



# *ZBilling*

## 1 Установка ZBilling (на примере Ubuntu 14.04 LTS)

Возьмем за исходный материал новую установку ubuntu 14.04 server.  
Произведем настройку сетевых интерфейсов:

```
sudo nano /etc/network/interfaces

auto lo eth0 eth1
iface lo inet loopback

# Интерфейс подключенный к локальной сети
iface eth0 inet static
    address 192.168.1.1
    netmask 255.255.255.0

# Интерфейс подключенный с сети Интернет
iface eth1 inet static
    address 10.10.10.2
    netmask 255.255.255.0
    gateway 10.10.10.1
```

Применим настройки:

```
sudo ifdown eth0 && ifup eth0 && ifdown eth1 && ifup eth1
```

Зададим DNS серверы в файле /etc/resolvconf/resolv.conf.d/base

```
sudo nano /etc/resolvconf/resolv.conf.d/base

nameserver 8.8.8.8
nameserver 8.8.4.4
```

Применим изменения.

```
sudo resolvconf -u
```

Обновим систему.

```
sudo apt-get update
sudo apt-get upgrade
```

Установим необходимые для работы ZBilling пакеты.

```
sudo apt-get install mysql-server mysql-client apache2 php5 libapache2-mod-php5
php5-mysql php5-gd ipset pmacct
```

Во время установки будет запрошен пароль для пользователя root для mysql – можете задать произвольный пароль.

Произведем настройку демона pmacct.

```
sudo nano /etc/pmacct/pmacctd.conf

! pmacctd configuration
!
```

```

!
!
daemonize: true
pidfile: /var/run/pmacctd.pid
syslog: daemon
! Зададим фильтр для нашей локальной сети
pcap_filter: not ip broadcast and not ip multicast and not ether broadcast and
dst net 192.168.0.0/16 and not src net 192.168.0.0/16
! Указываем интерфейс подключенный к локальной сети
interface: eth0
!
sql_recovery_logfile: /var/lib/pmacct/recovery_log
! Указанный пользователь и база данных mysql будут созданы на следующем шаге
установки
plugins: mysql
sql_db: zbilling
sql_table: netstat
sql_passwd: zbpasw
sql_user: zbuser
sql_refresh_time: 60
sql_optimize_clauses: true
aggregate: src_host,dst_host,dst_port,src_port
sql_history: 1m
sql_history_roundoff: mh
sql_dont_try_update: true

```

Произведем настройку iptables.

```
nano /etc/iptables.up.rules
```

```

# Разрешающие правила для доступа из локальной сети
-A INPUT -s 192.168.0.0/16 -j ACCEPT
-A INPUT -s 127.0.0.1 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
# Запрещаем все подключения извне
-A INPUT ! -s 192.168.0.0/16 -j REJECT --reject-with icmp-host-prohibited
# Разрешающие правила для маршрутизации локальной сети
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -d 192.168.0.0/16 -j ACCEPT
# Одни из ключевых правил разрешающих маршрутизацию пакетов с фильтрацией по
ipset для разрешенных пользователей и на «бесплатные» направления
-A FORWARD -m set -j ACCEPT --match-set freedest dst
-A FORWARD -m set -j ACCEPT --match-set iusers src
# Разрешаем весь трафик с самого сервера
-A FORWARD -s 127.0.0.1/32 -j ACCEPT
-A FORWARD -s 192.168.1.1/32 -j ACCEPT
-A FORWARD -s 10.10.10.2/32 -j ACCEPT
-A FORWARD -s 127.0.0.1 -j ACCEPT
# Подобного рода запрещающие правила нужны для «немедленного» обрыва сессий
запрещенных пользователей
-A FORWARD -p udp -m udp -m set -o eth1 -j REJECT --reject-with icmp-port-
unreachable ! --match-set iusers src.
-A FORWARD -p udp -m udp -m set -i eth1 -j REJECT --reject-with icmp-port-
unreachable ! --match-set iusers dst.
-A FORWARD -p tcp -m tcp -m set -o eth1 -j REJECT --reject-with tcp-reset !
--match-set iusers src.
-A FORWARD -p tcp -m tcp -m set -i eth1 -j REJECT --reject-with tcp-reset !
--match-set iusers dst.
-A FORWARD -m set -i eth1 -j REJECT --reject-with icmp-net-unreachable !

```

```

--match-set iusers dst.
-A FORWARD -m set -o eth1 -j REJECT --reject-with icmp-net-unreachable !
--match-set iusers src
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
COMMIT
*nat
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# Разрешаем прохождение icmp в Интернет из локальной сети
-A POSTROUTING -p icmp -o eth1 -j MASQUERADE
# 192.0.2.1 – зарезервирован для использования в документации, клиент
авторизации использует этот адрес в качестве адреса сервера по умолчанию.
# Перенаправляем его на сам сервер, при условии что сервер с Zbilling будет
шлюзом, клиенты смогут подключаться и по этому адресу.
-A PREROUTING -p tcp -m tcp -d 192.0.2.1 --dport 80 -j DNAT --to-destination
192.168.1.1
# Разрешаем доступ к «бесплатным» хостам
-A PREROUTING -p tcp -m tcp -m set -i eth0 --dport 80 -j ACCEPT --match-set
freedest dst
# Перенаправление на информационную страницу для неразрешенных пользователей
-A PREROUTING -p tcp -m tcp -m set -i eth0 --dport 80 -j DNAT --to-destination
192.168.1.1 ! --match-set iusers src
# Собственно сам NAT
-A POSTROUTING -m set -o eth1 -j MASQUERADE --match-set freedest dst
-A POSTROUTING -m set -o eth1 -j MASQUERADE --match-set iusers src
COMMIT
*mangle
:PREROUTING ACCEPT [3711:552910]
:INPUT ACCEPT [1099:78318]
:FORWARD ACCEPT [2597:472279]
:OUTPUT ACCEPT [1853:111283]
:POSTROUTING ACCEPT [3055:504480]
COMMIT

```

Скачаем и распакуем архив с zbilling

```

cd /tmp/
wget http://citsk.ru/files/zbilling-1.0.tar.bz2
tar -xvf zbilling-1.0.tar.bz2
cd zbilling-1.0/

```

Создадим необходимые каталоги и установим вспомогательные скрипты.

```

sudo mkdir /etc/zbilling/
sudo mkdir /usr/share/zbilling/
sudo cp zbd.php /usr/share/zbilling/zbd.php
sudo cp zbilling /etc/init.d/zbilling
sudo chown root:root /etc/init.d/zbilling
sudo chmod +x /etc/init.d/zbilling
sudo update-rc.d zbilling defaults 80

```

Выполним скрипт инициализации базы данных.

```
mysql -p < zbilling.sql
```

Копируем код web интерфейса в папку www

```
sudo cp -R html /var/www/
```

Удаляем индексный файл по умолчанию,

```
sudo rm /var/www/html/index.html
```

устанавливаем права

```
sudo chown -R www-data:www-data /var/www/html
```

Установим разрешения для /var/www

```
sudo nano /etc/apache2/apache2.conf
```

```
<Directory /var/www/html>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

Включим поддержку планировщика для mysql.

```
sudo nano /etc/mysql/my.cnf
```

добавить

```
event_scheduler=ON
```

в секцию [mysqld]

Включаем маршрутизацию.

```
sudo nano /etc/sysctl.conf
```

Раскомментируем строку:

```
net.ipv4.ip_forward=1
```

Применим внесенные изменения.

```
sudo sysctl -p
```

Добавим в автозагрузку небольшой скрипт:

```
nano /etc/init.d/local.autostart
```

```
#!/bin/sh
sleep 20
ipset -N iusers iphash
ipset -N freedest iphash
/sbin/iptables-restore < /etc/iptables.up.rules
```

```
chmod +x /etc/init.d/local.autostart
update-rc.d local.autostart defaults 80
```

Копируем вспомогательные скрипты.

```
sudo mkdir /usr/share/zbilling/  
sudo cp zbd.php /usr/share/zbilling/zbd.php  
sudo cp zbilling /etc/init.d/zbilling  
sudo chown root:root /etc/init.d/zbilling  
sudo chmod +x /etc/init.d/zbilling  
sudo update-rc.d zbilling defaults 80
```

Настроим основные параметры zbilling.

```
nano /etc/zbilling/config.ini
```

```
; Параметры базы данных  
db_name=zbilling  
db_user=zbusер  
db_pass=zbpas  
; Используемые внешние команды  
ipset=/sbin/ipset  
tc=/sbin/tc  
iusers=iusers  
logfile=/var/log/zbilling.log  
lan=eth0  
; Параметры шейпера  
lan_rate=1000Mbit  
wan_rate=100Mbit  
; Ограничение скорости для клиента по умолчанию  
cl_rate=80Mbit  
; Локальная сеть  
local_net=192.168.0.0/16
```

Перезапустим службы.

```
sudo service mysql restart  
sudo service apache2 restart  
sudo service pmacct restart  
sudo service zbilling restart
```

## 2 Веб интерфейс

Стартовая страница системы доступна для всех пользователей локальной сети и содержит основную информацию о текущем пользователе, его тарифном плане и потреблению трафика за текущий период.

Основное меню программы выглядит следующим образом:



«**Главная**» - основная «приветственная» страница



Александр Викторович Руднев, добро пожаловать на страницу ZBilling

**Авторизация:**

Вы вошли как [имя] (авторизация по IP адресу)

Ваш тарифный план: **Безлимит 5Мбит**

**Баланс:**

Остаток: **Не ограничен**

**Потреблено трафика:**

за сегодня: **64 Мб**

за текущий месяц: **6.2 Гб**

**Отчеты по потреблению трафика:**

[Статистика](#)

[Динамика](#)

«Статистика» - отображает детальную статистику (по посещенным хостам и по использованным протоколам) по потреблению трафика для текущего пользователя.

**Статистика**

Статистика потребления трафика.

[По хостам](#) | [По протоколам](#)

#	Хост			Трафик	
21	23.235.43.133			6.1 Кб	1
22	23.235.43.175			23.8 Кб	1
23	23.235.43.249			23.5 Мб	1
24	31.13.93.3			83.9 Кб	1
25	31.13.204.53			54 б	1
26	31.41.166.181			449 б	1
27	31.131.253.250			5.7 Мб	1
28	37.9.89.68			10.1 Кб	1
29	37.9.89.70			7.3 Кб	1
30	37.140.166.225			5.8 Кб	1
31	37.140.166.228			17.2 Кб	1
32	37.140.166.230			13.4 Кб	1
33	37.157.254.201			508 б	1
34	37.247.39.118			36.8 Мб	1
35	46.137.72.197			2.6 Кб	1
36	46.137.79.34			44.7 Кб	2
37	46.137.106.221			4.8 Кб	1
38	46.137.107.237			7.2 Кб	1
39	46.165.196.88			133.9 Кб	1
40	46.165.208.104			552 б	1

Найдено 836 строк, показаны 21 - 40

«Динамика» - графическое представление потребления трафика с течением времени.

## Статистика

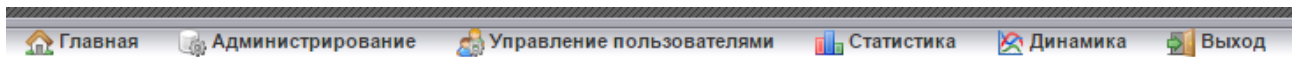
Распределение активности потребления трафика с течением времени.

За период | По дням недели | По времени



«Управление» - административный раздел веб интерфейса. Для входа в административную часть по умолчанию используется учетная запись «**administrator**» и пароль «**administrator**» (не забудьте поменять пароль на свой).

Основное меню в режиме администрирования выглядит следующим образом:



«**Главная**» - аналогична пользовательскому режиму.

### «Администрирование»

**Пользователи** — данный раздел служит для управления пользователями имеющими доступ к административной панели для администрирования и просмотра полной статистики потребления трафика пользователями.

Зарегистрированные в системе пользователи.

#	Логин	Полное имя	Сменить пароль	Администратор
1	administrator	Администратор		<input checked="" type="checkbox"/>

Найдено 1 строк, показаны 1 - 1

Страница 1 из 1  
Сохранить изменения

**Допустимые домены** — позволяет задать имена доменов допустимых при авторизации при помощи клиента. Имя домена необходимо указывать в коротком формате, то есть для домена example.local для корректной работы необходимо указать EXAMPLE.

Допустимые домены Active Directory.

#	Краткое имя домена	Комментарий	Разрешен
1	EXAMPLE	example.local	<input checked="" type="checkbox"/>

Найдено 1 строк, показаны 1 - 1

Страница 1 из 1  
Сохранить изменения

**Тарифные планы** — на данной странице доступны для просмотра редактирования и добавления тарифные планы используемые в программе.



## Тарифы.

#	Наименование тарифа	Соответствующая группа AD	Комментарий	Безлимит	Скорость kbps	Лимит трафика	Стоимость 1Mb	Единица измерения	Порог отключения
1	Безлимит 5Мбит	EXAMPLE#0.5120#Безлимит 5Мбит	Безлимит 5Мбит	<input type="checkbox"/>	5120	20	1	Mb	0

Найдено 1 строк, показаны 1 - 1

Страница 1 из 1

Сохранить изменения

**Общедоступные ресурсы** — на этой странице задаются хосты доступ к которым будет независим от статуса авторизации. Данный список ресурсов также будет отображен на главной странице. Для фильтрации доступа к ресурсам используется только ip адрес узла, поля url и отображаемое имя используются только для наглядного представления ресурсов в виде ссылок на главной странице.

### Добавление нового ресурса

IP	<input type="text"/>
URL	<input type="text"/>
Отображаемое имя ресурса	<input type="text"/>
Комментарий	<input type="text"/>
<input type="checkbox"/> Не отображать	

«**Управление пользователями**» - служит для редактирования списка пользователей имеющих доступ к сети Интернет. На этой странице также возможно добавление новых пользователей.

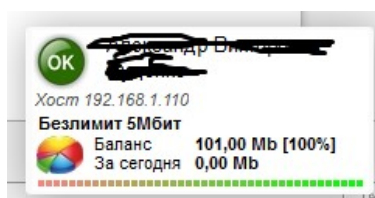
## Список пользователей Интернет.

#	Имя	Тариф	Баланс	Начислено	Трафик	Вход	Управление
1	[REDACTED]	Безлимит 5Мбит	101.00	101 Мб	0 б	192.168.1.110	n/a

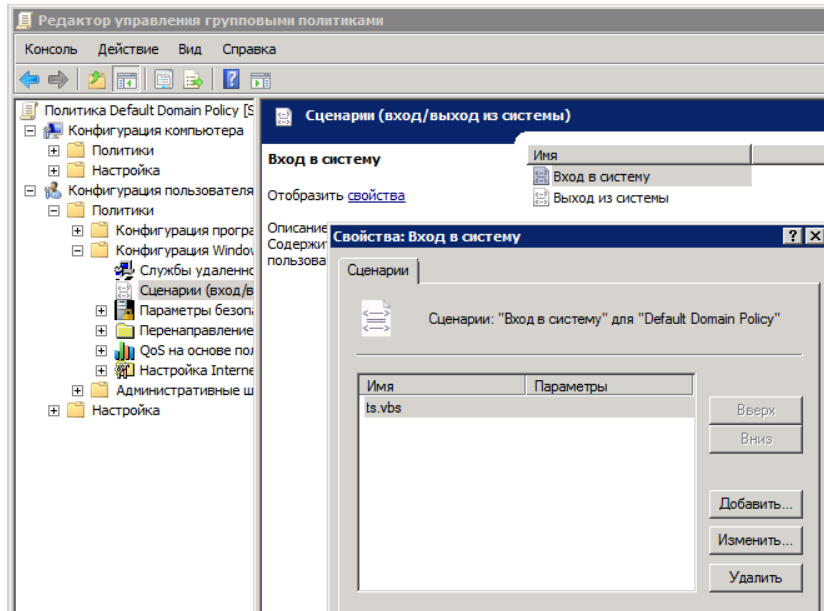
«**Статистика**», «**Динамика**» - аналогичны страницам для пользователей, но позволяет просматривать статистику по всем пользователям.

## 3 Интеграция с Active Directory, клиент авторизации

Программа поддерживает интеграцию со службами каталогов. Для авторизации используется клиент авторизации запускаемый на рабочих станциях.



Для автоматизации запуска клиента удобно использовать групповые политики и общедоступные сетевые ресурсы, в частности скрипт входа пользователя в систему.



Скрипт запуска ts.vbs в общем виде может иметь следующий вид:

```
on error resume next
```

```
set wshNetwork = WScript.CreateObject( "WScript.Network")
```

```
Set WSHShell = CreateObject("WScript.Shell")
```

```
Set objFSO = CreateObject("Scripting.FileSystemObject")
```

```
do while WSHNetwork.username = ""
```

```
    WScript.Sleep 250
```

```
loop
```

```
Set Env = WshShell.Environment("Process")
```

```
Env("__COMPAT_LAYER")="runasinvoker"
```

```
cfgInternetGroup = "Пользователи Интернет" 'Группа AD членам которой доступ в Интернет разрешен
```

```
SysShare = "\\example.local\sysshare$"
```

```
function IsMember(Group) ' Является ли пользователь членом группы
    dim lAdsPath, lUser, lGroup
    if IsEmpty(lGroupDict) then
        set lGroupDict = CreateObject("Scripting.Dictionary")
        lGroupDict.CompareMode = vbTextCompare
        lAdsPath = WshNetwork.UserDomain & "/" & WshNetwork.UserName
    on error resume next
        set lUser = GetObject("WinNT://" & lAdsPath & ",user")
        if Err.Number then
            IsMember = false
            exit Function
        End IF
    on error Goto 0
        for each lGroup in lUser.Groups
            lGroupDict.Add lGroup.Name, ""
        next
        set lUser = Nothing
    End If
    IsMember = CBool(lGroupDict.Exists(Group))
end Function
```

```
'Запуск клиента авторизации ZBilling
```

```
if IsMember(cfgInternetGroup) then
    if objFSO.FileExists(SysShare + "\zba.exe") then
        WshShell.Run SysShare + "\zba.exe"
        'Создание ярлыка
        DesktopPath = WSHShell.SpecialFolders("Desktop")
        Set oShellLink = WSHShell.CreateShortcut(DesktopPath + "\Интернет.lnk")
        ' Целевой путь к файлу для которого создаётся ярлык:
        oShellLink.TargetPath = SysShare + "\zba.exe"
        oShellLink.WindowStyle = 1
```

```
oShellLink.Save
end if
else
  if objFSO.FileExists(wshShell.SpecialFolders("Desktop") + "\Интернет.lnk")
  then
    objFSO.DeleteFile(wshShell.SpecialFolders("Desktop") + "\Интернет.lnk")
  end if
end if
```

Где "Пользователи Интернет" — имя группы Active Directory пользователям которой доступ к сети Интернет разрешен, а "[\\example.local\sysshare\\$](#)" путь к сетевому ресурсу где размещен исполняемый файл клиента авторизации.

Для работы клиента авторизации необходимо указать адрес сервера на котором установлен zbilling. По умолчанию клиент обращается к серверу с адресом 192.0.2.1 (данный адрес зарезервирован для использования в качестве примеров для документации) при условии что сервер с zbilling является одним из вышестоящих шлюзов для рабочей станции и настройки iptables на сервере выполнены в соответствии с инструкцией клиент сможет подключиться по этому адресу. Помимо этого адрес сервера можно задать (по приоритету использования):

1. В командной строке в виде «zba.exe server=<http://192.168.1.103/>».
2. В файле zba.ini из каталога с программой (если файла нет, его можно создать в любом текстовом редакторе).

Содержимое файла должно иметь следующий вид:

```
[server]
ServerName=http://192.168.1.103/
```

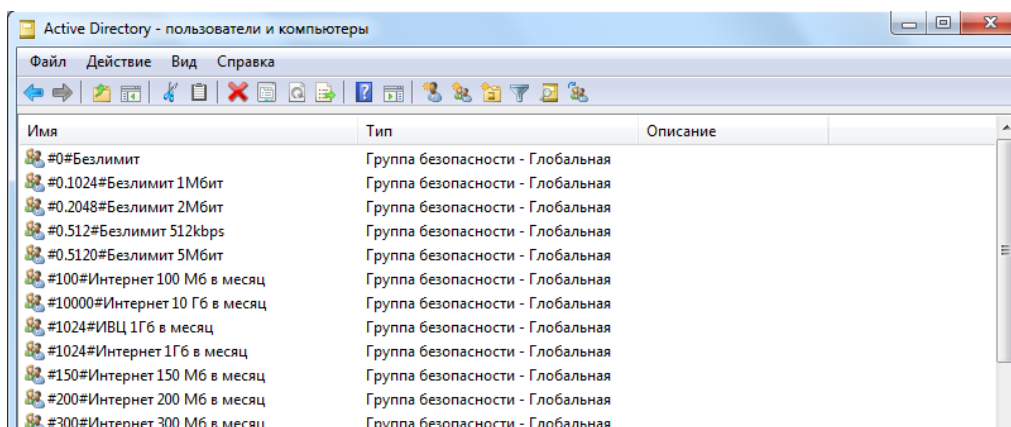
Где 192.168.1.103 ip адрес сервера Zbilling.

2. В ветви реестра HKCU\Software\Policies\zldo\zb\ServerName.

Для запуска отладочного режима служит ключ запуска программы «cdebug» например «zba.exe cdebug server=<http://192.168.1.103/>». При таком запуске программа во время работы будет вести лог файл «Log\ConectionsErrors.log» (относительно каталога с zba.exe).

После подключения клиента авторизации к серверу, исходя из параметров учетной записи Active Directory, пользователю будет предоставлен доступ к сети Интернет. При первом подключении будет создана учетная запись в системе и при необходимости тарифный план.

Для задания тарифных планов и разрешений доступа пользователей необходимо создать особые группы в Active Directory и включить необходимых пользователей в них (при обработке данных учитывается также и вложенность групп).



Имя	Тип	Описание
#0#Безлимит	Группа безопасности - Глобальная	
#0.1024#Безлимит 1Мбит	Группа безопасности - Глобальная	
#0.2048#Безлимит 2Мбит	Группа безопасности - Глобальная	
#0.512#Безлимит 512kbps	Группа безопасности - Глобальная	
#0.5120#Безлимит 5Мбит	Группа безопасности - Глобальная	
#100#Интернет 100 Мб в месяц	Группа безопасности - Глобальная	
#10000#Интернет 10 Гб в месяц	Группа безопасности - Глобальная	
#1024#ИВЦ 1Гб в месяц	Группа безопасности - Глобальная	
#1024#Интернет 1Гб в месяц	Группа безопасности - Глобальная	
#150#Интернет 150 Мб в месяц	Группа безопасности - Глобальная	
#200#Интернет 200 Мб в месяц	Группа безопасности - Глобальная	
#300#Интернет 300 Мб в месяц	Группа безопасности - Глобальная	

Синтаксис для имен специальных групп:

1. С ограничением по трафику -

*#ограничение в Mb в месяц#*отображаемое имя группы

2. С ограничением по скорости трафика

*#0.ограничение скорости в kbps#*отображаемое имя группы

3. Без ограничений:

*#0#*отображаемое имя группы

Если пользователь не включен не в одну из специальных групп, доступ с сети интернет для него будет заблокирован.