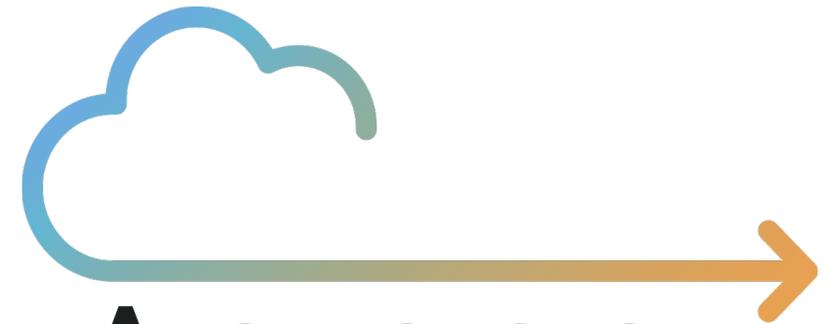
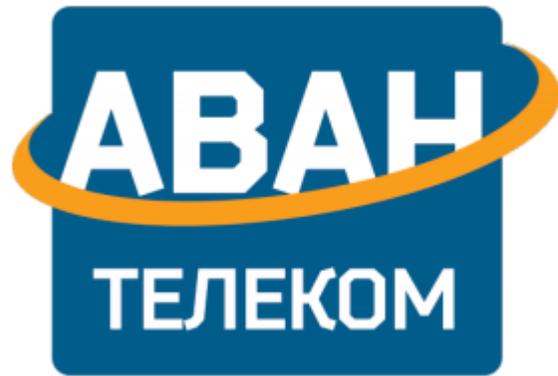




Мikrotik в качестве фаервола для SIP сервера

**Увеличивайте свою
технологическую оснащенность**

Проекты



Авантелеком

Облака



T.8 800 333 44 56

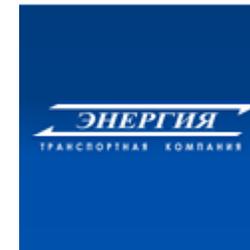
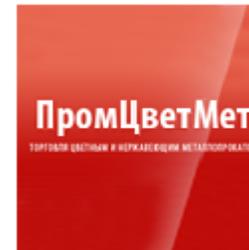
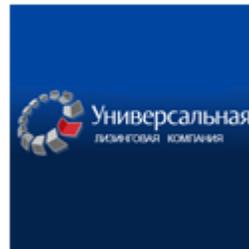
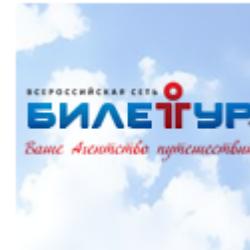


sales@avantelecom.ru



www.avantelecom.ru

0 компании



ХОРОШАЯ
СТРАХОВАЯ
КОМПАНИЯ



Т.8 800 333 44 56

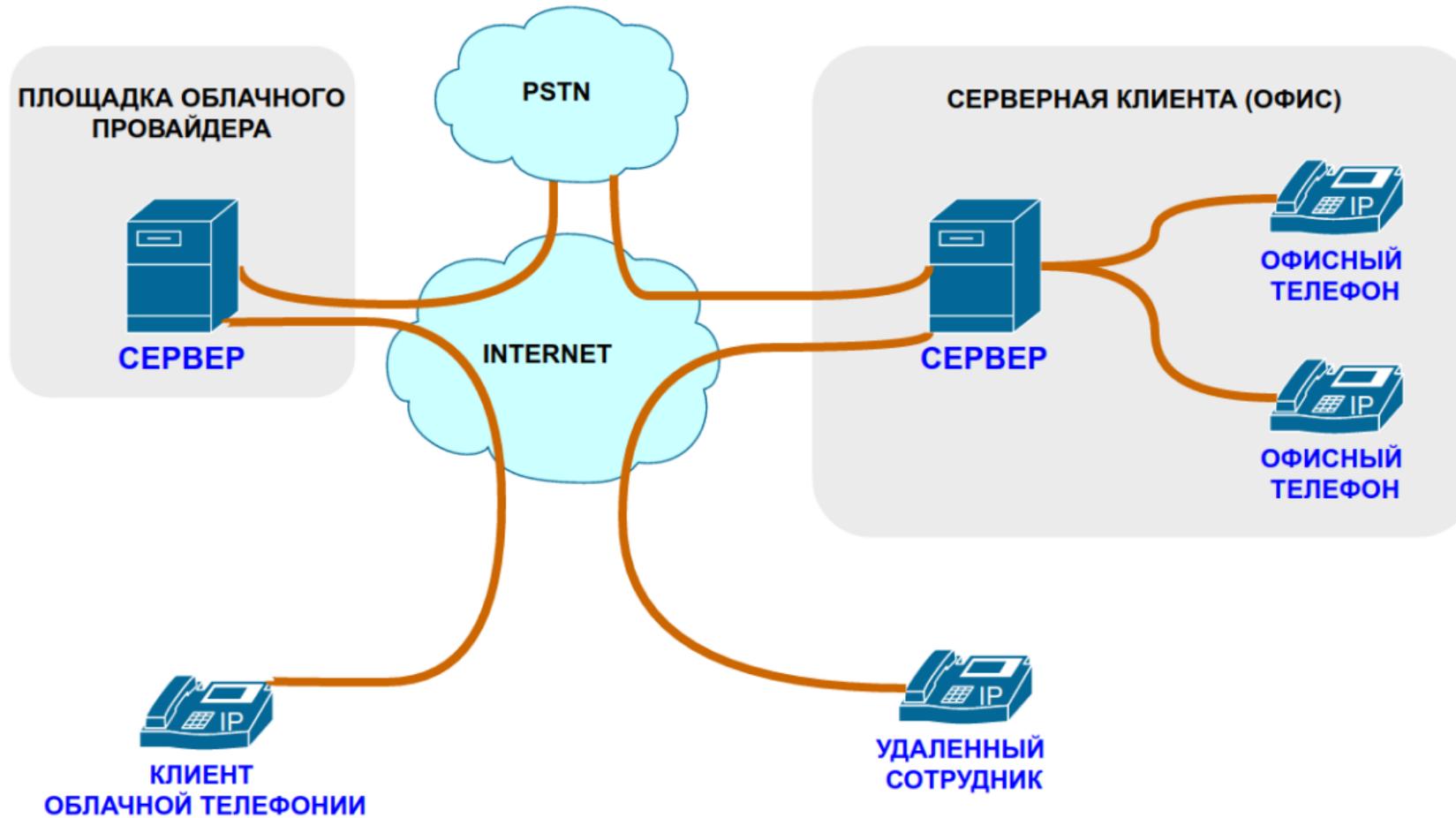


sales@avantelecom.ru



www.avantelecom.ru

Обычно это так



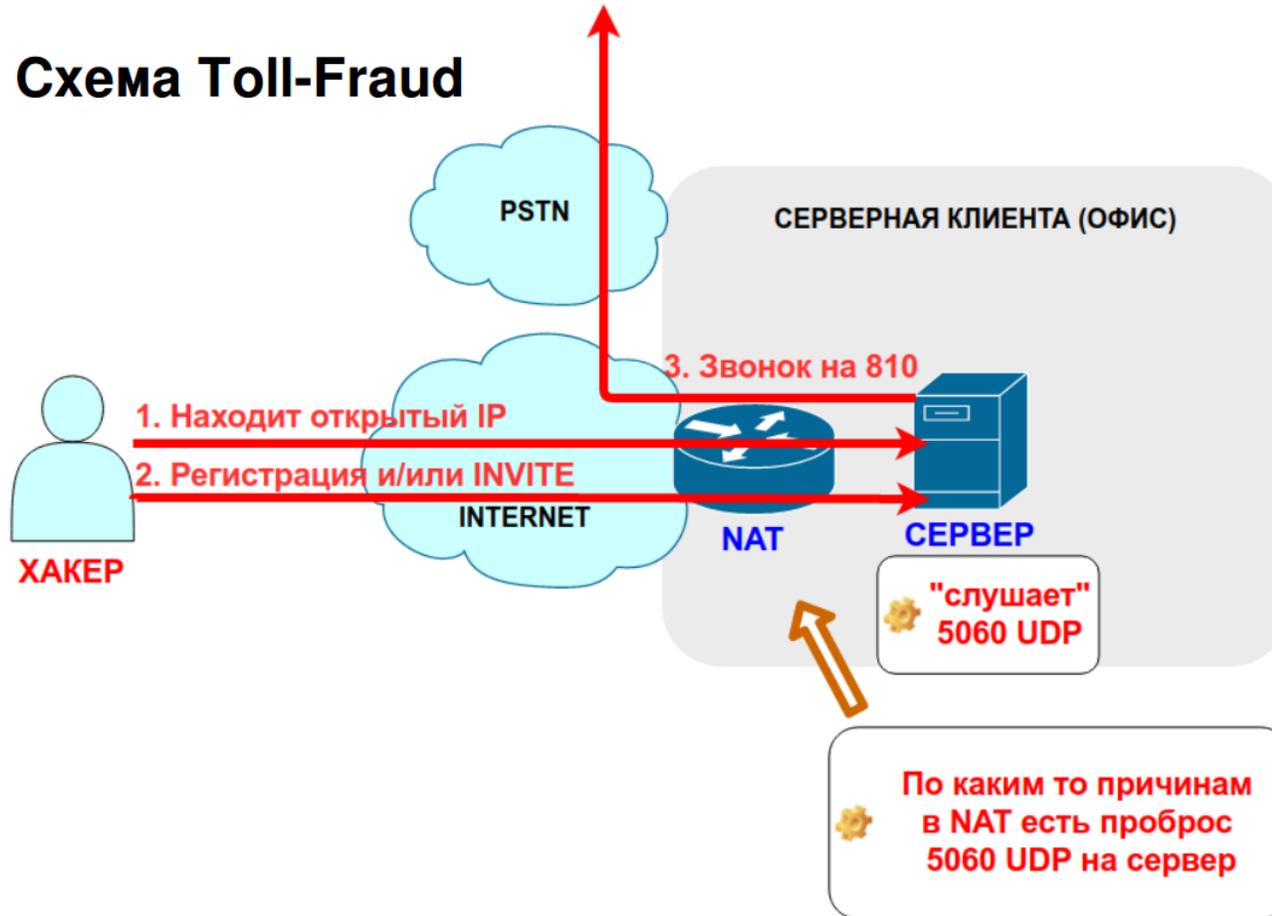
Цели злоумышленников и типы атак

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



Toll-Fraud

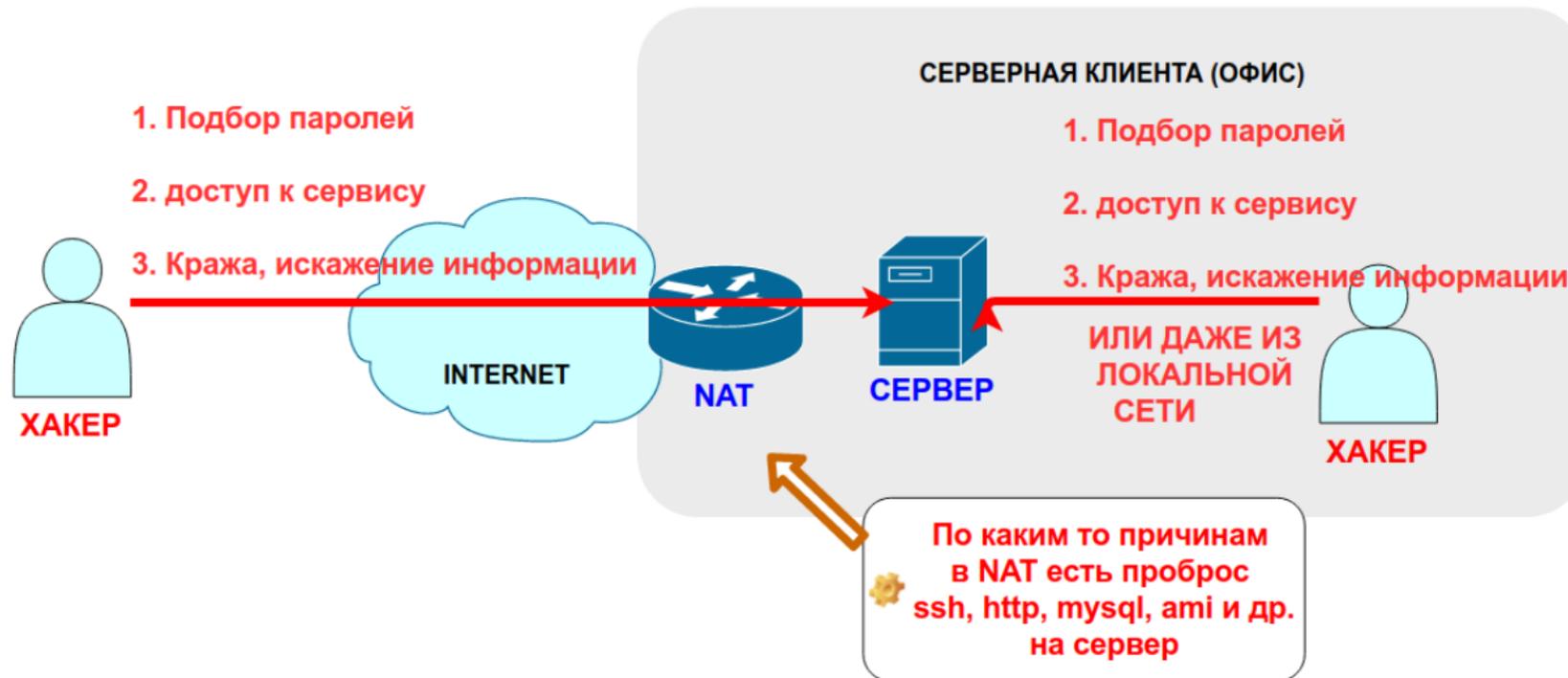
Схема Toll-Fraud



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

Кража

Кража и(или) порча информации



DDoS

- Обычный DDoS
- DDoS на SIP

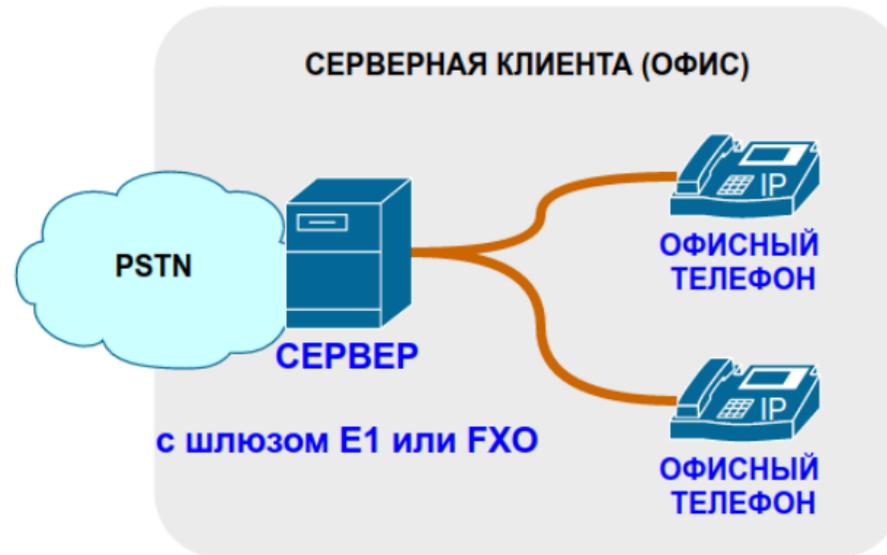


Стандартные меры борьбы

- 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:

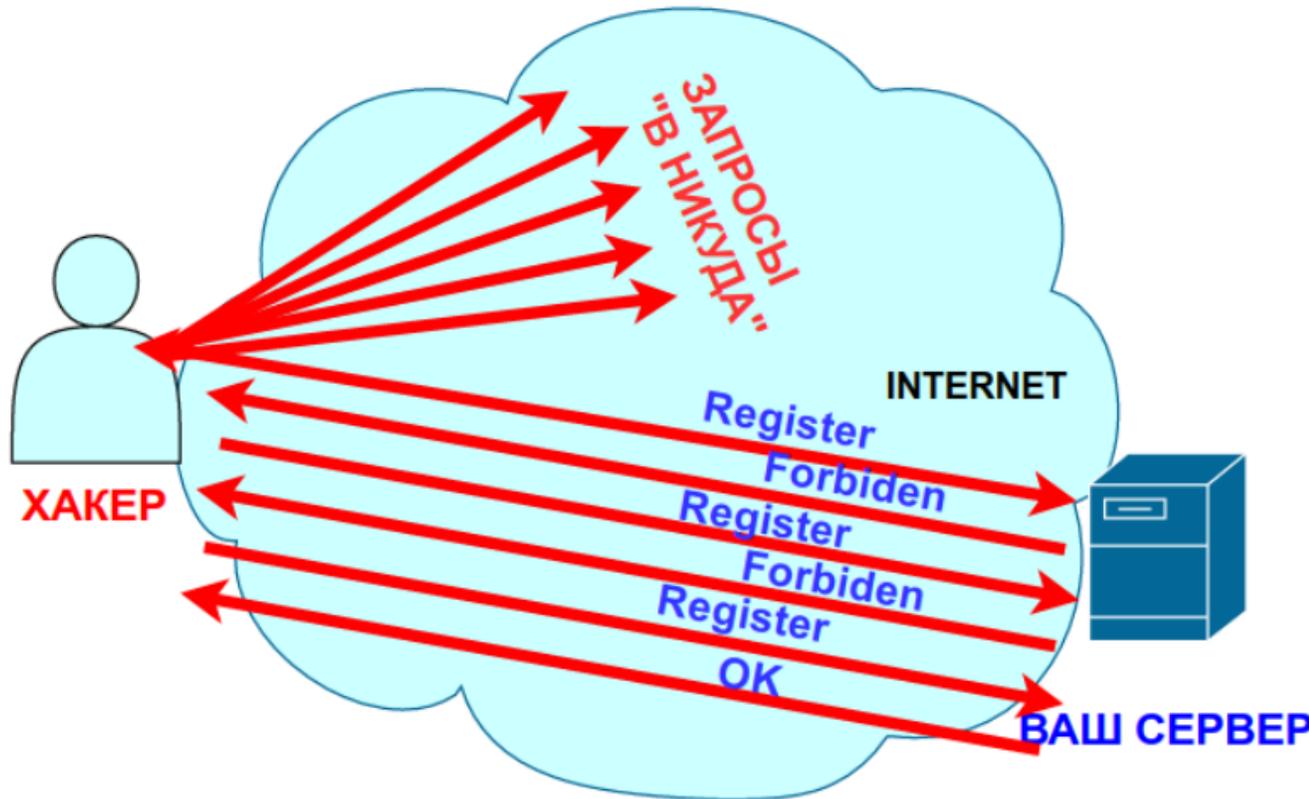
- Нет подключения к любому провайдеру
- Нет интеграции с облачными CRM
- Нет удаленных подключений

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



Список и правило

The screenshot displays the Mikrotik WinBox Firewall configuration interface. On the left, a list of firewall rules is shown, all named 'gringo' with various source addresses. On the right, three panels show the configuration for a specific rule:

- Firewall Rule <>** (General tab): Chain: forward, Src. Address: [empty], Dst. Address: [empty].
- Firewall Rule <>** (General tab): Src. Address List: gringo, Dst. Address List: [empty], Layer7 Protocol: [empty].
- Firewall Rule <>** (Action tab): Action: drop, Log: [unchecked], Log Prefix: [empty].

Важно помнить о количестве правил и производительности устройства!

Схема хонипот (honeypot)

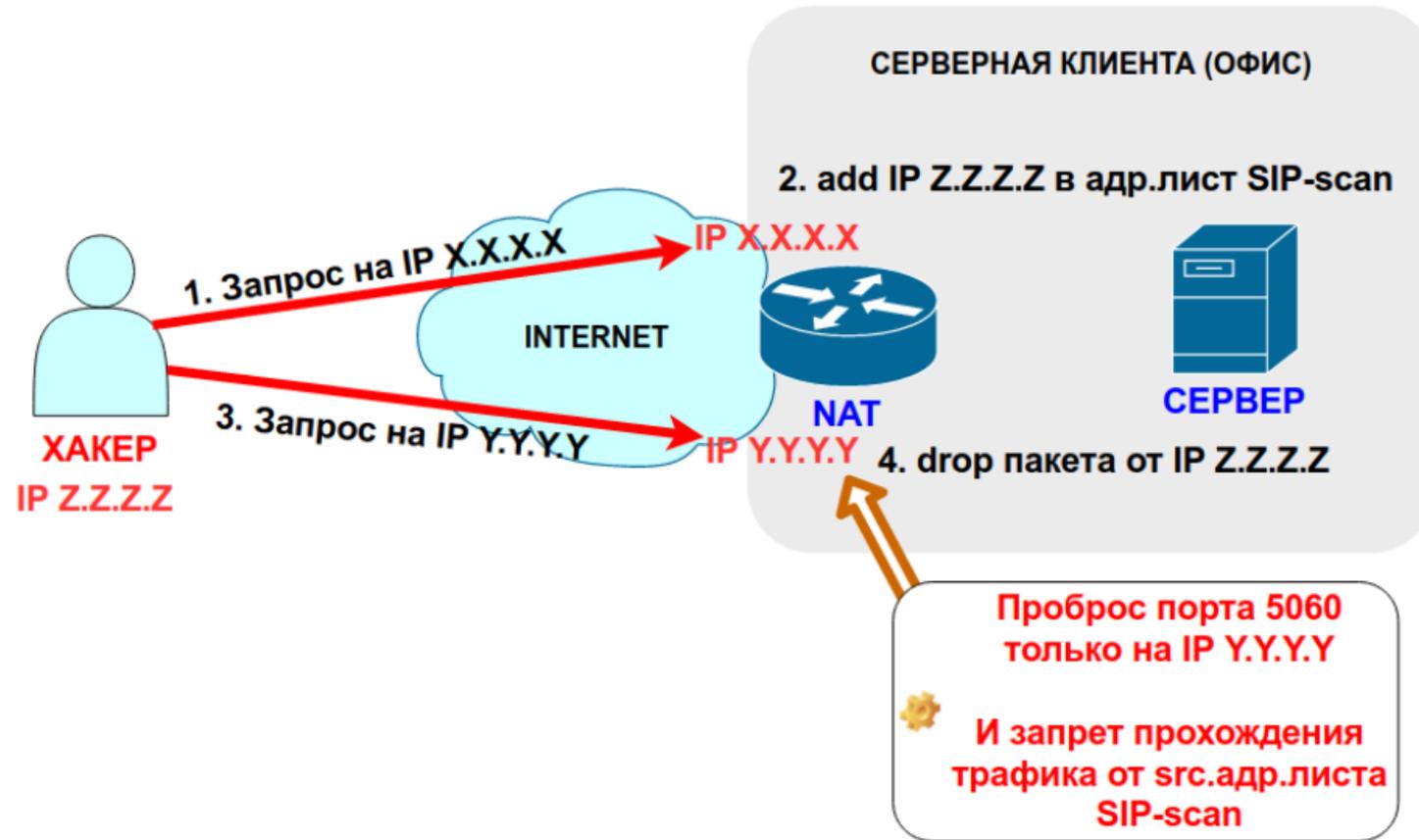


Схема хонипот (honeypot) - реализация

Добавляем

Firewall Rule <5060>

General | Advanced | Extra | Action | Statistics

Chain **input**

Src. Address

Dst. Address

Protocol 17 (udp)

Src. Port:

Dst. Port: 5060

Any. Port:

P2P:

Firewall Rule <5060>

General | Advanced | Extra | Action | Statistics

Action **add src to address list**

Log

Log Prefix

Address List **sip-scan**

Timeout

Ограничиваем

Firewall Rule <>

General | Advanced | Extra | Action | Statistics

Chain **forward**

Src. Address

Dst. Address

Protocol

Firewall Rule <>

General | Advanced | Extra | Action | Statistics

Src. Address Lis **sip-scan**

Dst. Address List

Layer7 Protocol

Content *

Firewall Rule <>

General | Advanced | Extra | Action | Statistics

Action **drop**

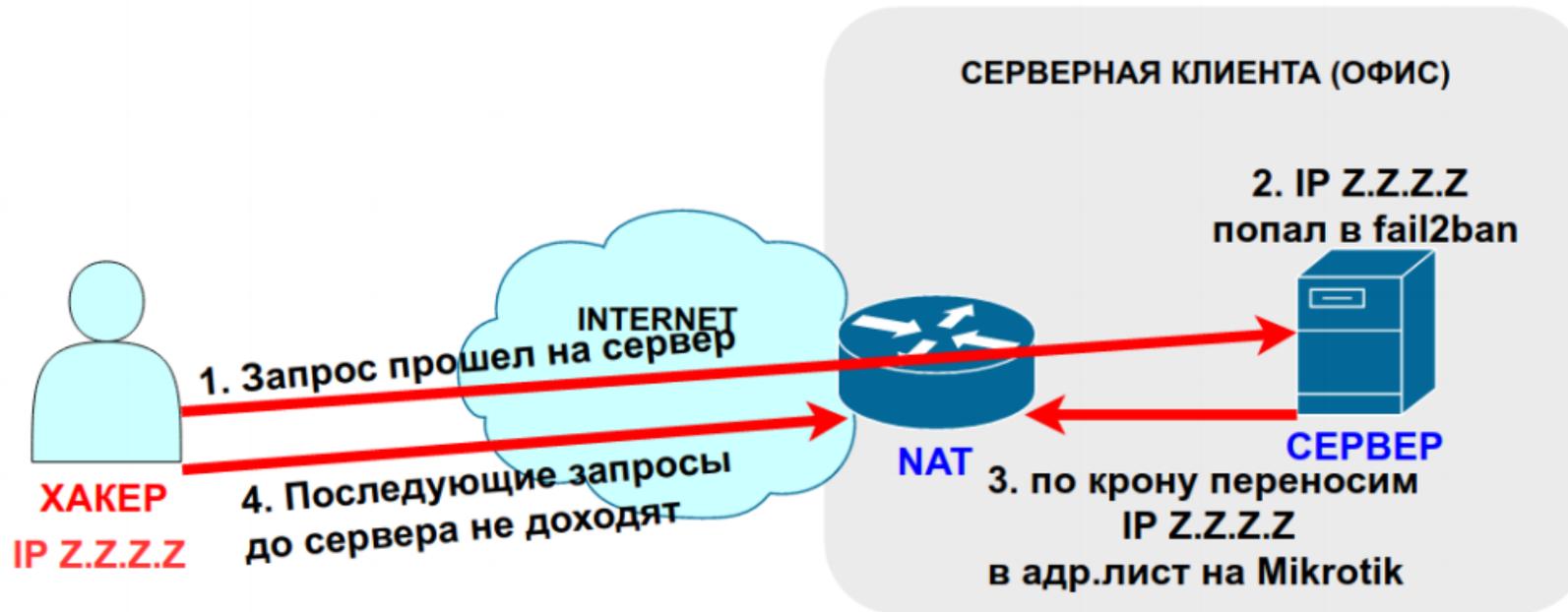
Log

Log Prefix



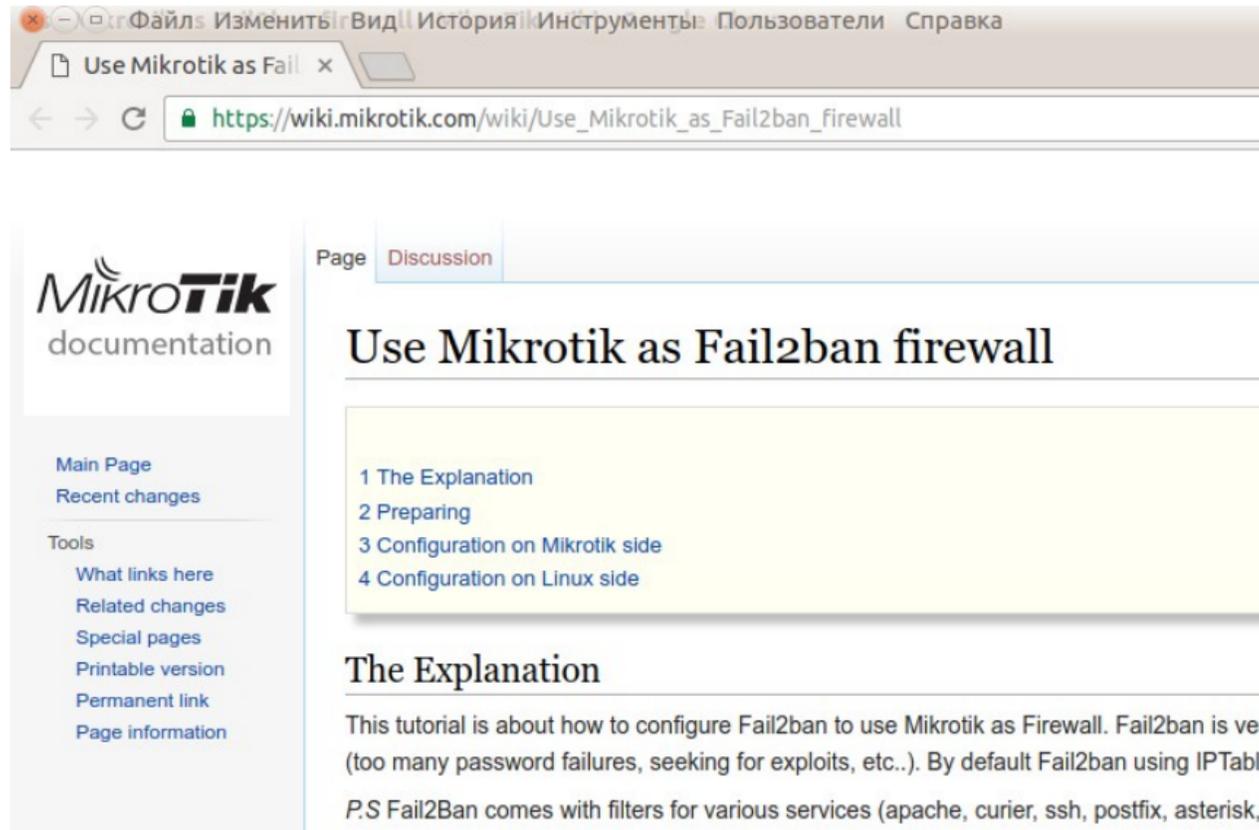
FAIL2BAN в связке с Mikrotik

Fail2ban с обратной связью



FAIL2BAN - реализация

Скрипт на оф. вики Mikrotik



The screenshot shows a web browser window with the URL https://wiki.mikrotik.com/wiki/Use_Mikrotik_as_Fail2ban_firewall. The page is titled "Use Mikrotik as Fail2ban firewall" and is part of the Mikrotik documentation. The page content includes a table of contents with the following items:

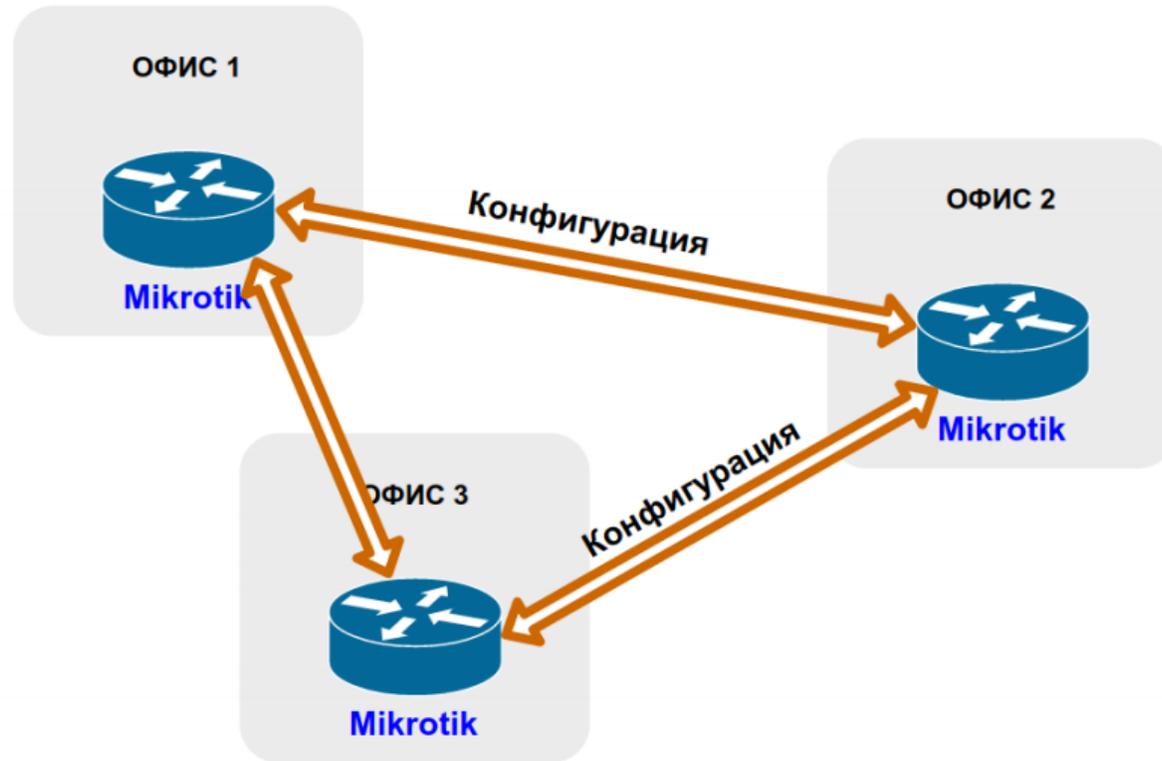
- 1 The Explanation
- 2 Preparing
- 3 Configuration on Mikrotik side
- 4 Configuration on Linux side

The "The Explanation" section begins with the text: "This tutorial is about how to configure Fail2ban to use Mikrotik as Firewall. Fail2ban is very (too many password failures, seeking for exploits, etc..). By default Fail2ban using IPTable P.S Fail2Ban comes with filters for various services (apache, curier, ssh, postfix, asterisk, €".

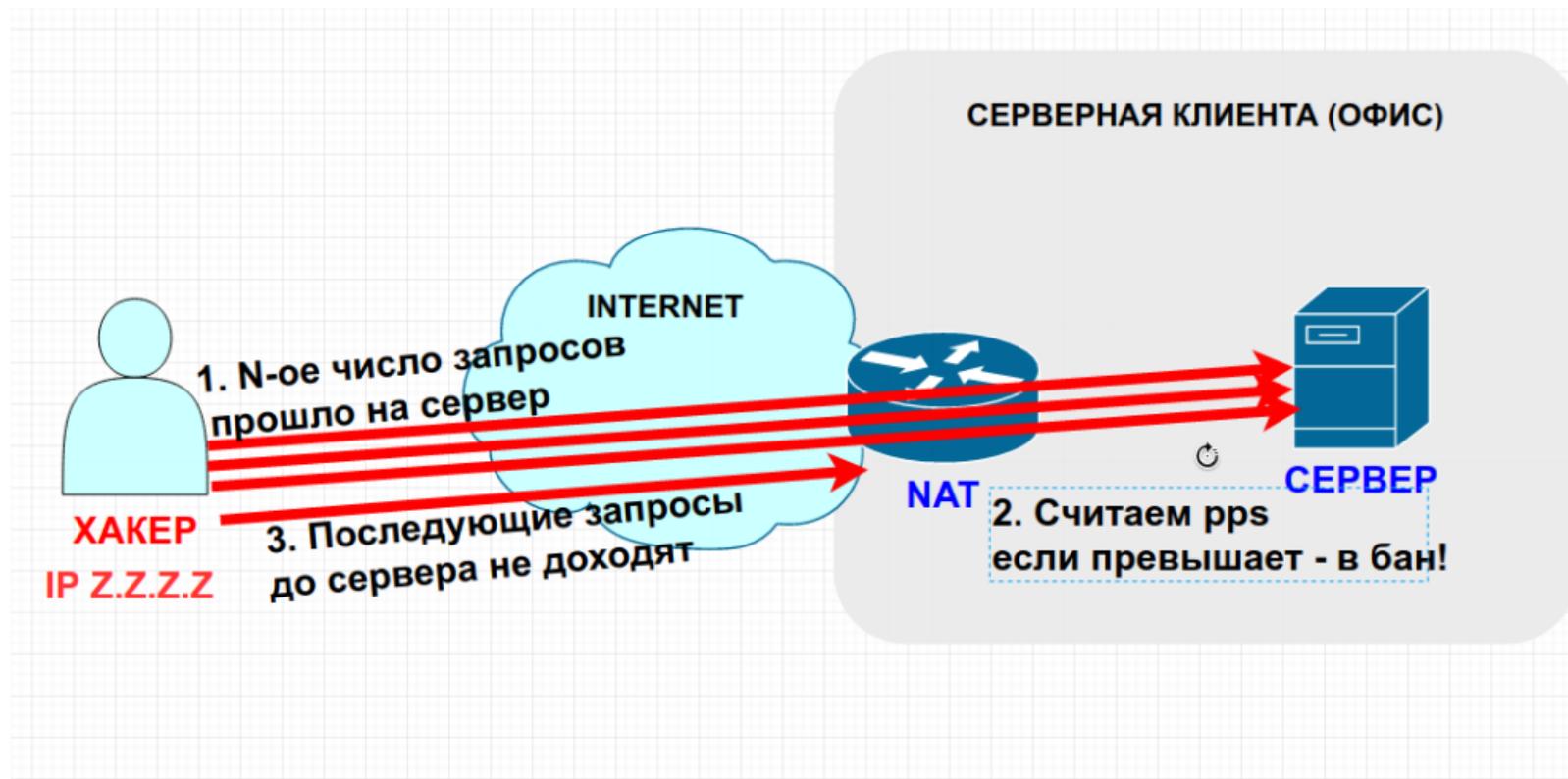


Адрес листы

Копируем адрес листы с одного на другой Микротик

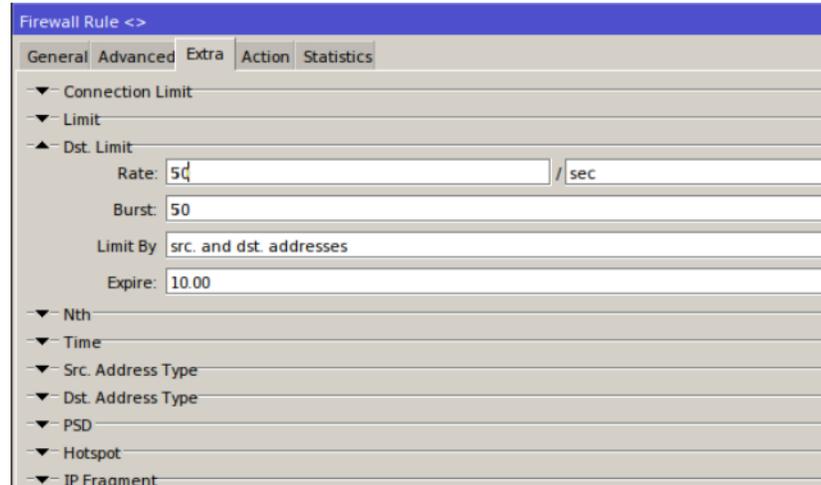


Ограничиваем pps



PPS - реализация

Пример проверки pps



Firewall Rule <>

General Advanced **Extra** Action Statistics

▼ Connection Limit

▼ Limit

▲ Dst. Limit

Rate: 50 / sec

Burst: 50

Limit By: src. and dst. addresses

Expire: 10.00

▼ Nth

▼ Time

▼ Src. Address Type

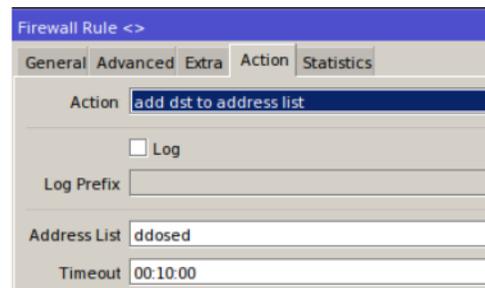
▼ Dst. Address Type

▼ PSD

▼ Hotspot

▼ IP Fragment

До 50 pps еще ок, свыше блокируем



Firewall Rule <>

General Advanced Extra **Action** Statistics

Action: add dst to address list

Log

Log Prefix:

Address List: ddosed

Timeout: 00:10:00



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

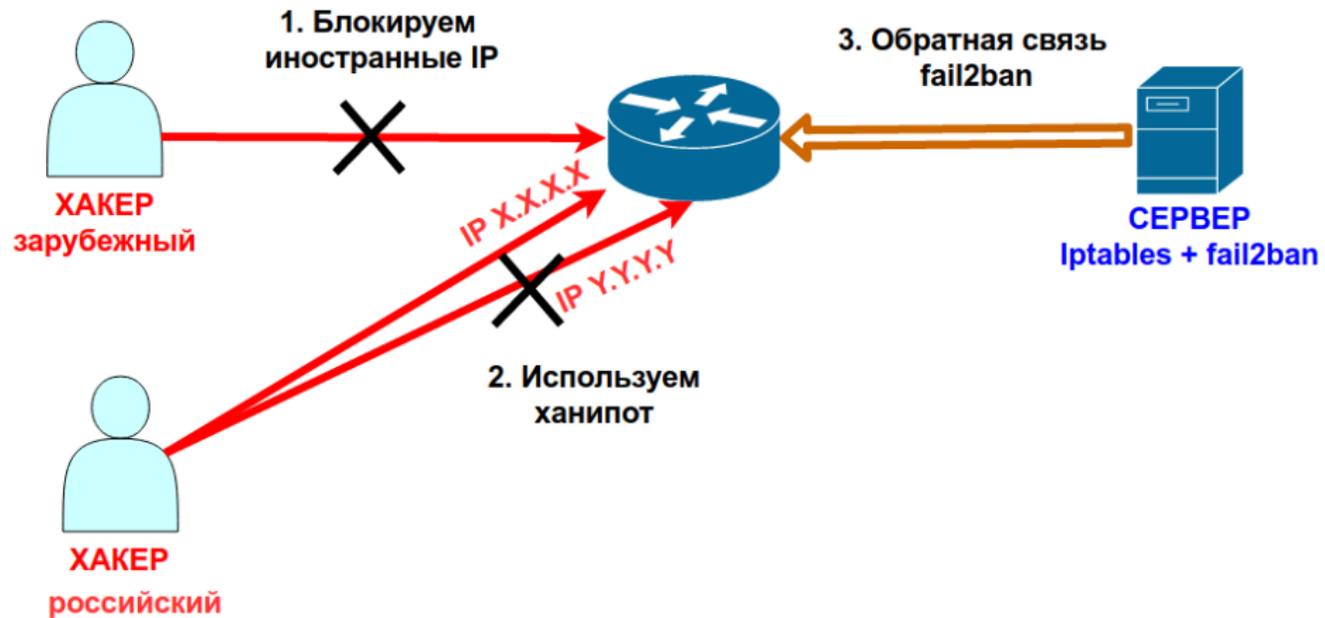


1. Анализ пакетов на содержание "403 Forbidden", считаем их
2. При определенном количестве добавляем IP Z.Z.Z.Z в адрес лист
3. Блокируем этот адрес лист



99 процентная связка защиты

Решаем 99% проблем



Та самая «галка» про анонимные звонки

Настройка телефона

Основное	СЕТЬ	УСЛ	ТЕЛЕФОН	управление	БЕЗОПАСНОСТЬ	Выход
Настройки дополнительных служб						
Не беспокоить:	<input type="checkbox"/>	Push XML Server:				
Включить переадресацию вызова:	<input checked="" type="checkbox"/>	Код сообщения при DND:	480(Временно недоступе			
Semi-Attended Transfer:	<input checked="" type="checkbox"/>	Код сообщения при занято:	486(Busy Here)			
Включить "Ожидание вызова":	<input checked="" type="checkbox"/>	Код сообщения при отклонении вызова:	603			
Включить "3-х конференцию":	<input checked="" type="checkbox"/>	Active URI Limit IP:				
Принимать любые вызовы:	<input type="checkbox"/>	Скрыть DTMF:	Отключен			
Enable Auto Handdown:	<input checked="" type="checkbox"/>	Завершение разговора (настройка длительности размыкания линии при завершении соединения):	3 секунд(ы)			
Ring From Headset:	<input type="checkbox"/>	Включить автодозвон:	<input type="checkbox"/>			
Включить режим тишины:	<input type="checkbox"/>	Интервал автодозвона:	10 (1~180)секунд(ы)			
Запретить исходящие:	<input type="checkbox"/>	Количество попыток автодозвона:	10 (1~100)			
Включить интерком:	<input checked="" type="checkbox"/>	Точка-точка IP - префикс:	.			
Включить интерком без микрофона:	<input type="checkbox"/>	Пароль для звонков:	<input type="checkbox"/>			
	<input type="checkbox"/>	Префикс для звонков по				



Уведомление технической поддержки

Пошли звонки на 810.....

Уведомление технической поддержки

- Электронная почта
- SMS
- Alert в системе мониторинга



www.avantelecom.ru

Мой личный мобильный

+7 914 777 36 80

Владислав Вирясов

Директор по развитию

