АВАН ТЕЛЕКОМ

Mikrotik в качестве фаервола для SIP сервера

Увеличивайте свою технологическую оснащенность

Проекты

АВАН ТЕЛЕКОМ

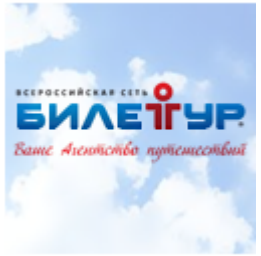
Авантелеком
Облака

VOIP-DV
www.voip-dv.ru

Т.8 800 333 44 56
sales@avantelecom.ru
www.avantelecom.ru

О компании

АВАН ТЕЛЕКОМ

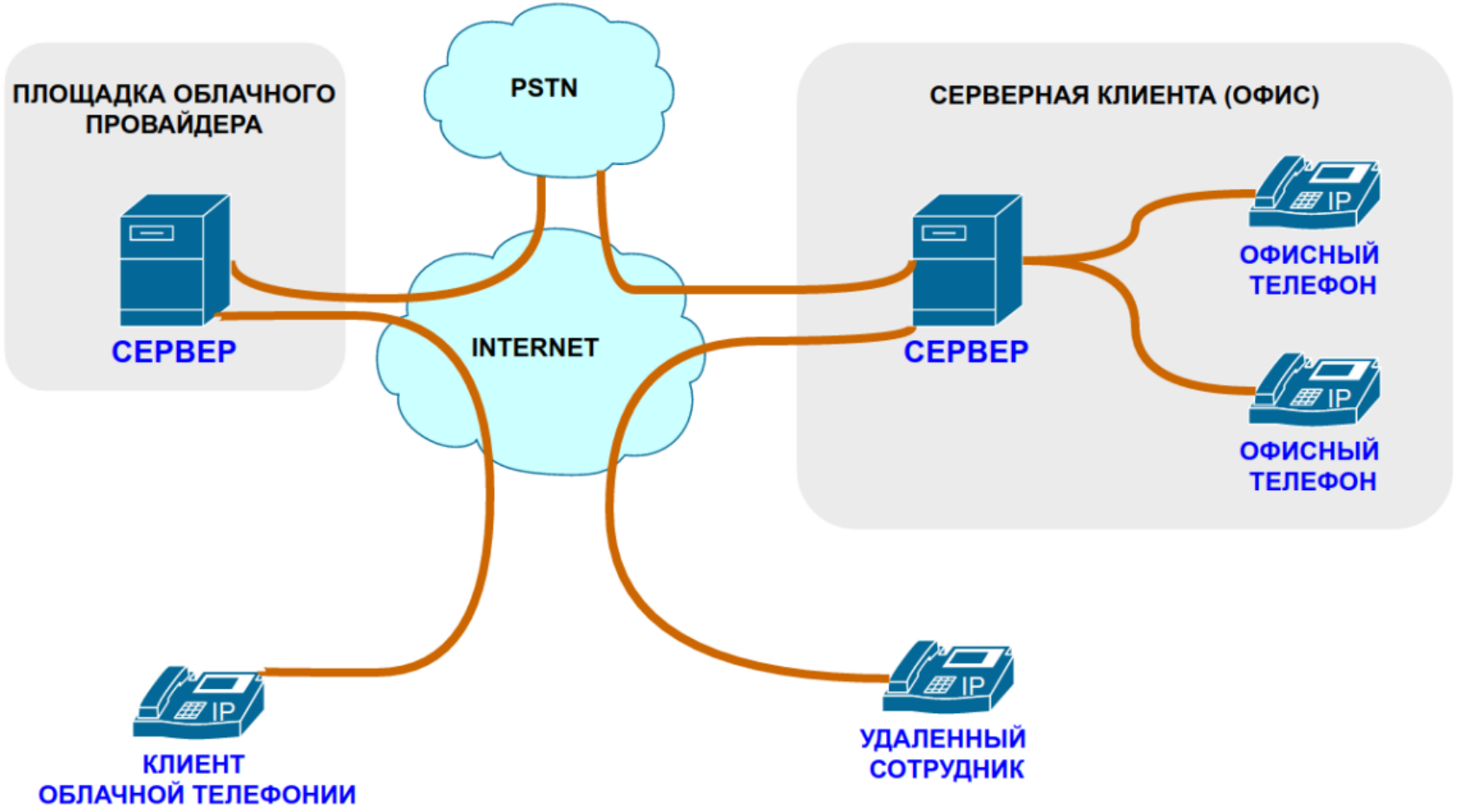


Т.8 800 333 44 56

sales@avantelecom.ru

www.avantelecom.ru

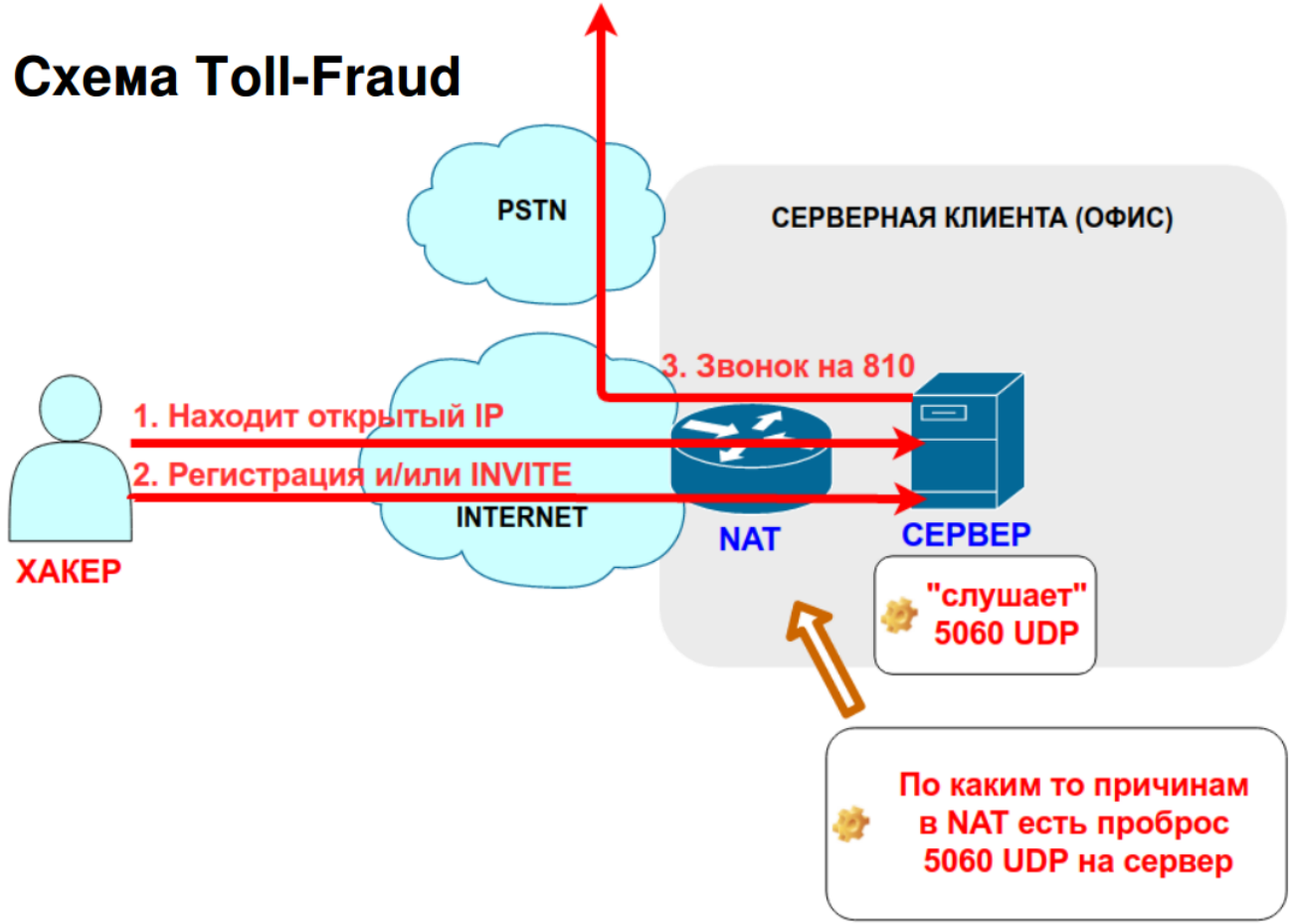
Обычно это так



Цели злоумышленников и типы атак

1. Перепродажа трафика (Toll-Fraud).
2. DDOS.
3. Кража или порча информации.

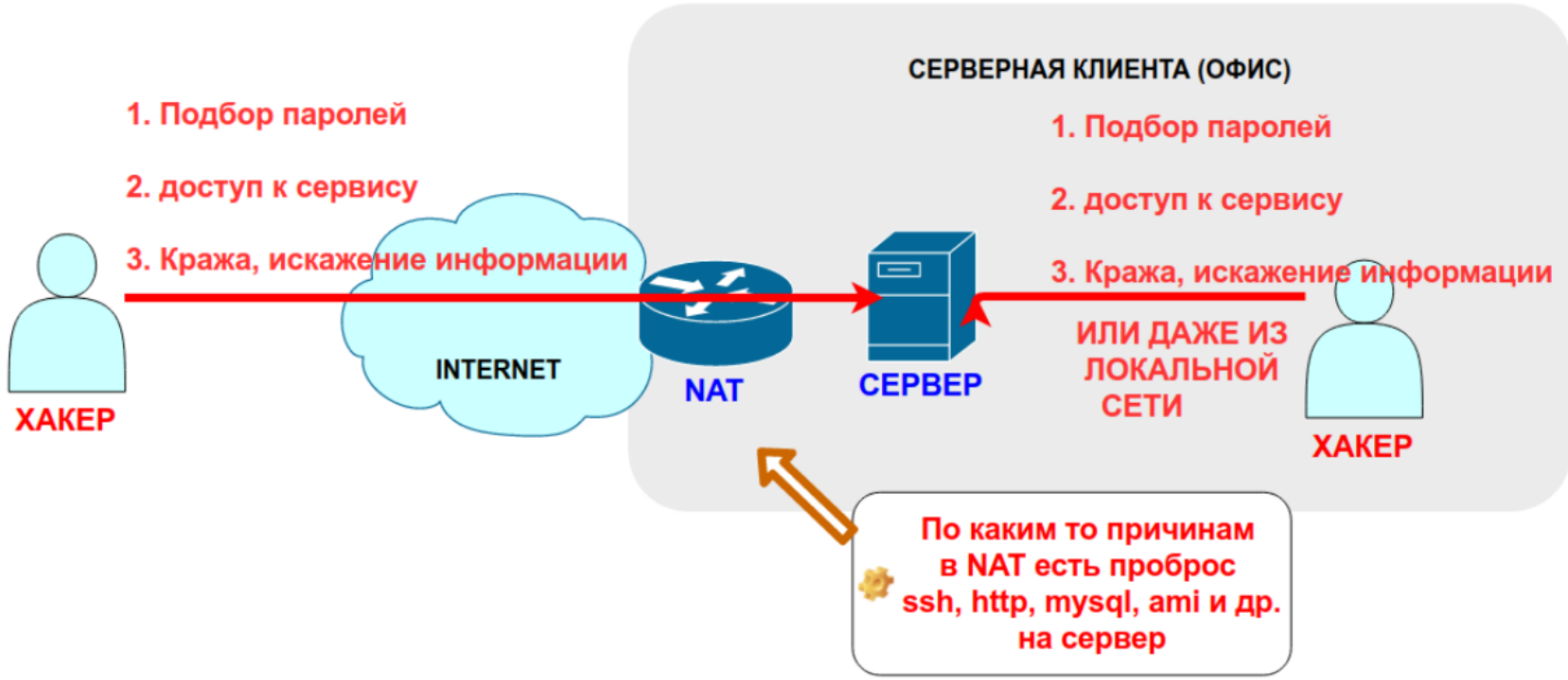
Toll-Fraud



Также сюда можно отнести взлом пароля AMI, пароля mysql, программных компонент, которые установлены на сервере и доступны из сети интернет (FreePBX, phpmyadmin)

Кража

Кража и(или) порча информации



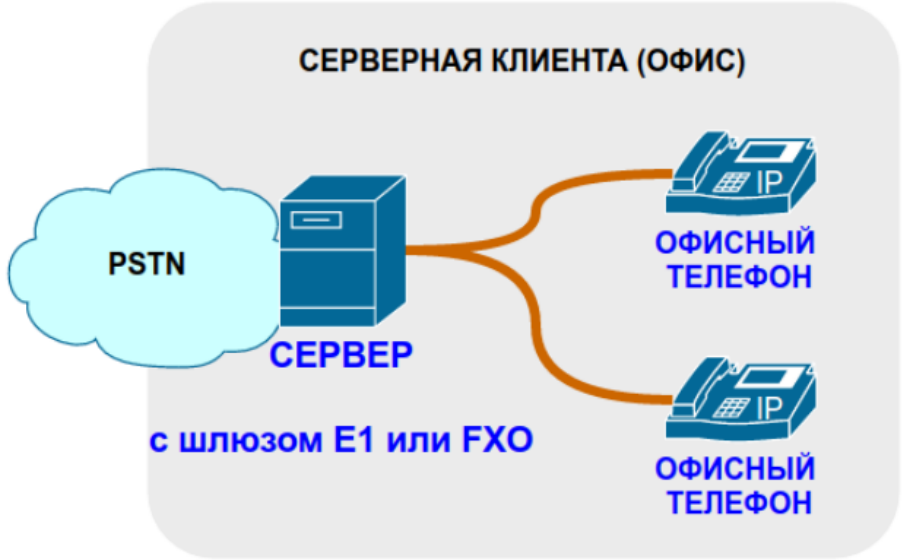
DDoS

- Обычный DDoS
- DDoS на SIP

Стандартные меры борьбы

- Настройка поведения sip на стороне asterisk
- Отключение анонимных звонков
- Использование контекста по умолчанию
- Использование списков доступа acl
- Использование iptables и fail2ban
- Использование сложных паролей
- Регулярное обновление по
- Использование микротик

Нет Интернета – нет проблем



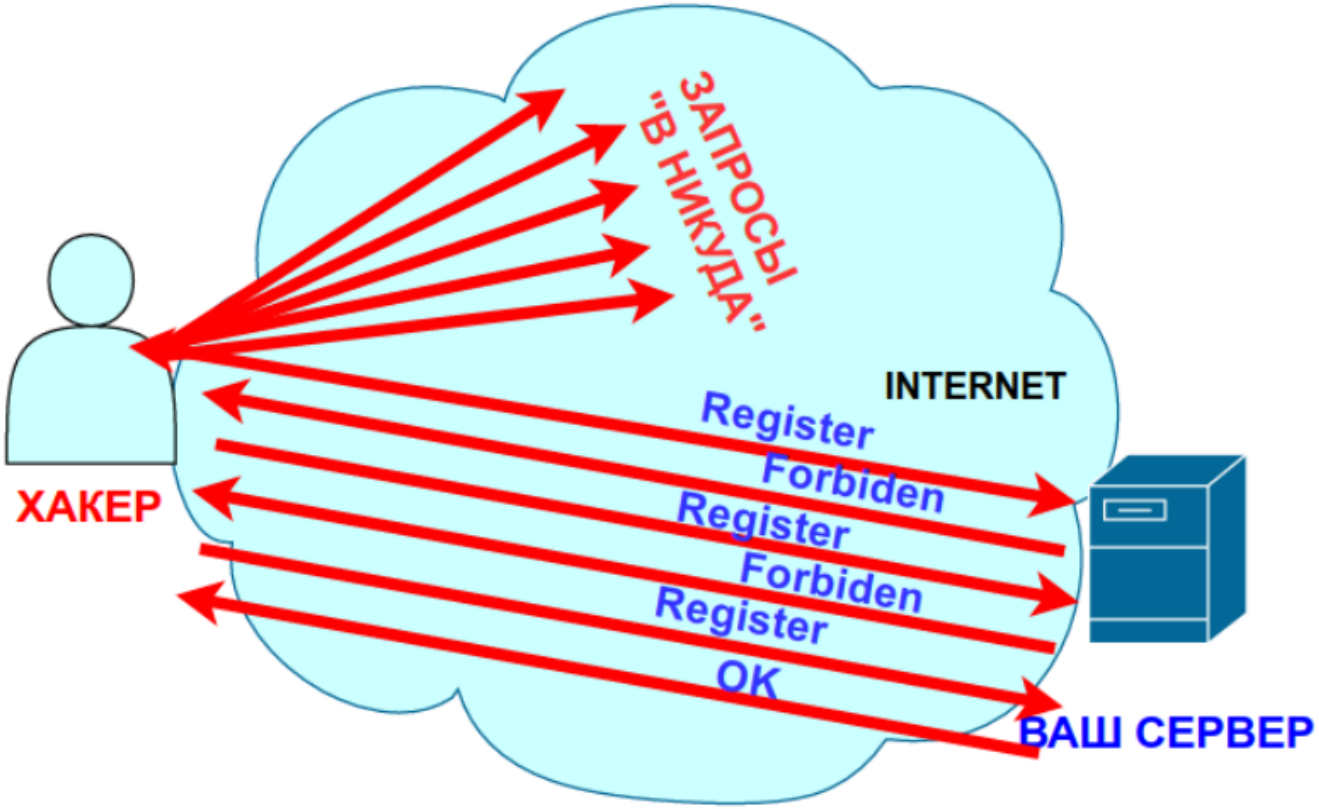
НО:

- **Нет подключения к любому провайдеру**
- **Нет интеграции с облачными CRM**
- **Нет удаленных подключений**

Основные способы защиты на Mikrotik

- **Блокировка иностранных сетей**
- **Использование приманок**
- **Fail2ban с обратной связью**
- **Лимит пакетов**
- **Регулярное обновление RouterOS и аудит журналов (в том числе потребления ресурсов)**

Нашли ваш сервер — случайность?



Ищет он простым перебором IP-адресов, посылая на порт 5060 (SIP), 4569 (IAX) и 5038 (AMI) запросы, либо (в общем случае) любой другой порт другого протокола. В SIP - это запросы на регистрацию или установления соединения

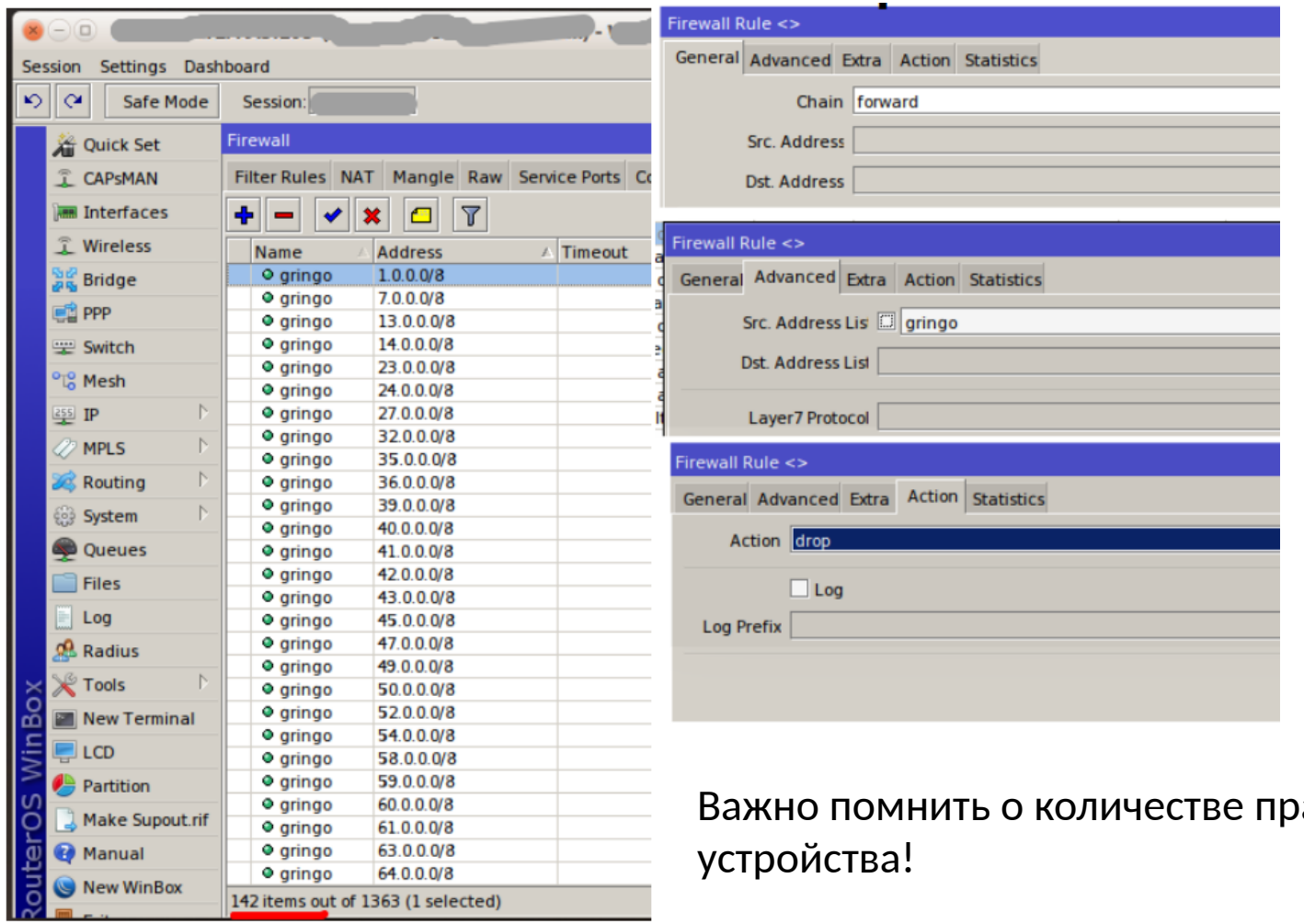
Блокируем всех иностранцев

Т.8 800 333 44 56

sales@avantelecom.ru

www.avantelecom.ru

Список и правило



Важно помнить о количестве правил и производительности устройства!

Схема хонипот (honeypot)

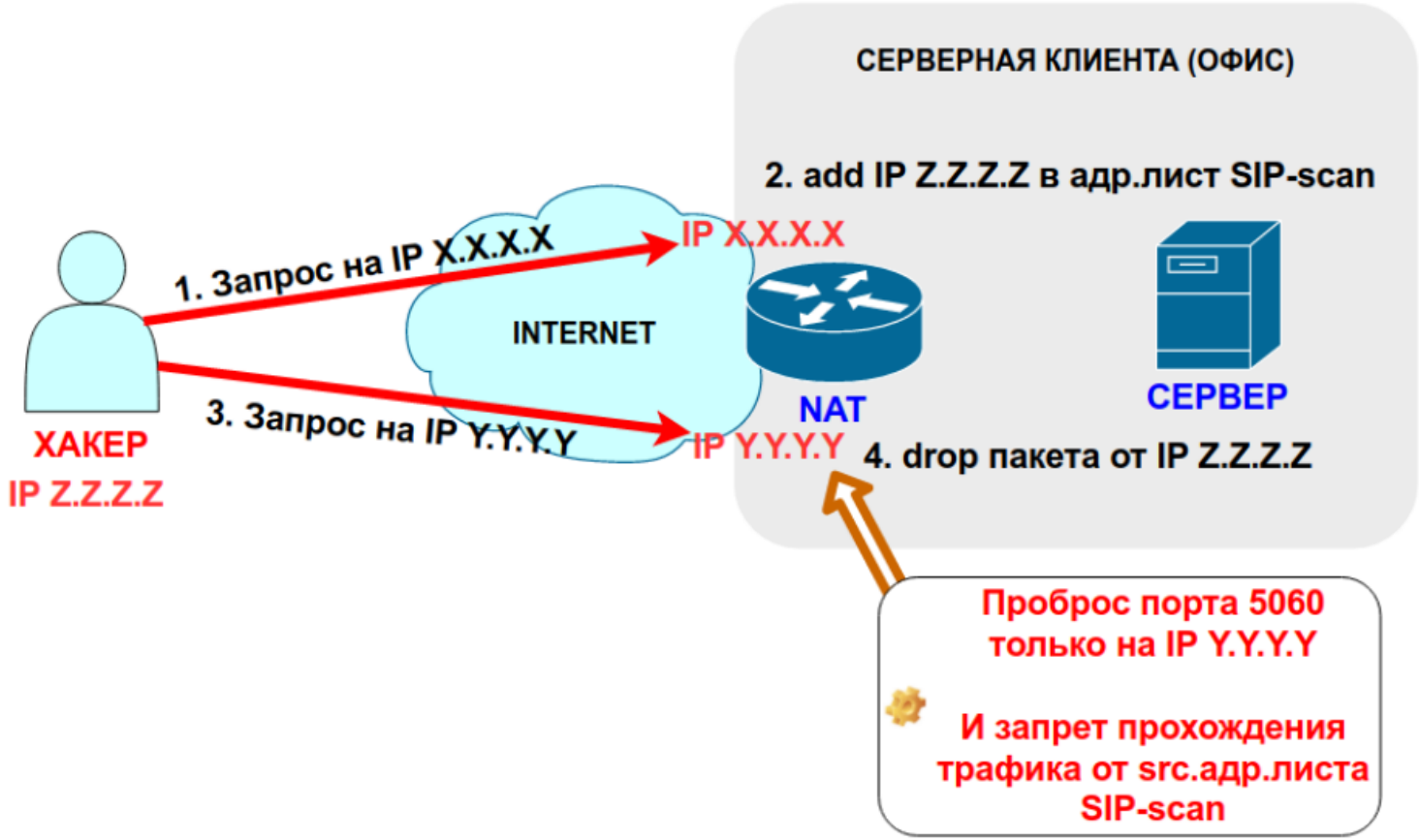
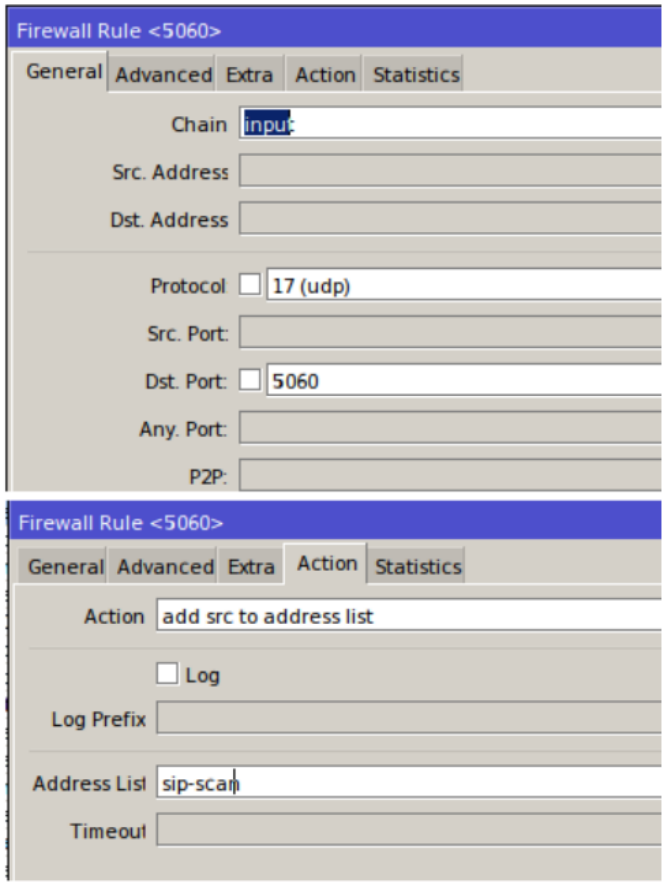
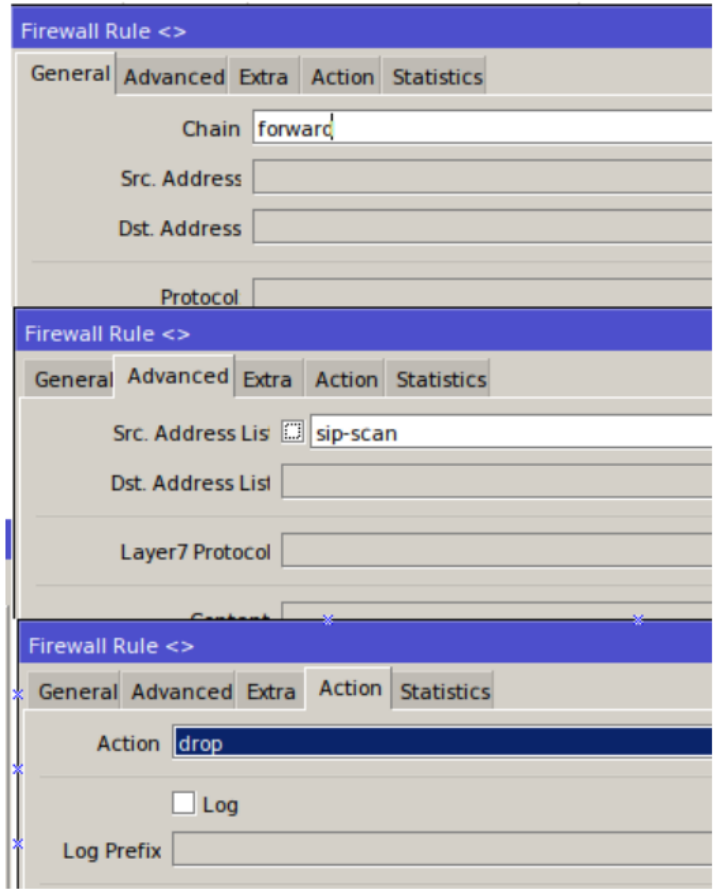


Схема хонипот (honeypot) - реализация

Добавляем



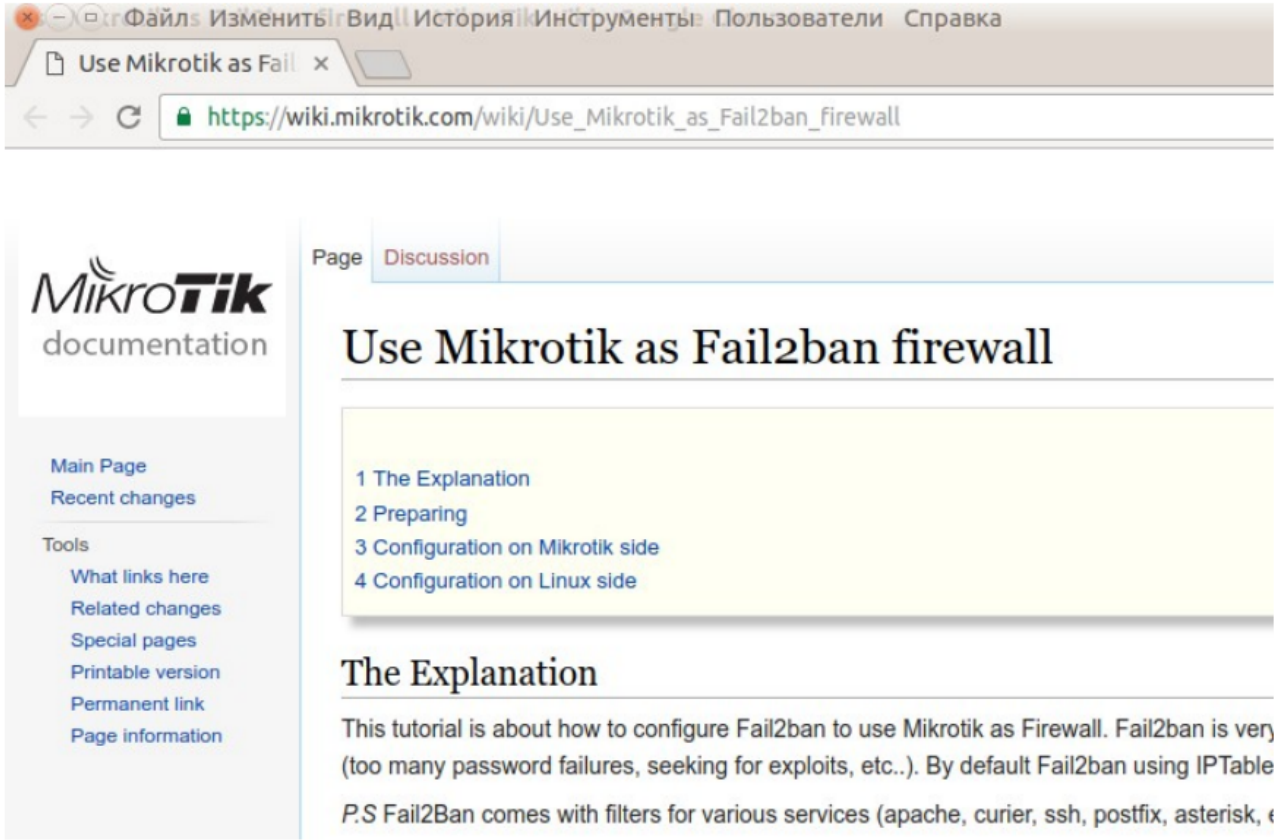
Ограничиваем



FAIL2BAN в связке с Mikrotik

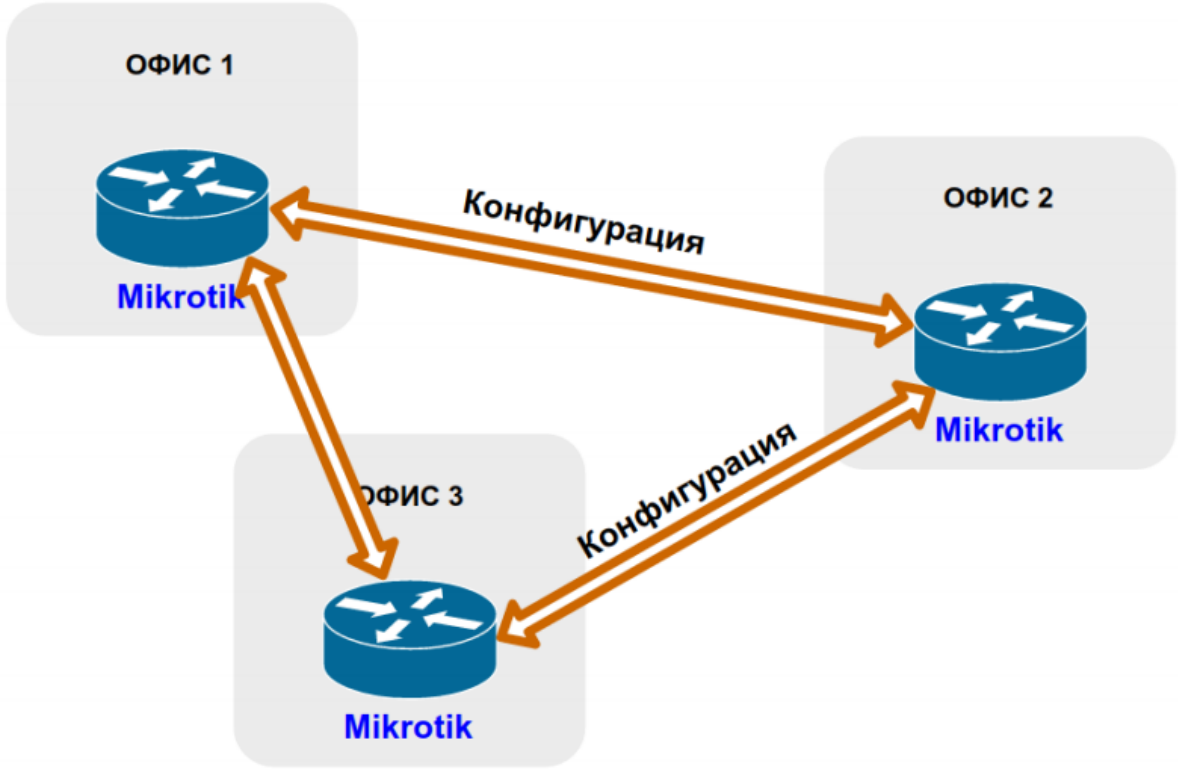
FAIL2BAN - реализация

Скрипт на оф. вики Mikrotik



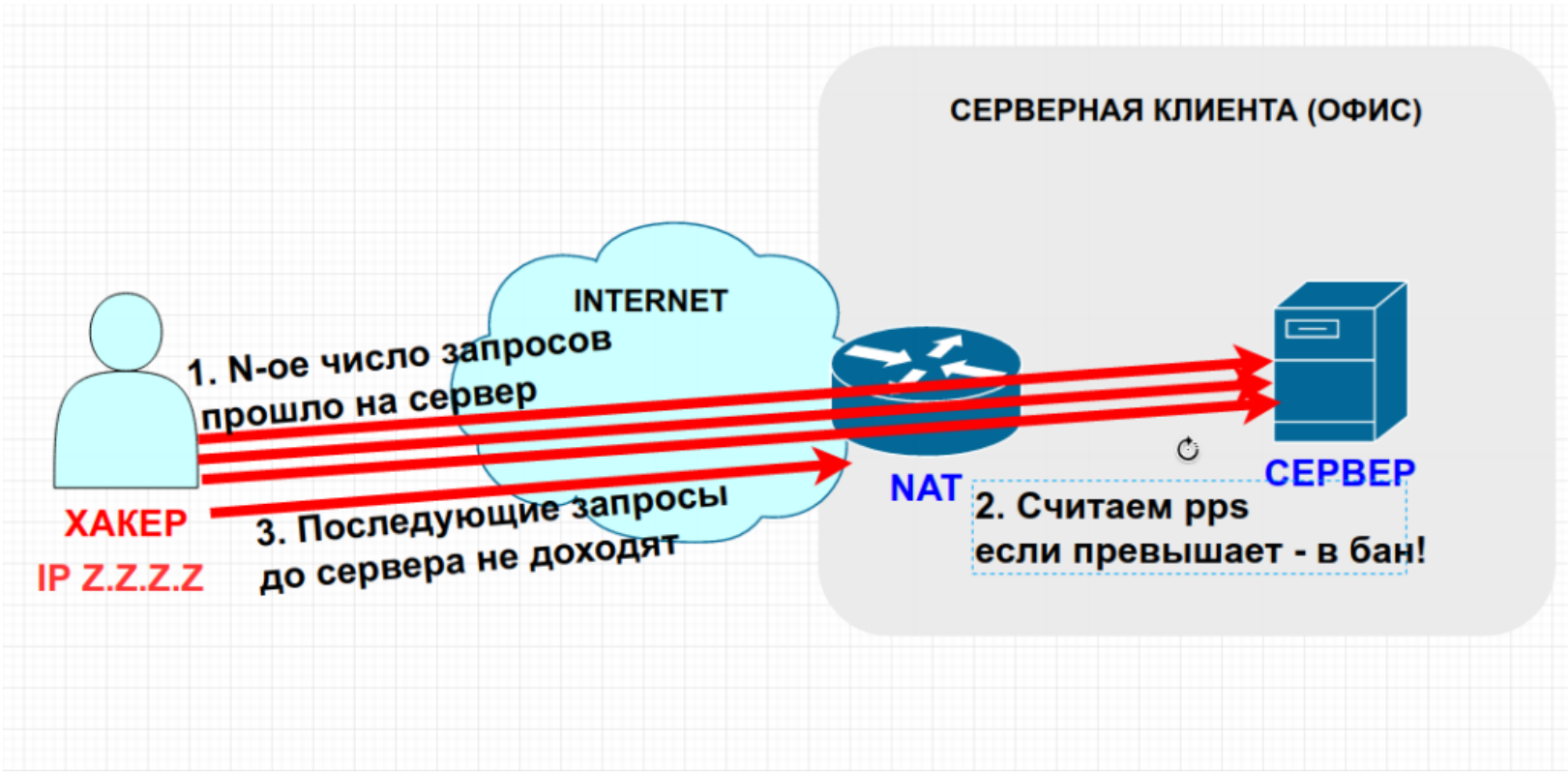
Адрес листы

Копируем адрес листы с одного на другой Микротик



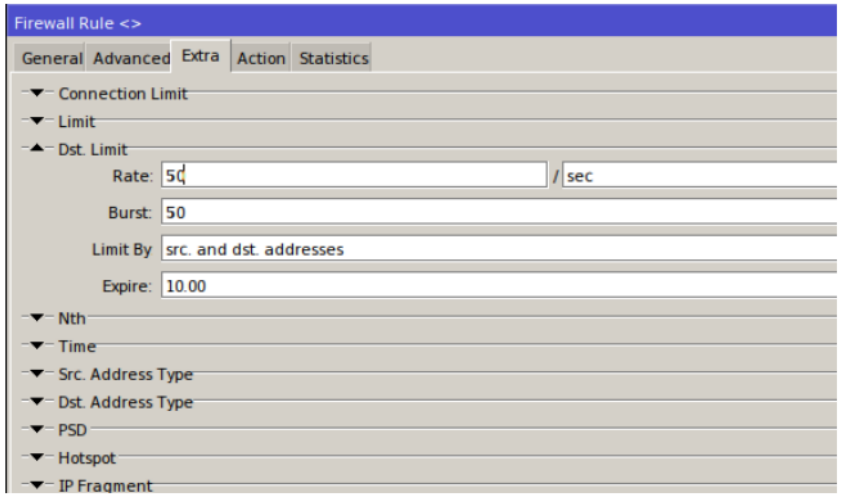
PPS

Ограничиваем pps

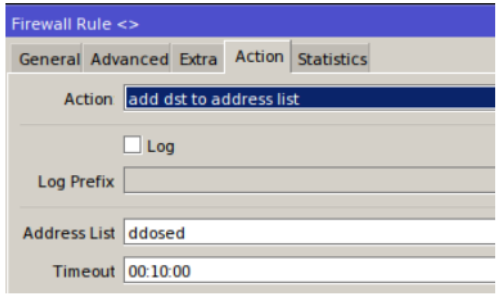


PPS - реализация

Пример проверки pps



До 50 pps еще ок, свыше блокируем



Адрес листы

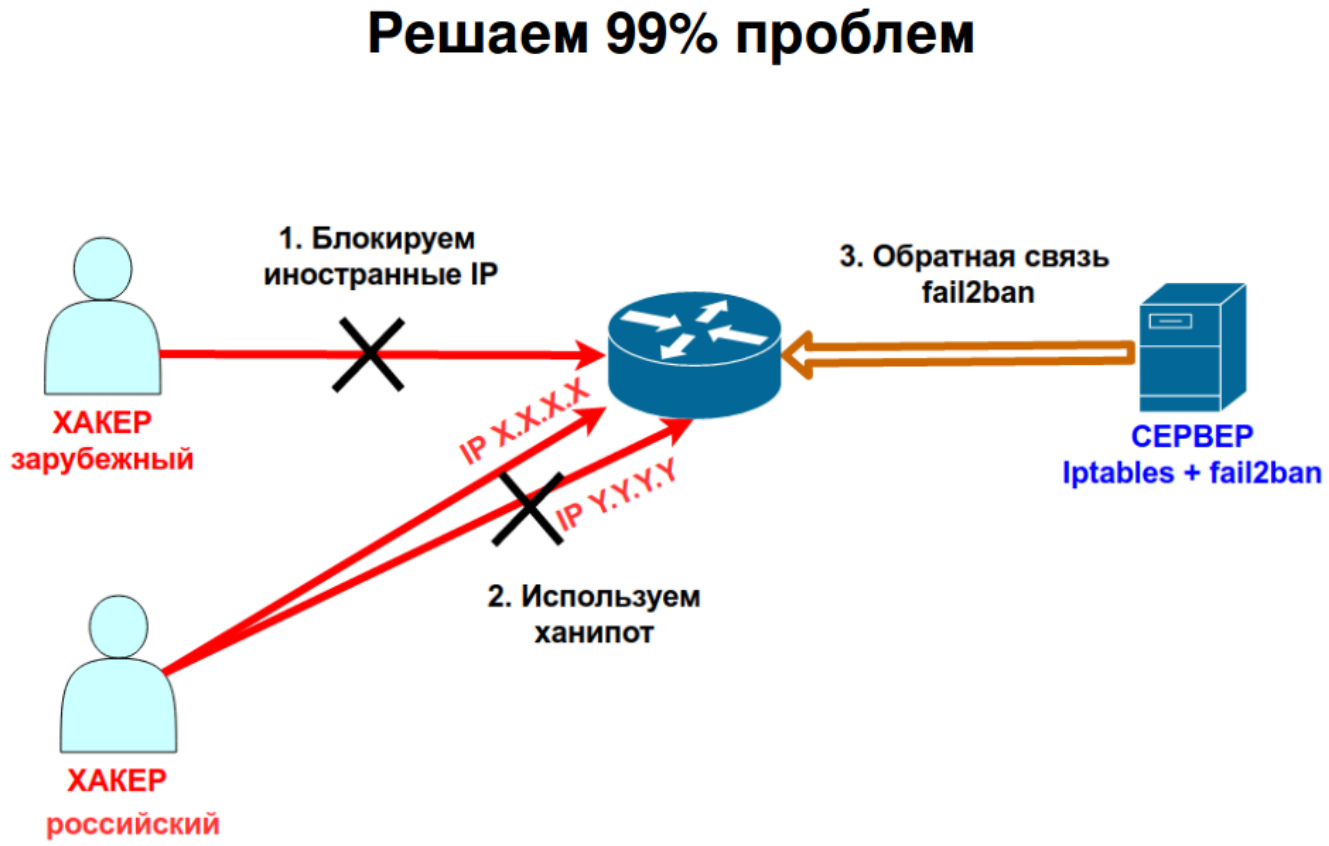
Скрипт конвертации динамических в статические адрес листов

```
# Convert dynamic to static in address-lists so dynamic records do not get deleted after a router reboot.
:local comment
:local address
:local list
:local disabled
:local found

:set found 0;

/ip firewall address-list
:foreach a in=[find] do={
  :if ([get $a dynamic] = true) do={
    /system logging disable 0
    :set found 1;
    :set comment [get $a comment]
    :set address [get $a address]
    :set list [get $a list]
    :set disabled [get $a disabled]
    remove $a
    add address=$address list=$list comment=$comment disabled=$disabled
  }
}
:if ($found=1) do={
/system logging enable 0
:log info "Dynamic to static conversion finished. System logging enabled."
:set found 0;
}
```

Схема фильтрации по регулярным выражениям

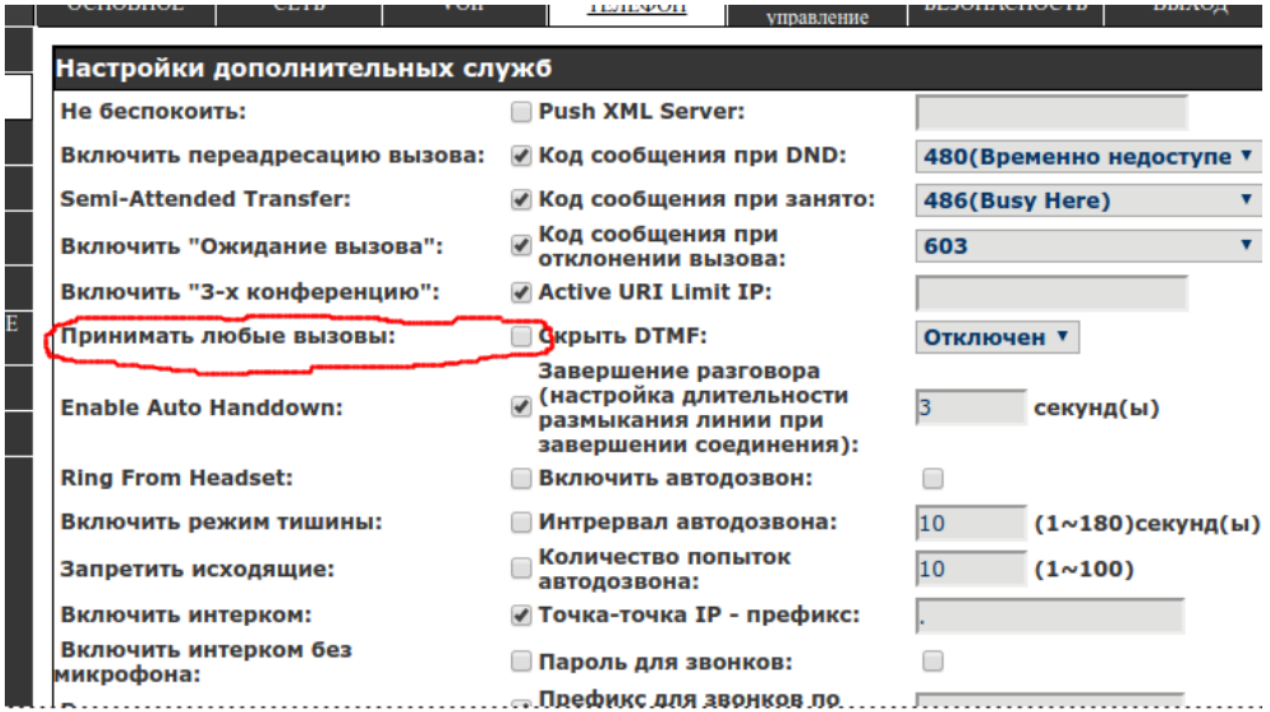
1. Анализ пакетов на содержание "403 Forbidden", считаем их
2. При определеном количестве добавляем IP Z.Z.Z.Z в адрес лист
3. Блокируем этот адрес лист

99 процентная связка защиты



Та самая «галка» про анонимные звонки

Настройка телефона



T.8 800 333 44 56

sales@avantelecom.ru

www.avantelecom.ru

Уведомление технической поддержки

Пошли звонки на 810…….

Уведомление технической поддержки

- Электронная почта
- SMS
- Alert в системе мониторинга

Выводы

www.avantelecom.ru

Мой личный мобильный

+7 914 777 36 80

Владислав Вирясов

Директор по развитию