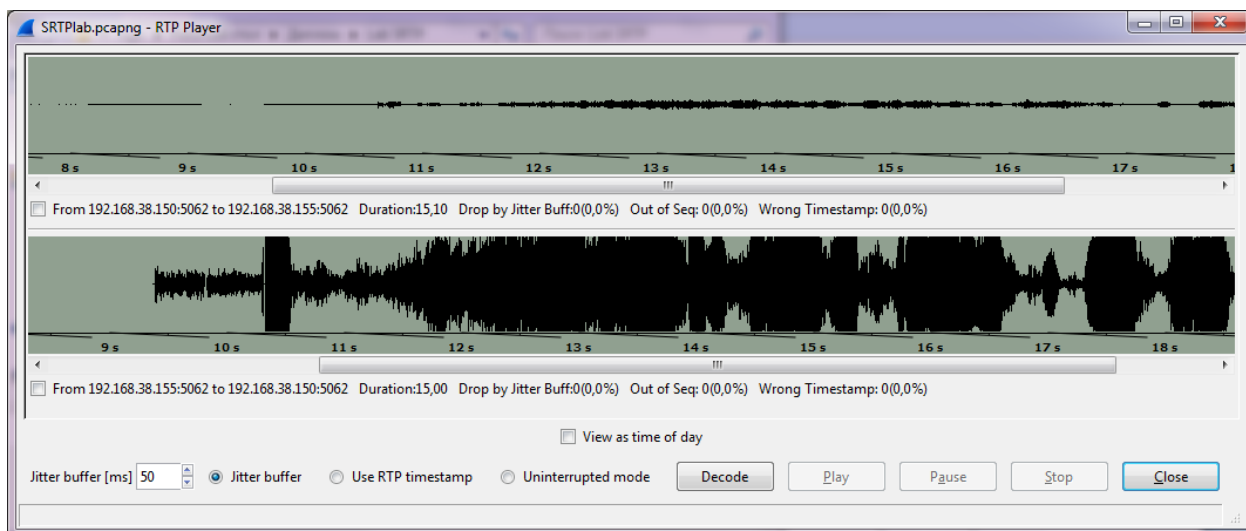


Рис. 5.49 Звонок без SRTP

Содержание отчёта:

- 1) Титульный лист;
- 2) Цель работы;
- 3) Скриншоты настройки протоколов на сервере;

- 4) Скриншоты дампа и анализа звонков в Wireshark;
- 5) Выводы о проделанной работе.

Контрольные вопросы:

- 1) Ход работы;
- 2) Протокол SRTP;
- 3) Протокол TLS.

5.4 Лабораторная работа №4. Использование программы Fail2Ban

Цель работы: Настройка встроенной программы Fail2Ban, предназначенной для защиты от подбора пароля перебором. Проверка эффективности работы данного средства.

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

Таблица 5.5

ПК1 Ip адрес: _____ MAC адрес: _____ Номер SIP: _____	ПК2 Ip адрес: _____ MAC адрес: _____ Номер SIP: _____
IP адрес сервера Elastix: _____	

Порядок выполнения лабораторной работы:

- 1) Fail2Ban уже входит в комплект Elastix. Следует только его правильно настроить для дальнейшей работы с системой asterisk. Требуется создать файл /etc/fail2ban/filter.d/asterisk.conf с определённым содержанием. Уточните местонахождение данного файла у преподавателя и проверьте его содержание.

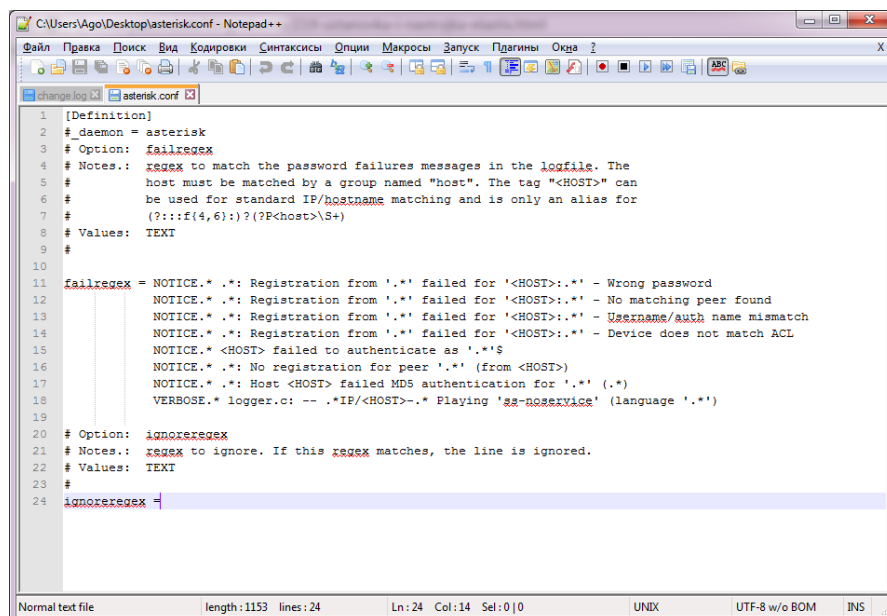


Рис. 5.50 файл Asterisk.conf

2) Воспользуйтесь знакомым модулем Webmin, чтобы загрузить данный файл на сервер Elastix.

Зайдите через браузер по адресу - <https://Ирадрессервера:10000/>

Логин – root, пароль совпадает с паролем Elastix.

Проследуйте по пути: *others->upload and download->upload to server*

Выберите файл asterisk.conf и загрузите по следующему адресу:

/etc/fail2ban/filter.d/

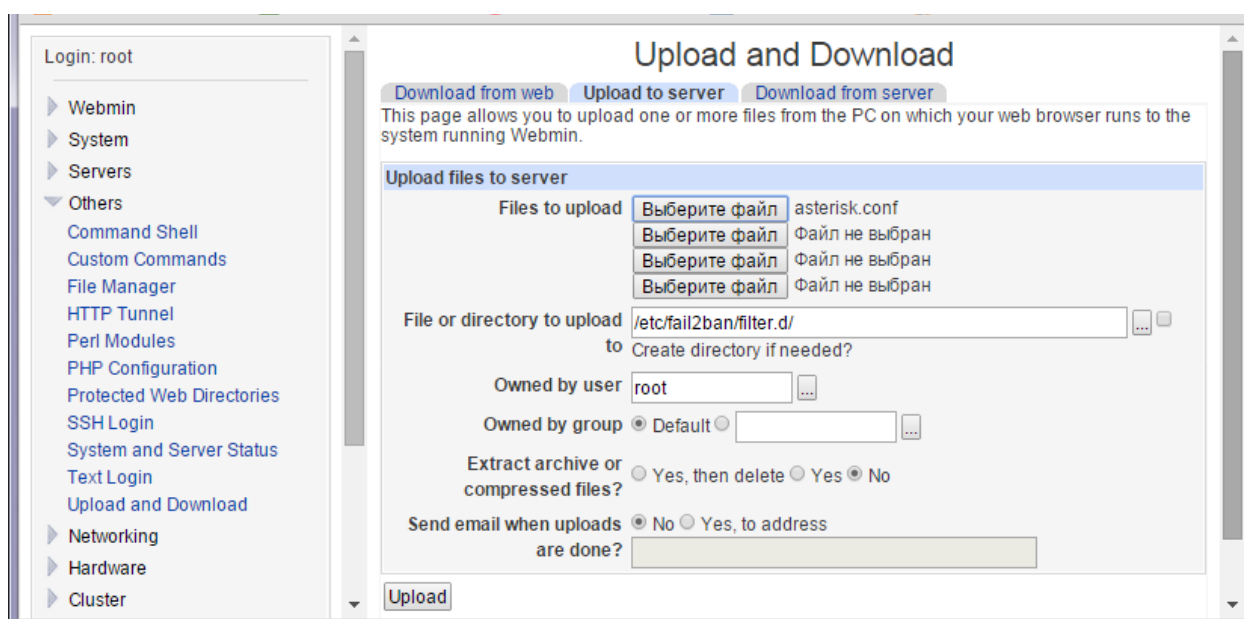


Рис. 5.51 Webmin:загрузка на сервер

Проверьте, успешно ли был загружен файл командой:

```
nano /etc/fail2ban/filter.d/asterisk.conf
```

Сделайте скриншот.

3) Отредактируйте файл jail.conf

```
nano /etc/fail2ban/jail.conf
```

Добавьте в конец файла следующие строки:

```
[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=ASTERISK, protocol=all]
sendmail-
whois[name=ASTERISK,dest=root,sender=fail2ban@local]
logpath = /var/log/asterisk/full
maxretry = 3
bantime = 600
```

Последние 2 строки позволяют установить количество допустимых попыток логина и время бана.

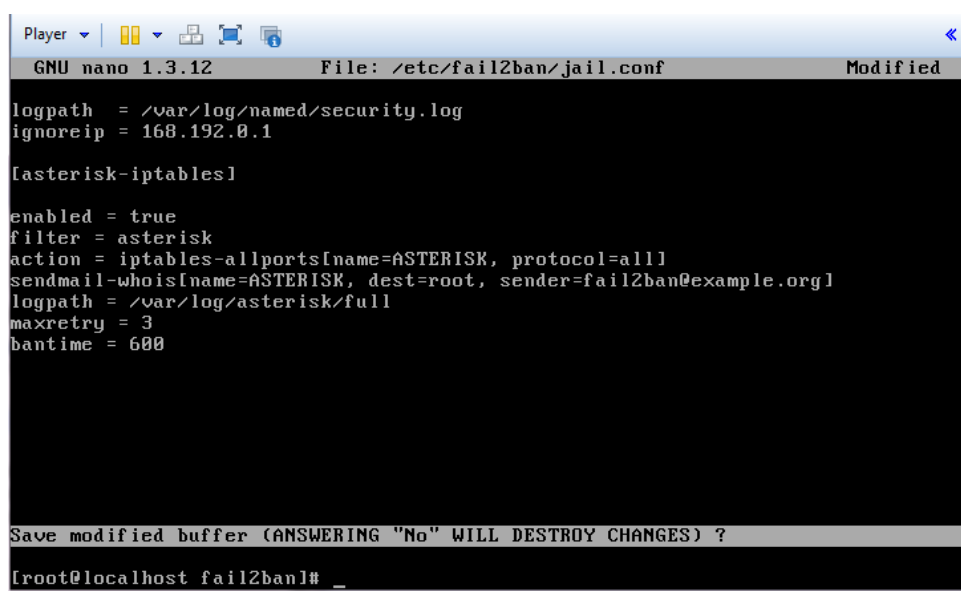


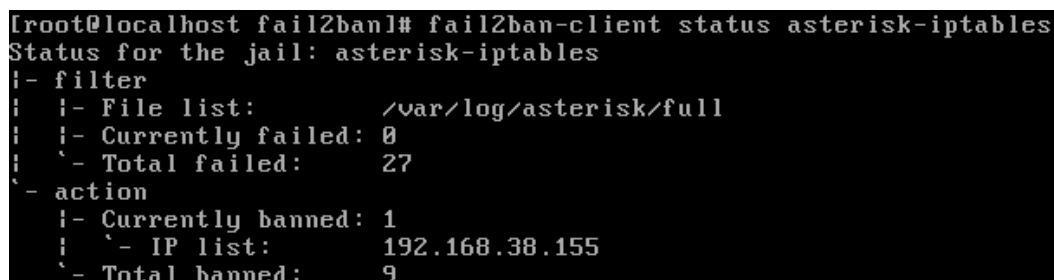
Рис. 5.52 jail.conf

4) Запустите Fail2Ban с помощью следующей команды:

```
/etc/init.d/fail2ban start
```

Попробуйте несколько раз зарегистрироваться с помощью phoner с неправильным паролем и проверьте, произошла ли блокировка адреса злоумышленника.

```
fail2ban-client status asterisk-iptables
```



```
[root@localhost fail2ban]# fail2ban-client status asterisk-iptables
Status for the jail: asterisk-iptables
|- filter
|   |- File list:          /var/log/asterisk/full
|   |- Currently failed: 0
|   '- Total failed:      27
|- action
|   |- Currently banned: 1
|   '- IP list:          192.168.38.155
'- Total banned:         9
```

Рис. 5.53 Проверка списка заблокированных адресов

Содержание отчёта:

- 1) Титульный лист
- 2) Цель работы
- 3) Скриншоты процесса настройки и работы программы
- 4) Выводы о проделанной работе

Контрольные вопросы:

- 1) Принцип работы Fail2Ban

5.5 Лабораторная работа №5. Подключение к Elastix через VPN туннель.

Цель работы: освоить применение технологии VPN туннеля в системах на базе UNIX, для обеспечения безопасного подключения к серверу через единственный порт VPN.

Подготовка к лабораторной работе: Каждая бригада должна иметь ПК с предустановленной системой Elastix. На Elastix должна быть загружена утилита Webmin.

Таблица 5.6

ПК1 Ip адрес: _____ MAC адрес: _____ Номер SIP: _____	IP-адрес сервера Elastix: _____
--	---------------------------------

Порядок выполнения лабораторной работы:

Часть первая: генерация сертификатов и ключей.

- 1) Установите пакет OpenVPN с помощью команды:

```
yum install openvpn
```

```
=====
Package           Arch           Version           Repository        Size
=====
Installing:
openvpn           i386           2.3.6-1.el5       epel              435 k
Transaction Summary
=====
Install      1 Package(s)
Upgrade     0 Package(s)

Total download size: 435 k
Is this ok [y/N]: y_
```

Рис. 5.54 Установка OpenVPN

- 2) Установите пакет easy-rsa:

```
yum install easy-rsa
```

```

=====
Package      Arch      Version      Repository    Size
=====
Installing:
easy-rsa      noarch      2.2.2-1.el5      epel           26 k
=====
Transaction Summary
=====
Install      1 Package(s)
Upgrade      0 Package(s)
=====
Total download size: 26 k
Is this ok [y/N]: _

```

Рис. 5.55 Установка easy-rsa

3) Скопируйте папку easy-rsa и файл sever.conf в папку /etc/openssl:

```

cp -a /usr/share/easy-rsa /etc/openssl/
cp /usr/share/doc/openssl-2.3.6/sample/sample-config-
files/server.conf /etc/openssl/

```

4) Перейдите в папку /etc/openssl/ и выведите список файлов

```

cd /etc/openssl/
ls

```

```

[root@localhost sample]# cd /etc/openssl/
[root@localhost openssl]# ls
easy-rsa  server.conf
[root@localhost openssl]# _

```

Рис. 5.56 Список файлов в папке openssl

5) Авторизация клиента будет происходить посредством RSA-ключей. Для упрощения процесса будут использоваться скрипты. Перейдите в папку, где будет происходить генерация ключей и отредактируйте файл vars, в котором подставьте свои значения переменных COUNTRY, PROVINCE, CITY и т.д.

```

cd /etc/openssl/easy-rsa/2.0/
nano vars

```

```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="RU"
export KEY_PROVINCE="SPB"
export KEY_CITY="Saint-Petersburg"
export KEY_ORG="Bonch"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="iktzunit"
```

Рис. 5.57 Значения для сертификатов по умолчанию

- 6) Загрузите переменные файла и постройте CA (Certificate Authority). В качестве common name укажите имя сервера Elastix

```
source ./vars
./clean-all
./build-ca
```

```
[root@localhost 2.0]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openssl/easy-rsa/
2.0/keys
[root@localhost 2.0]# ./clean-all
[root@localhost 2.0]# ./build-ca
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [SPB]:
Locality Name (eg, city) [Saint-Petersburg]:
Organization Name (eg, company) [Bonch]:
Organizational Unit Name (eg, section) [iktzunit]:
Common Name (eg, your name or your server's hostname) [Bonch CA]:localhost_
```

Рис. 5.58 Фрагмент создания CA

- 7) Создайте сертификат и ключ для сервера. В процессе создания, оставьте все значения по умолчанию и согласитесь на подписание сертификата.

```
./build-key-server server
```

```

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-0.9.8.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'RU'
stateOrProvinceName :PRINTABLE:'SPB'
localityName      :PRINTABLE:'Saint-Petersburg'
organizationName  :PRINTABLE:'Bonch'
organizationalUnitName:PRINTABLE:'iktzunit'
commonName        :PRINTABLE:'server'
name              :PRINTABLE:'EasyRSA'
emailAddress      :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until May 27 17:08:17 2025 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
[root@localhost 2.0]# _

```

Рис. 5.59 Генерация ключа сервера

- 8) Произведите генерацию ключа Диффи-Хеллмана. Учтите, что процесс генерации занимает довольно длительное время.

```
./build-dh
```

- 9) Клиенту необходимо выдать свой ключ. Для клиента с именем client1 ключ создаётся командой:

```
./build-key client
```

Все значения оставьте по умолчанию.

```

root@localhost 2.0]# ./build-key client1
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
if you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [SPB]:
Locality Name (eg, city) [Saint-Petersburg]:
Organization Name (eg, company) [Bonch]:
Organizational Unit Name (eg, section) [iktzunit]:
Common Name (eg, your name or your server's hostname) [client1]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:_

```

Рис. 5.60 Генерация ключа клиента

Часть вторая: настройка OpenVPN.

- 1) Войдите в midnight commander (команда mc) и отредактируйте файл server.conf следующим образом:

```
port 1194
proto udp
dev tun
ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key
dh /etc/openvpn/easy-rsa/2.0/keys/dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 10.8.0.0 255.255.255.0"
client-to-client
keepalive 10 120
comp-lzo
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
log /var/log/openvpn.log
verb 3
mute 20
```

Рис. 5.61 Содержание файла server.conf

- 2) Установите на ПК программу OpenVPN, сохраните состояние виртуальной машины и перезагрузите компьютер.
- 3) С помощью утилиты webmin загрузите на свой компьютер 3 файла (ca.crt , client1.crt , client1.key) и поместите их в папку *C:\Program Files\OpenVPN\config*.
- 4) В папке куда вы поместили ключи создайте файл voip.ovpn следующего содержания:

```
client
dev tun
proto udp
remote xxx.xxx.xxx.xxx 1194
resolv-retry infinite
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
```

```
comp-lzo
```

```
verb 3
```

,где xxx.xxx.xxx.xxx – адрес сервера Elastix.

5) Запустите сервис OpenVPN на Elastix с помощью команды:

```
Service openvpn start
```

6) Запустите Firewall Elastix. При настройках по умолчанию, он не пропускает VPN трафик через порт 1194. Выберите опцию Define Ports и добавьте новый порт с названием VPN, протокол UDP, №1194.

7) Добавьте новое правило в Firewall для VPN. Protocol - UDP, Source – ANY, Destination – VPN. Поднимите это правило на вторую позицию.

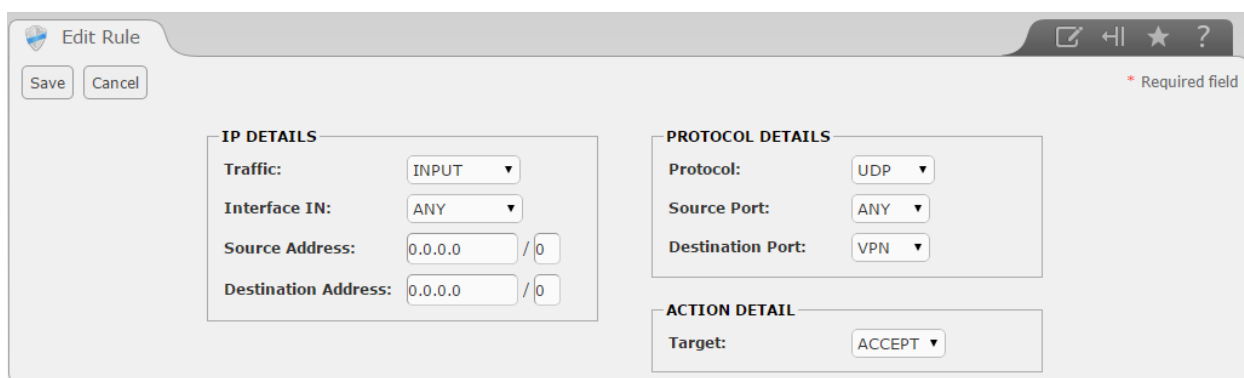


Рис. 5.62 Правило АСCEPT для VPN трафика

8) Создайте правило АСCEPT с адресов 10.8.0.0/24, тип протокола – ALL.

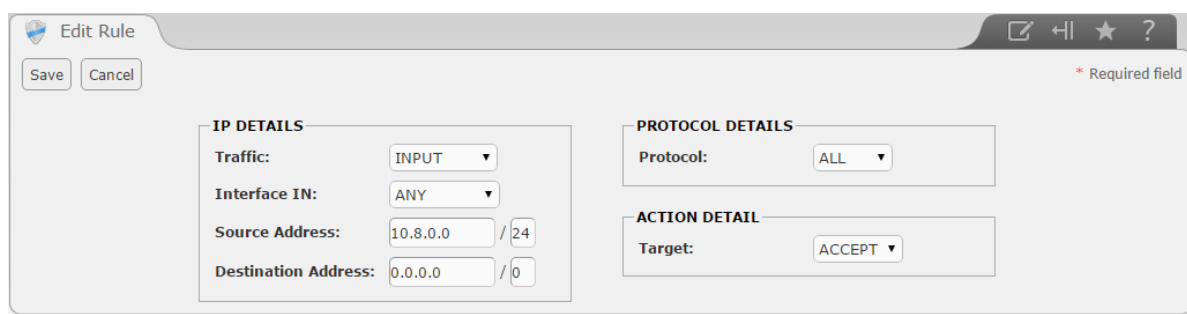


Рис. 5.63 Правило АСCEPT для группы адресов

9) Расположите правила следующим образом:

- IN ACCEPT:lo 0.0.0.0 ALL;

- IN ACCEPT:ANY 0.0.0.0 UDP Dest.Port. VPN;
- IN ACCEPT:ANY 10.8.0.0/24 ALL;
- IN REJECT: ANY 0.0.0.0 ALL.
- Остальные правила по умолчанию

Будьте внимательны, после применения данных правил любое соединение с сервером будет запрещено. Если потребуется настроить firewall заново, наберите “setup” и отключите firewall.

<input type="checkbox"/>	1				IN: lo	0.0.0.0/0	0.0.0.0/0	ALL			
<input type="checkbox"/>	2				IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: VPN		
<input type="checkbox"/>	3				IN: ANY	10.8.0.0/24	0.0.0.0/0	ALL			
<input type="checkbox"/>	4				IN: ANY	0.0.0.0/0	0.0.0.0/0	ALL			

Рис. 5.64 Порядок правил Firewall

- 10) Запустите от имени администратора openvpn-gui по адресу C:\Program Files\OpenVPN\bin и подключитесь к серверу. Сохраните сообщения журнала в отдельный файл. Если в журнале проскакивает сообщение о неправильном времени применения сертификата, переведите дату на день вперёд.

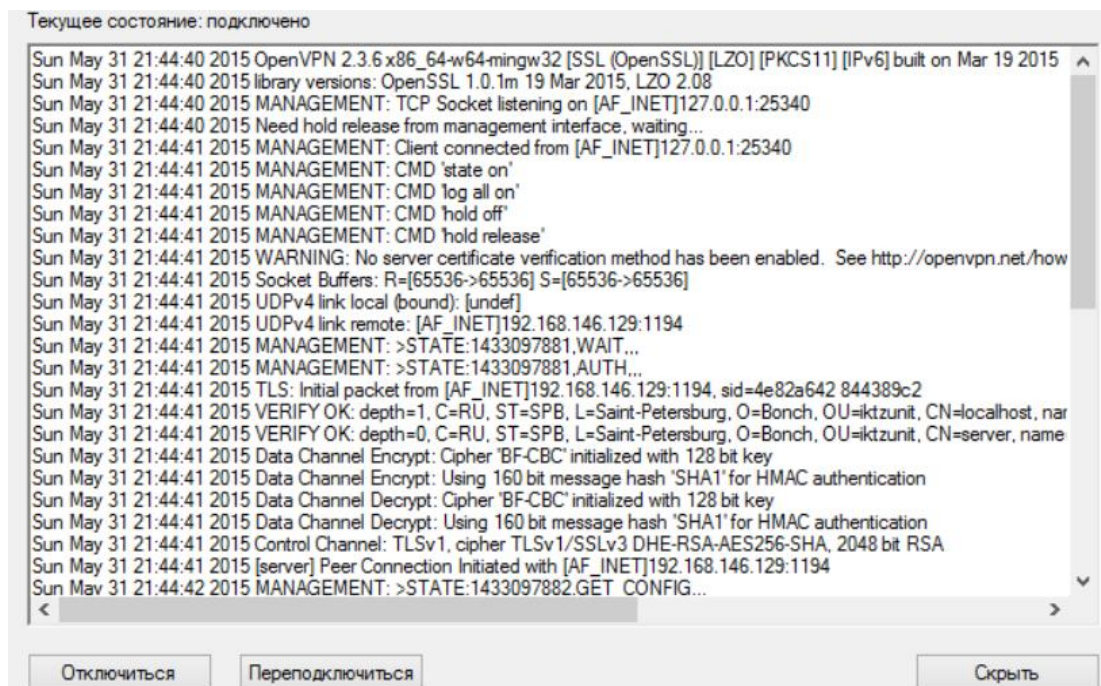


Рис. 5.65 Состояние подключения по VPN

- 11) Серверу теперь присвоен адрес 10.8.0.1, зайдите через браузер на web-интерфейс, а также произведите пинг с ПК на сервер и с сервера на ПК, сделайте скриншоты.

Содержание отчёта:

- 1) Титульный лист;
- 2) Цель работы;
- 3) Скриншоты: генерация сертификатов, настройка firewall'а, проверка openvpn, журнал подключения по VPN;
- 4) Выводы о проделанной работе.

Контрольные вопросы:

- 1) Принцип работы VPN туннеля;
- 2) Настройка Firewall;
- 3) Шифрование: RSA, протокол Диффи-Хеллмана, TLS.

Список использованной литературы:

1. Меггелен Дж., Мадсен Л., Смит Дж. Asterisk: будущее телефонии, 2-е издание. – Пер. с англ. – СПб: Символ-Плюс, 2009. – 656 с., ил.
2. Ben Sharif, Elastix without tears, 2009г – 257с., ил.
3. Платов М. Asterisk и Linux – миссия IP-телефония [Текст] /М. Платов// Системный Администратор. -2005 г. -№ 31. – С. 12-19.
4. База знаний Asterisk [Электронный ресурс]. –режим доступа: asterisk.ru/knowledgebase
5. Bob Fryer, A Guide to the Elastix Firewall GUI [pdf], 2011г. - 20с.
6. Bob Fryer, Elastix Security Guide V2.0 [pdf], 2014г. – 26с.
7. RFC 3605. С. Huitema. RTCP: Real Time Control Protocol. - IEFT, October 2003.
8. IP-телефония / Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. - М. : Москва "Радио и Связь", 2006. - 334с. - ISBN 5-256-01585-0
9. Asterisk будущее телефонии / Джим Ван Меггелен, Лейф Мадсен, Джаред Смит. - М. : Символ - Плюс, 2009. - 638с. - ISBN 5-93286-128-2
10. Протоколы обеспечения безопасности IP-телефонии / М. М. Ковцур // Первая миля. - 2012. - №5. - С. 18-26.

