

Никоноров М.Ю, Ефременко А.В



Asterisk

Телефония Asterisk с нуля

Подробное пошаговое руководство. Коды

Приложение к одноименному видеокурсу

Оглавление

1. Устанавливаем ОС Linux сборки CentOS.....	4
2. Установка Putty.....	4
3. Установка Asterisk.....	4
4. Конфигурация Asterisk для совершения звонков между внутренними абонентами.....	5
5. Конфигурация Asterisk на работу через транк (принимаем звонки с внешних телефонов).....	6
6. Реализация функций Asterisk.....	6
6.1 Установка музыки вместо гудка.....	6
6.2 Создание интерактивного (голосового) меню.....	7
6.3 Перенаправление звонков.....	9
6.4 Запись разговоров.....	9
6.5 Простой автоответчик.....	11
6.6 Улучшение работы автоответчика и записи звонков.....	12
6.7 Установка системы просмотра статистики звонков.....	15
6.8 Усовершенствуем голосовую почту. Голосовая почта на каждый телефон с отправкой уведомления по e-mail.....	19
6.9 Перехват звонков. Pickup.....	23
7. Усиливаем безопасность Asterisk. 17 шагов которые сохранят Ваши деньги.....	23
7.1 Меняем SIP порт.....	23
7.2 Запрещаем чужакам SIP подключение.....	23
7.3 Защищаем сервер от перебора по номерам.....	23
7.4 Устанавливаем более сильные пароли для sip-клиентов.....	23
7.5 Запрещаем международные вызовы на уровне Dial плана.....	24
7.6 Настройка встроенного фаерволла iptables.....	24
7.7 Изменяем порт SSH, запрещаем пользователю логиниться как root через ssh, добавляем нового пользователя.....	24
7.8 Выключаем Apache из автозагрузки и меняем его порт.....	24
7.9 Отключаем ненужные модули и протоколы Asterisk.....	25
7.10 Изменим порт управления Астериском (AMI).....	25
7.11 Настраиваем систему fail2ban.....	25
7.12 Защита от DOS атак.....	28

7.13 Улучшение защиты от DOS атак.....	28
7.14 Защита от сканирования портов.....	31
7.15 Сертификация SSH.....	31
7.16 Отключение samba.....	31
7.17 Дополнительная защита.....	31
7.18 Итоги обеспечения безопасности.....	31
8. Реализация дополнительных функций Asterisk	32
8.1 Конференц-связь Asterisk	32
8.2 Парковка вызовов	35
8.3 Переадресация звонков (FollowMe).....	35
8.4 Очередь звонков. Создаем Call-центр.	37
8.5 Работа Asterisk в зависимости от дня недели и времени суток	37
9. Заключение.....	38

1. Устанавливаем ОС Linux сборки CentOS

2. Установка Putty

3. Установка Asterisk

```
wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz  
wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar.gz  
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-11-current.tar.gz
```

Для 32 бита:

```
./configure && make menuselect && make && make install
```

Для 64 бита:

```
./configure --libdir=/usr/lib64 && make menuselect && make && make install
```

4. Конфигурация Asterisk для совершения звонков между внутренними абонентами

У нас открывается файл. Пишем свои конфиги в самое начало файла. В моем случае это определение двух sip клиентов (телефонов):

```
[1001]
type=friend
regexten=1001
secret=1234
context=outcoling
host=dynamic
callerid="1001" <1001>
disallow=all
allow=alaw
allow=ulaw
language=ru
callgroup=1
pickupgroup=1
qualify=yes
canreinvite=yes
call-limit=4
nat=no

[1002]
type=friend
host=dynamic
insecure=invite
username=1002
secret=45678
context=outcoling
disallow=all
allow=alaw
```

5. Конфигурация Asterisk на работу через транк (принимаем звонки с внешних телефонов)

И над нашими sip клиентами [1001] и [1002] пишем следующий код:

```
[general]
register => 00000:password@sip.zadarma.com/00000

[zadarma]
type=friend
username=00000
secret=password
fromuser=00000
fromdomain=sip.zadarma.com
host=sip.zadarma.com
nat=yes
insecure=invite
context=incoming
canreinvite=no
```

6. Реализация функций Asterisk

6.1 Установка музыки вместо гудка.

```
desktop\pscp.exe D:\Jessi.wav root@ip адрес CentOS:/var/lib/asterisk/moh/mymusic
```

6.2 Создание интерактивного (голосового) меню.

и добавляем:

```
[7777]
type=friend
host=dynamic
insecure=invite
username=7777
secret=1213
context=outcoling
disallow=all
allow=alaw
```

затираем все, что делали там ранее, и вместо это пишем:

[incoming]

```
exten => _X.,1,Goto(menu,s,1) ;если нам кто-то звонит, то входящий звонок из файла sip.conf поступает на этот контекст. После чего звонок переадресовывается с помощью функции Goto на контекст menu
```

[outgoing]

```
exten => _XXXXXXXXXX,1,Dial(SIP/zadarma/${EXTEN})
```

```
exten => _XXXX,1,Dial(SIP/${EXTEN},,m)
```

```
exten => 7777,1,Goto(menu,s,1) ;если мы изнутри позвоним на этот номер, то мы сможем проверить работу нашего голосового меню. Благодаря этой строчки нет необходимости для проверки звонить постоянно с внешки
```

[menu]

```
exten => s,1,Background(/var/lib/asterisk/moh/voicemail/voicemail) ;здесь ловится звонок из контекста incoming и проигрывается записанное нами приветствие. Не надо указывать расширение файла, достаточно указать само имя файла с записанным голосом
```

```
exten => 1,1,Dial(SIP/1001,,m) ;если человек нажал цифру 1, то звоним нашему внутреннему абоненту 1002
```

```
exten => 2,1,Dial(SIP/1002,,m) ;если человек нажал цифру 2, то звоним нашему внутреннему абоненту 1005
```

```
exten => s,n,Wait(5) ;если человек не нажал ничего, ждем 5 секунд и
```

```
exten => s,n,Dial(SIP/1001&SIP/1002,,m) ; тогда звоним сразу двум абонентам
```


6.3 Перенаправление звонков

6.4 Запись разговоров

Это простой общий пример. Ниже будет приведен мой конкретный Dial план:

```
[incoming]
```

```
exten => _X.,1,Goto(menu,s,1)
```

```
[outgoing]
```

```
exten => _X.,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN});_X.,  
означает, что для ЛЮБЫХ исходящих номеров начинает определяться название файла
```

```
exten => _X.,2,MixMonitor(/records/callrecords/${fname}.wav);_X., означает, что для ЛЮБЫХ исходящих  
номеров начинается запись файла и сохраняется по пути, который мы создали в нашем linux:  
/records/callrecords/
```

```
exten => _XXXXXXXXXX,3,Dial(SIP/zadarma/${EXTEN})
```

```
exten => _XXXX,3,Dial(SIP/${EXTEN},,t&m,)
```

```
exten => 7777,1,Goto(menu,s,1);
```

```
[menu]
```

```
exten => s,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN});буква s в  
данном случае означает, что нет точного определения в каком конкретном случае начнется  
определение имени файла. Эта строка просто начинает работать сама по себе как только вызывается  
экстеншен [menu]
```

```
exten => s,2,MixMonitor(/records/callrecords/${fname}.wav)
```

```
exten => s,3,Background(/var/lib/asterisk/moh/voicemail/voicemail)
```

```
exten => 1,1,Dial(SIP/1001,30,m&t)
```

```
exten => 2,1,Dial(SIP/1002,30,m&t)
```

```
exten => s,4,Wait(5)
```

```
exten => s,5,Dial(SIP/1001&SIP/1002,30,t&m)
```

Удаляем оттуда все, и пишем то, что предлагаю я:

```
# smb.conf is the main Samba configuration file. You find a full commented
# version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE if the
# samba-doc package is installed.
# Date: 2008-06-06

[global]
workgroup = WORKGROUP
server string = Samba Mega Server %v
hosts allow = ALL

# ----- Logging Options -----
log file = /var/log/samba/%m.log
# max 50KB per log file, then rotate
max log size = 1024

# ----- Standalone Server Options -----
security = share
#encrypt passwords = yes
socket options = TCP_NODELAY SO_SNDBUF=8192 SO_RCVBUF=8192 IPTOS_LOWDELAY

# ----- Browser Control Options -----
local master = yes
os level = 255
preferred master = yes

# ----- Name Resolution -----
dns proxy = yes

# -----Charsets-----
unix charset = utf8
dos charset = cp1251
display charset = cp1251

# -----Share Definitions -----

[share]
comment = records
path = /records #здесь указывается папка, которую мы расшариваем
browseable = yes
```

```
writable = yes
```

```
guest ok = yes #позволяет подключаться к папке кому угодно, без аутентификации
```

6.5 Простой автоответчик

h) Теперь настроим Dial план в файле extensions.conf. Затираем все то, что мы писали ранее и пишем так:

```
[incoming]
```

```
exten => _X.,1,Goto(menu,s,1)
```

```
[outcoling]
```

```
exten => _X.,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
```

```
exten => _X.,2,MixMonitor(/records/callrecords/${fname}.wav,b)
```

```
exten => _XXXXXXXXXX,3,Dial(SIP/zadarma/${EXTEN})
```

```
exten => _XXXX,3,Dial(SIP/${EXTEN},,t&m,)
```

```
exten => 7777,3,Goto(menu,s,1,t&m)
```

```
[menu]
```

```
exten => s,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
```

```
exten => s,2,MixMonitor(/records/callrecords/${fname}.wav)
```

```
exten => s,3,Background(/var/lib/asterisk/moh/voicemail/voicemail)
```

```
exten => 1,1,Dial(SIP/1001,30,m&t)
```

```
exten => 1,2,Goto(autoanswer,s,1) ;Если 1001 не ответил или сбросил вызов, перенаправляем на автоответчик
```

```
exten => 2,1,Dial(SIP/1002,30,m&t)
```

```
exten => 2,2,Goto(autoanswer,s,1) ;Если 1002 не ответил или сбросил вызов, перенаправляем на автоответчик
```

```
exten => s,4,Wait(5)
```

```
exten => s,5,Dial(SIP/1001&SIP/1002,30,t&m) ;если в течении 30 секунд ни 1001 ни 1002 не ответили или сбросили вызов, то вызывается контекст autoanswer (автоответчик)
```

```
exten => s,6,Goto(autoanswer,s,1)
```

```
[autoanswer]
```

```
exten => s,1,Background(/var/lib/asterisk/moh/voicebox/название нашего файла приветствия без расширения) ;проигрывается наше записанное приветствие. Мол все заняты
```

```
exten => s,2,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN}) ;здесь выполняется определение имени файла, в которое будет записан голос чувака, оставляющего сообщение на автоответчик
```

```
exten => s,3,Record(/records/voicemail/${fname}.wav,0,15,X) ;теперь записывается сам файл. При начале выполнения этой строчки, чувак на том конце слышит бииб.
```

```
exten => s,4,Hangup
```

6.6 Улучшение работы автоответчика и записи звонков

Открывается редактор nano. Пишем туда код:

```
<?php  
  
$file_list = glob("*.wav");  
  
$q[]="";  
$q[]="января";  
$q[]="февраля";  
$q[]="марта";  
$q[]="апреля";  
$q[]="мая";  
$q[]="июня";  
$q[]="июля";  
$q[]="августа";  
$q[]="сентября";  
$q[]="октября";  
$q[]="ноября";  
$q[]="декабря";  
$dlina=count($file_list);
```

```

echo "Количество файлов = ".$dlina."<br>";
?>
<form name="test" method="post" action="index.php">
    Введите год месяц число, например (20110228)<input name="date" type="text" value="<?php echo
$_POST['date']; ?>"size="10">
    <input type="submit" value="Отправить">
</form>
<?php

if ($_POST['date']<>"") {
$day=substr($_POST['date'], 6, 2);
$month=substr($_POST['date'], 4, 2);
$year=substr($_POST['date'], 0, 4);
echo "Звонки записанные ".$day." ".$q[$month]." ".$year."<br>";
$datelist=$_POST['date'];
echo "<pre>";
for ($i=0;$i<=count($file_list);$i++)
{
$day=substr($file_list[$i], 6, 2);
$month=substr($file_list[$i], 4, 2);
$year=substr($file_list[$i], 0, 4);
$time=substr($file_list[$i], 8, 4);
$napravlenie=substr($file_list[$i], 13, 20);
$timeq=$time[0].".".$time[1].":".$time[2].".".$time[3];

$string=substr($file_list[$i], 0, strlen($datelist));
if ($string==$datelist) echo "<a href="."$file_list[$i].">".$day." ".$q[$month]." ".$year." в ".$timeq."
".$napravlenie."</a>\n";

```

```
}  
echo "</pre>";  
}  
?>
```

Полный экстеншен в моем случае выглядит следующим образом:

```
[incoming]  
exten => _X.,1,Goto(menu,s,1)  
  
[outcoling]  
exten => _X.,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})  
exten => _X.,2,MixMonitor(/var/www/html/callrecords/${fname}.wav,b)  
exten => _XXXXXXXXXX,3,Dial(SIP/zadarma/${EXTEN})  
exten => _XXXX,3,Dial(SIP/${EXTEN},,t&m,)  
exten => 7777,3,Goto(menu,s,1,t&m)  
exten => 9999,3,Goto(autoanswer,s,1,t&m)  
  
[menu]  
exten => s,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})  
exten => s,2,MixMonitor(/var/www/html/callrecords/${fname}.wav)  
exten => s,3,Background(/var/lib/asterisk/moh/voicemail/voicemail)  
exten => 1,1,Dial(SIP/1001,30,m&t)  
exten => 1,2,Goto(autoanswer,s,1)  
exten => 2,1,Dial(SIP/1002,30,m&t)  
exten => 2,2,Goto(autoanswer,s,1)  
exten => s,4,Wait(5)  
exten => s,5,Dial(SIP/1001&SIP/1002,30,t&m)  
exten => s,6,Goto(autoanswer,s,1)
```

```
[autoanswer]
```

```
exten => s,1,Background(/var/lib/asterisk/moh/voicebox/busy)
```

```
exten => s,2,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
```

```
exten => s,3,Record(/var/www/html/voicemail/${fname}.wav,0,15,X)
```

```
exten => s,4,Hangup
```

6.7 Установка системы просмотра статистики звонков

и пишем туда вот этот код:

```
<?php
    $dblocation = "localhost";
    $dbname = "test";
    $dbuser = "root";
    $dbpasswd = "ваш пароль который вы поставили на сервер MySQL";

    $dbcnx = @mysql_connect($dblocation, $dbuser, $dbpasswd);
    if (!$dbcnx){
        echo "<p>К сожалению, не доступен сервер MySQL</p>";
        exit();
    }
    if (!@mysql_select_db($dbname,$dbcnx)){
        echo "<p>К сожалению, не доступна база данных</p>";
        exit();
    }
    $ver = mysql_query("SELECT VERSION()");
    if (!$ver){
        echo "<p>Ошибка в запросе</p>";
        exit();
    }
}
```

```
}  
echo mysql_result($ver, 0);  
?>
```

в) Создаем в базе “asterisk” таблицу “cdr”, вот с такой структурой

```
mysql> use asterisk;  
  
mysql> CREATE TABLE `cdr` (  
  `id` int(11) unsigned NOT NULL auto_increment,  
  `calldate` datetime NOT NULL default '0000-00-00 00:00:00',  
  `clid` varchar(80) NOT NULL default '',  
  `src` varchar(80) NOT NULL default '',  
  `dst` varchar(80) NOT NULL default '',  
  `dcontext` varchar(80) NOT NULL default '',  
  `channel` varchar(80) NOT NULL default '',  
  `dstchannel` varchar(80) NOT NULL default '',  
  `lastapp` varchar(80) NOT NULL default '',  
  `lastdata` varchar(80) NOT NULL default '',  
  `duration` int(11) NOT NULL default '0',  
  `billsec` int(11) NOT NULL default '0',  
  `disposition` varchar(45) NOT NULL default '',  
  `amaflags` int(11) NOT NULL default '0',  
  `accountcode` varchar(20) NOT NULL default '',  
  `uniqueid` varchar(32) NOT NULL default '',  
  `userfield` varchar(255) NOT NULL default '',  
  PRIMARY KEY (`id`),  
  KEY `calldate` (`calldate`),  
  KEY `accountcode` (`accountcode`),  
  KEY `uniqueid` (`uniqueid`),  
  KEY `dst` (`dst`),  
  KEY `src` (`src`)  
) ENGINE=InnoDB AUTO_INCREMENT=1 DEFAULT CHARSET=latin1;
```


г) Теперь даем доступ для пользователя “asterisk_user” с паролем “Some_Pass_Aster01” к базе “asterisk” только с локалхоста.

```
mysql> grant all on asterisk.* to 'asterisk_user'@'localhost' identified by 'Some_Pass_Aster01';
```

```
mysql> flush privileges;
```

и вместо записи [global] которая там есть (вместо неё) пишем:

```
[global]
hostname=localhost
dbname=asterisk
table=cdr
password=Some_Pass_Aster01
user=asterisk_user
sock=/var/lib/mysql/mysql.sock
```

5. Теперь осталось прикрутить web интерфейс, который и будет выводить данные из базы MySQL.

и изменяем там последний раздел share definitions на:

```
# -----Share Definitions -----
[share]
comment = share
path = /var
browseable = yes
writable = yes
guest ok = yes
read only = no
directory mask = 0777
force create mode = 0777
```

Там вместо

```
$db_type = 'mysql';
$db_host = 'localhost';
$db_port = '3306';
$db_user = 'cdrasterisk';
$db_pass = 'astcdr123';
$db_name = 'cdrasterisk';
$db_table_name = 'cdr';
```

прописываем

```
$db_type = 'mysql';  
$db_host = 'localhost';  
$db_port = '3306';  
$db_user = 'asterisk_user';  
$db_pass = 'Some_Pass_Aster01';  
$db_name = 'asterisk';  
$db_table_name = 'cdr';  
$db_options = array();
```

6.8 Усовершенствуем голосовую почту. Голосовая почта на каждый телефон с отправкой уведомления по e-mail.

в самый конец файла добавляем следующие строчки:

```
smtp_sasl_auth_enable = yes  
smtp_sasl_password_maps = hash:/etc/postfix/mailpasswd  
smtp_sasl_security_options = noanonymous  
smtp_sasl_type = cyrus  
smtp_sasl_mechanism_filter = login  
smtp_sender_dependent_authentication = yes  
sender_dependent_relayhost_maps = hash:/etc/postfix/sender_relay  
sender_canonical_maps = hash:/etc/postfix/canonical  
smtp_generic_maps = hash:/etc/postfix/generic
```

В моем конкретном случае это выглядит так:

[1001]

type=friend

host=dynamic

insecure=invite

username=1001

secret=1234

context=outcoling

disallow=all

allow=alaw

mailbox=1001@default ;это ГОЛОСОВОЙ ПОЧТОВЫЙ ЯЩИК куда будет записываться голос

language=en

[1002]

type=friend

host=dynamic

insecure=invite

username=1002

secret=45678

context=outcoling

disallow=all

allow=alaw

mailbox=1002@default ;это ГОЛОСОВОЙ ПОЧТОВЫЙ ЯЩИК куда будет записываться голос

language=en

Так же регистрируем еще одного sip клиента. Его назначение станет ясно позже:

```
[700]
type=friend
host=dynamic
insecure=invite
username=700
secret=5555
context=outcoling
disallow=all
allow=alaw
```

В моем конкретном случае, весь файл extention.conf будет выглядеть следующий образом (добавлены те строки, у которых есть комментарий):

```
[incoming]
exten => _X.,1,Goto(menu,s,1)

[outcoling]
exten => _X.,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
exten => _X.,2,MixMonitor(/var/www/html/callrecords/${fname}.wav,b)
exten => _XXXXXXXXXX,3,Dial(SIP/zadarma/${EXTEN})
exten => _XXXX,3,Dial(SIP/${EXTEN},,t&m,)
exten => 7777,3,Goto(menu,s,1,t&m)
exten => 9999,3,Goto(autoanswer,s,1,t&m)
exten => 700,1,VoiceMailMain() ;здесь если позвонить на номер 700 мы сможем прослушать свою
голосовую почту

[menu]
exten => s,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
exten => s,2,MixMonitor(/var/www/html/callrecords/${fname}.wav)
exten => s,3,Background(/var/lib/asterisk/moh/voicemail/voicemail)
exten => 1,1,Dial(SIP/1001,30,m&t)
```

```
exten => 1,2,Voicemail(1001@default) ;здесь работает так: если SIP/1001 не ответил в течении 30 секунд или сбросил звонок, попадаем на его личный автоответчик 1001@default
```

```
exten => 2,1,Dial(SIP/1002,30,m&t)
```

```
exten => 2,2,Voicemail(1002@default) ;здесь работает так: если SIP/1002 не ответил в течении 30 секунд или сбросил звонок, попадаем на его личный автоответчик 1002@default
```

```
exten => s,4,Wait(5)
```

```
exten => s,5,Dial(SIP/1001&SIP/1002,30,t&m)
```

```
exten => s,6,Goto(autoanswer,s,1)
```

```
[autoanswer]
```

```
exten => s,1,Background(/var/lib/asterisk/moh/autoanswer/busy)
```

```
exten => s,2,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
```

```
exten => s,3,Record(/var/www/html/voicemail/${fname}.wav,0,15,X)
```

```
exten => s,4,Hangup
```

4. Теперь настроим файл voicemail.conf

Выше был приведен шаблон. А вот как это выглядит в моем конкретном случае:

```
[default]
```

```
1001 => 123, Mikhail, maycal593@gmail.com
```

```
1002 => 456, Alexander, darkmaycal@gmail.com
```

в) Скачаем пакет русской локализации, написав:

```
wget http://downloads.asterisk.org/pub/telephony/sounds/asterisk-core-sounds-ru-alaw-current.tar.gz
```

г) Распакуем скаченный пакет:

```
tar xzf asterisk-core-sounds-ru-alaw-current.tar.gz
```

6.9 Перехват звонков. Pickup

7. Усиливаем безопасность Asterisk. 17 шагов которые сохранят Ваши деньги.

7.1 Меняем SIP порт

7.2 Запрещаем чужакам SIP подключение

Покажу на примере [1001]. У меня это выглядит так:

```
[1001]
deny=0.0.0.0/0.0.0.0
permit=192.168.0.1/24
type=friend
host=dynamic
insecure=invite
username=1001
secret=1234
context=outcoling
disallow=all
allow=alaw
mailbox=1001@default
language=ru
allowguest=no
```

7.3 Защищаем сервер от перебора по номерам

7.4 Устанавливаем более сильные пароли для sip-клиентов.

7.5 Запрещаем международные вызовы на уровне Dial плана

В конец контекста [outcoling] добавим следующие строки:

```
exten => _7810X.,1,System(echo «To» ${EXTEN} «Ext» ${CALLERID(num)} | mail -s «8-10 ALARM»  
test@gmail.com);
```

```
exten => _7810X.,n,Hangup()
```

7.6 Настройка встроенного фаерволла iptables.

заменяем на:

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  
-A INPUT -p icmp -j DROP  
-A INPUT -i lo -j ACCEPT  
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m multiport --dports 137,138,139,445 -j ACCEPT  
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  
-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT  
-A INPUT -s 192.168.0.0/24 -p udp -m state --state NEW -m udp --dport 3348 -j ACCEPT  
-A INPUT -p udp -m state --state NEW -m udp --dport 10000:20000 -j ACCEPT  
-A INPUT -j REJECT --reject-with icmp-host-prohibited  
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
```

7.7 Изменяем порт SSH, запрещаем пользователю логиниться как root через ssh, добавляем нового пользователя

7.8 Выключаем Apache из автозагрузки и меняем его порт

7.9 Отключаем ненужные модули и протоколы Asterisk

и в этот файл прописываем следующее:

```
noload => chan_jingle.so
noload => chan_skinny.so
noload => chan_iax2.so
noload => chan_console.so
noload => chan_mgcp.so
noload => chan_gtalk.so
```

7.10 Изменим порт управления Астериском (AMI)

7.11 Настраиваем систему fail2ban

Итак, подключаем репозиторий:

```
rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

Найдем и заменим секцию [ssh-iptables] на следующий код:

```
[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=1265, protocol=tcp]
        sendmail-whois[name=SSH, dest=test@gmail.com, sender=Fail2Ban]
logpath = /var/log/secure
maxretry = 3
```

2) Над секцией [ssh-iptables] вставим следующий код:

```
[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=ASTERISK, port=3348, protocol=udp]
        sendmail-whois[name=ASTERISK, dest=test@gmail.com, sender=Fail2Ban]
logpath = /var/log/asterisk/messages
maxretry = 3
bantime = 90
```

Все оттуда удалим и вставим следующее:

```
# Fail2Ban configuration file
#
#
# $Revision: 251 $
#
[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
before = common.conf

[Definition]

#_daemon = asterisk

# Option: failregex
# Notes.: regex to match the password failures messages in the logfile. The
#        host must be matched by a group named "host". The tag "<HOST>" can
#        be used for standard IP/hostname matching and is only an alias for
```

```
# (?:::f{4,6};)?(?P<host>\S+)
```

```
# Values: TEXT
```

```
#
```

```
# Asterisk 1.8 uses Host:Port format which is reflected here
```

```
failregex = NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Wrong password
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - No matching peer found
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - No matching peer found
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Username/auth name mismatch
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Device does not match ACL
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Peer is not supposed to register
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - ACL error (permit/deny)
```

```
NOTICE.* *: Registration from '.*' failed for '<HOST>:.*' - Device does not match ACL
```

```
NOTICE.* *: Registration from '".*"' failed for '<HOST>:.*' - No matching peer found
```

```
NOTICE.* *: Registration from '".*"' failed for '<HOST>:.*' - Wrong password
```

```
NOTICE.* <HOST> failed to authenticate as '.*'$
```

```
NOTICE.* *: No registration for peer '.*' \ (from <HOST> \)
```

```
NOTICE.* *: Host <HOST> failed MD5 authentication for '.*' (.*)
```

```
NOTICE.* *: Failed to authenticate user .*@<HOST>.*
```

```
NOTICE.* *: <HOST> failed to authenticate as '.*'
```

```
NOTICE.* *: <HOST> tried to authenticate with nonexistent user '.*'
```

```
VERBOSE.*SIP/<HOST>-.*Received incoming SIP connection from unknown peer
```

```
# Option: ignoreregex
```

```
# Notes.: regex to ignore. If this regex matches, the line is ignored.
```

```
# Values: TEXT
```

```
#
```

```
ignoreregex =
```

У меня это выглядит так:

```
[general]
dateformat=%F %T

[logfiles]
security => security
```

7.12 Защита от DOS атак.

2) после строчки:

```
-A INPUT -i lo -j ACCEPT
```

добавим 2 новых записи:

```
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --set --name dos-attack
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --update --seconds 2 --
hitcount 20 --name dos-attack -j DROP
```

7.13 Улучшение защиты от DOS атак

Найдем строку

```
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --update --seconds 2 --
hitcount 20 --name dos-attack -j DROP
```

и заменим её на

```
-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --update --seconds 2 --
hitcount 20 --name dos-attack -j LOG --log-level INFO --log-prefix "SIP flood detected: "
```

Так же, после этой строки вставим следующие 2 строки:

```
-A INPUT -p udp --dport 3348 -m recent --set --name dos-attack
-A INPUT -p udp --dport 3348 -m recent --update --seconds 2 --hitcount 20 --name dos-attack -j LOG --log-
level INFO --log-prefix "SIP flood detected: "
```

Весь конфиг iptables у меня выглядит так:

```
# Generated by iptables-save v1.4.7 on Sun Nov 17 20:29:31 2013

*filter

:INPUT ACCEPT [0:0]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [6781:1108542]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

-A INPUT -p icmp -j DROP

-A INPUT -i lo -j ACCEPT

-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --set --name dos-attack

-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --update --seconds 2 --hitcount 20 --name dos-attack -j LOG --log-level INFO --log-prefix "SIP flood detected: "

-A INPUT -p udp --dport 3348 -m recent --set --name dos-attack

-A INPUT -p udp --dport 3348 -m recent --update --seconds 2 --hitcount 20 --name dos-attack -j LOG --log-level INFO --log-prefix "SIP flood detected: "

-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m multiport --dports 137,138,139,445 -j ACCEPT

-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 1265 -j ACCEPT

-A INPUT -s 192.168.0.0/24 -p tcp -m state --state NEW -m tcp --dport 7623 -j ACCEPT

-A INPUT -s 192.168.0.0/24 -p udp -m state --state NEW -m udp --dport 3348 -j ACCEPT

-A INPUT -p udp -m state --state NEW -m udp --dport 10000:20000 -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-host-prohibited

-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT

# Completed on Sun Nov 17 20:29:31 2013
```

В этот файл вставляем следующее содержимое:

```
# Fail2Ban configuration file

#

#

# $Revision: 251 $

#

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
before = common.conf

[Definition]

#_daemon = asterisk

# Option: failregex
# Notes.: regex to match the password failures messages in the logfile. The
#       host must be matched by a group named "host". The tag "<HOST>" can
#       be used for standard IP/hostname matching and is only an alias for
#       (?:::f{4,6}:)?(?P<host>\S+)
# Values: TEXT
#
# Asterisk 1.8 uses Host:Port format which is reflected here

failregex = SIP flood detected: IN=. * OUT= MAC=. * SRC=<HOST> DST=. *
ignoreregex =
```

Там над секцией [asterisk-iptables] вставляем следующее:

```
[dos-attack]
enabled = true
filter = dos-attack
action = iptables-allports[name=dos-attack, protocol=all]
        sendmail-whois[name=DOS-ATTACKER, dest=test@gmail.com, sender=Fail2Ban]
logpath = /var/log/messages
maxretry = 3
bantime = 90
```

7.14 Защита от сканирования портов

1) Установка пакета

```
a) yum install gcc gcc-c++ make automake unzip zip xz kernel-devel-`uname -r` iptables-devel
б) yum install perl-Text-CSV_XS
в) wget http://downloads.sourceforge.net/project/iptables-addons/Xtables-addons/1.37/iptables-addons-1.37.tar.xz
г) tar xvf xtables-addons-1.37.tar.xz
д) cd xtables-addons-1.37/
е) ./configure
ж) make && make install
```

7.16 Отключение samba

7.15 Сертификация SSH

7.17 Дополнительная защита

7.18 Итоги обеспечения безопасности

8. Реализация дополнительных функций Asterisk

8.1 Конференц-связь Asterisk

1. Настройка confbridge.conf

и после раздела [general] напишем следующее:

```
[darkmaycalbridge]
type=bridge
max_members=20
mixing_interval=10
internal_sample_rate=auto
record_conference=yes

[generaluser]
type=user
music_on_hold_when_empty=yes
music_on_hold_class=default
announce_user_count_all=yes
announce_join_leave=yes
dsp_drop_silence=yes
denoise=yes
pin=456

[menu]
type=menu
*=playback_and_continue(conf-usermenu)
*1=toggle_mute
1=toggle_mute
*2=leave_conference
2=leave_conference
```



```
*4=decrease_listening_volume
4=decrease_listening_volume
*5=reset_listening_volume
5=reset_listening_volume
*6=increase_listening_volume
6=increase_listening_volume
*7=decrease_talking_volume
7=decrease_talking_volume
*8=reset_talking_volume
8=reset_talking_volume
*9=increase_talking_volume
9=increase_talking_volume
*0=no_op
0=no_op
```

2. Настройка extensions.conf

и в конец контекста [outcoling] добавим строчку:

```
exten => 100,1,ConfBridge(1234,darkmaycalbridge,generaluser,menu)
```

3. Добавляем функцию, при которой конференция не начнется, пока не придет её лидер.

б) Так же в файл confbridge.conf добавляем нового пользователя:

```
[adminuser]
type=user
music_on_hold_when_empty=yes
music_on_hold_class=default
announce_user_count_all=yes
announce_join_leave=yes
dsp_drop_silence=yes
```

```
denoise=yes
```

```
marked=yes
```

```
admin=yes
```

```
pin=123
```

в) Добавляем новое меню для администратора (с более расширенными функциями возможности закрытия конференции и кика других участников)

```
[admin_menu]
```

```
type=menu
```

```
*=playback_and_continue(conf-adminmenu)
```

```
*1=toggle_mute
```

```
1=toggle_mute
```

```
*2=admin_toggle_conference_lock ; only applied to admin users
```

```
2=admin_toggle_conference_lock ; only applied to admin users
```

```
*3=admin_kick_last ; only applied to admin users
```

```
3=admin_kick_last ; only applied to admin users
```

```
*4=decrease_listening_volume
```

```
4=decrease_listening_volume
```

```
*6=increase_listening_volume
```

```
6=increase_listening_volume
```

```
*7=decrease_talking_volume
```

```
7=decrease_talking_volume
```

```
*8=no_op
```

```
8=no_op
```

```
*9=increase_talking_volume
```

```
9=increase_talking_volume
```

4. Русифицируем

скачаем языковой пакет и распакуем его:

```
wget http://downloads.asterisk.org/pub/telephony/sounds/asterisk-core-sounds-ru-alaw-current.tar.gz
tar xzf asterisk-core-sounds-ru-alaw-current.tar.gz
```

5. Записи конференций

8.2 Парковка вызовов

В самый конец контекста [outcoling] напишем:

```
exten => 900,1,Park()
exten => _9XX,1,ParkedCall(${EXTEN})
exten => _XXX, hint, park:${EXTEN}@parkedcalls
```

8.3 Переадресация звонков (FollowMe)

В самый конец файла напишем:

```
[1001]
context => outcoling
number = 00000000000,40
```

То-есть находим там строчки:

```
exten => 1,1,Dial(SIP/1001,10,m&t)
exten => 1,2,Voicemail(1001@default)
```

и меняем их на

```
exten => 1,1,Answer()  
exten => 1,2,Dial(SIP/1001,10,m&t)  
exten => 1,3,FollowMe(1001)  
exten => 1,4,Voicemail(1001@default)
```

Весь контекст [menu] выглядит следующим образом:

```
[menu]  
exten => s,1,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})  
exten => s,2,MixMonitor(/var/www/html/callrecords/${fname}.wav)  
exten => s,3,Background(/var/lib/asterisk/moh/voicemail/voicemail)  
exten => 1,1,Answer()  
exten => 1,2,Dial(SIP/1001,10,m&t)  
exten => 1,3,FollowMe(1001)  
exten => 1,4,Voicemail(1001@default)  
exten => 2,1,Dial(SIP/1002,30,m&t)  
exten => 2,2,Voicemail(1002@default)  
exten => 3,1,ConfBridge(1234,darkmaycalbridge,adminuser,menu)  
exten => s,4,Wait(5)  
exten => s,5,Dial(SIP/1001&SIP/1002,30,t&m)  
exten => s,6,Goto(autoanswer,s,1)
```

```
[outcoling]  
exten => _1001,1,Answer()  
exten => _1001,n,Dial(SIP/1001,10,t&m)  
exten => _1001,n,FollowMe(1001)
```

8.4 Очередь звонков. Создаем Call-центр.

1. Настройка файла agents.conf

2. Настройка файла queues.conf

и в самый конец файла пишем:

```
[operators]
music = default
strategy = ringall
context = queue-out
autofill = yes
announce-position = limit
wrapuptime=50
announce-frequency = 30
announce-holdtime = yes
joinempty = yes
member => Agent/1001
member => Agent/1002
```

4. Проверяем работу системы.

5. Теперь рассмотрим более подробно строчки, которые мы написали в конфигах.

8.5 Работа Asterisk в зависимости от дня недели и времени суток

В этом файле найдем контекст [incoming] и заменим его содержимое следующим:

```
exten => _X.,1,GotoIfTime(00:00-23:59|sat-sun|*|*?workinghours,s,1)
exten => _X.,2,GotoIfTime(18:00-09:00|mon-fri|*|*?workinghours,s,1)
exten => _X.,3,Goto(menu,s,1)
```

б) После контекста incoming добавим новый контекст workinghours со следующим содержимым:

```
[workinghours]
```

```
exten => s,1,Background(/var/lib/asterisk/moh/worktime/workingtime)
```

```
exten => s,2,Set(fname=${STRFTIME(${EPOCH},,%Y%m%d%H%M)}-${CALLERID(number)}-${EXTEN})
```

```
exten => s,3,Record(/var/www/html/voicemail/${fname}.wav,0,8,X)
```

```
exten => s,4,Hangup
```

9. Заключение