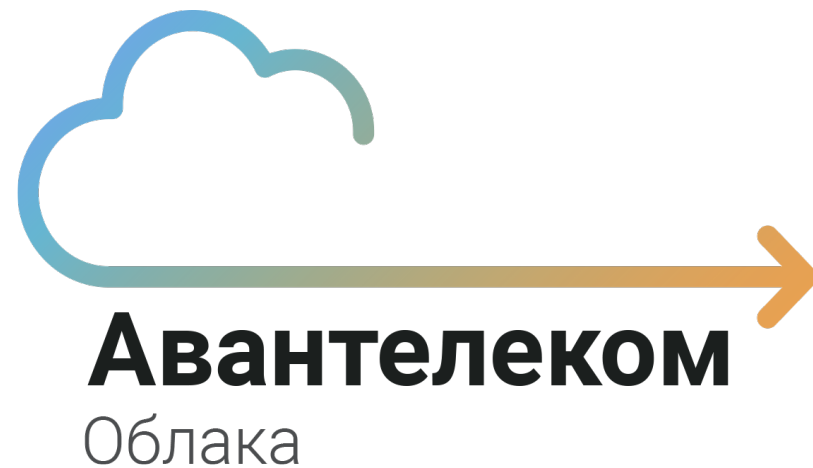




Мikrotik в качестве фаервола для SIP сервера

**Увеличивайте свою
технологическую оснащенность**

Проекты



T.8 800 333 44 56

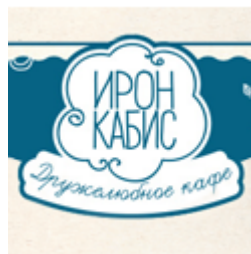


sales@avantelecom.ru

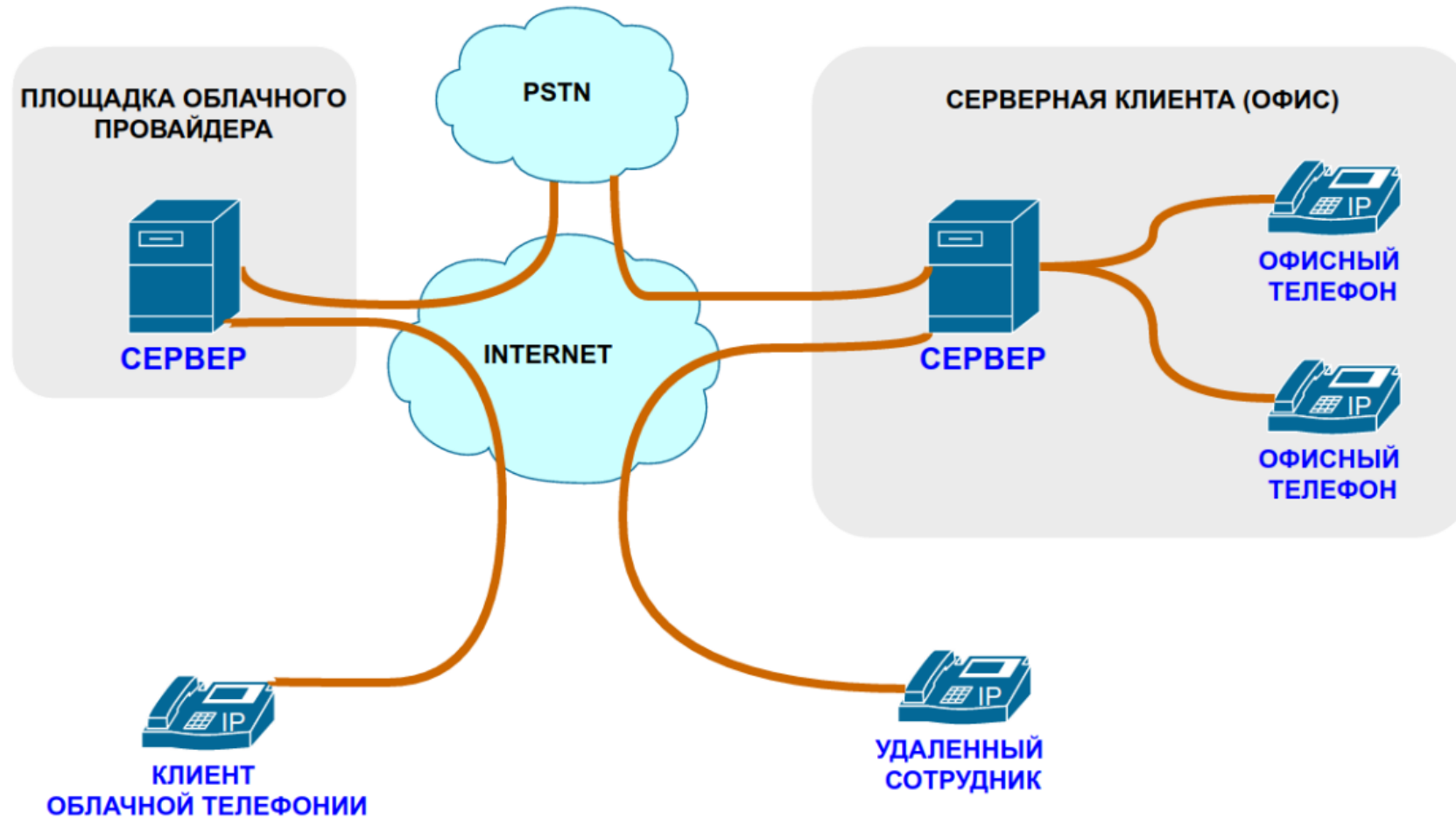


www.avantelecom.ru

О компании



Обычно это так



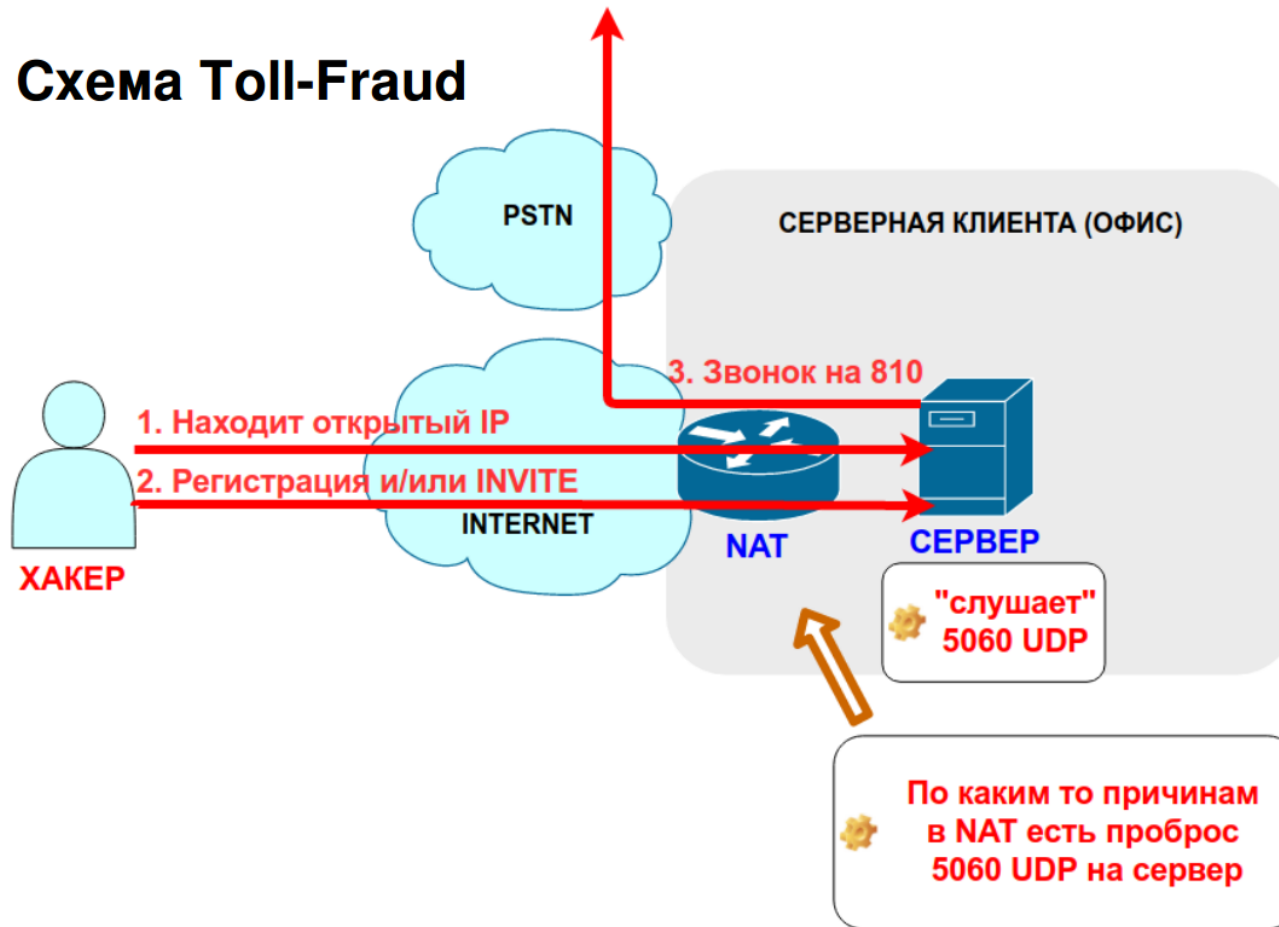
Цели злоумышленников и типы атак

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



Toll-Fraud

Схема Toll-Fraud

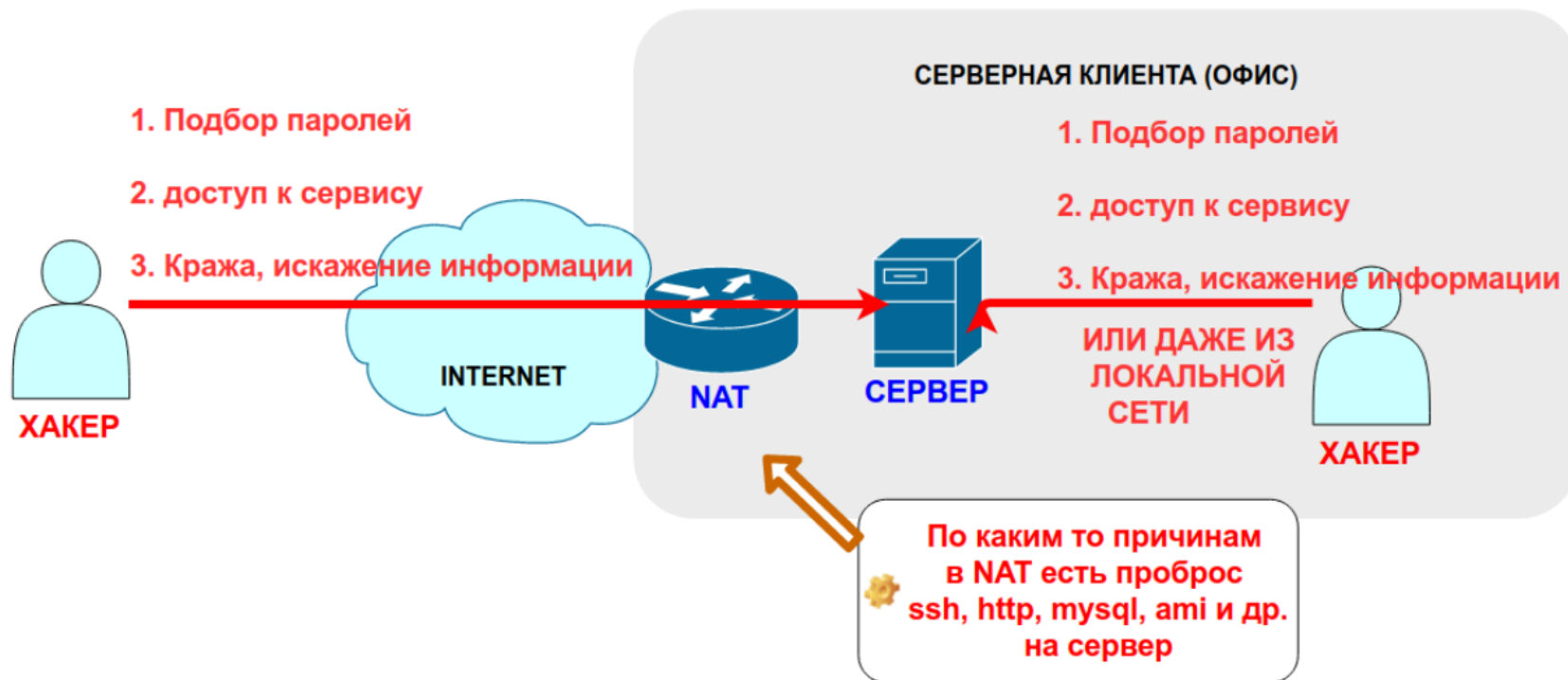


Также сюда можно отнести взлом пароля AMI, пароля mysql, программных компонент, которые установлены на сервере и доступны из сети интернет (FreePBX, phpmyadmin)



Кража

Кража и(или) порча информации



DDoS

- Обычный DDoS
- DDoS на SIP

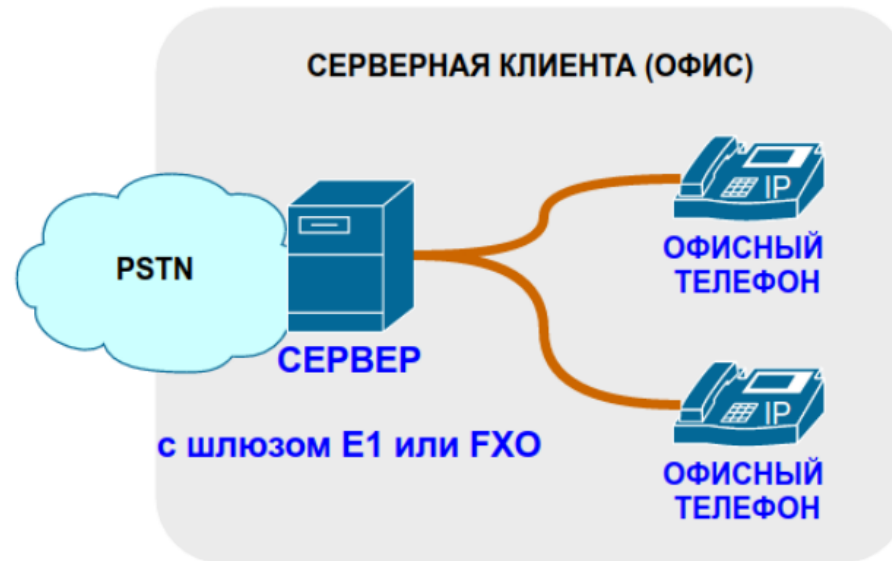


Стандартные меры борьбы

- 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

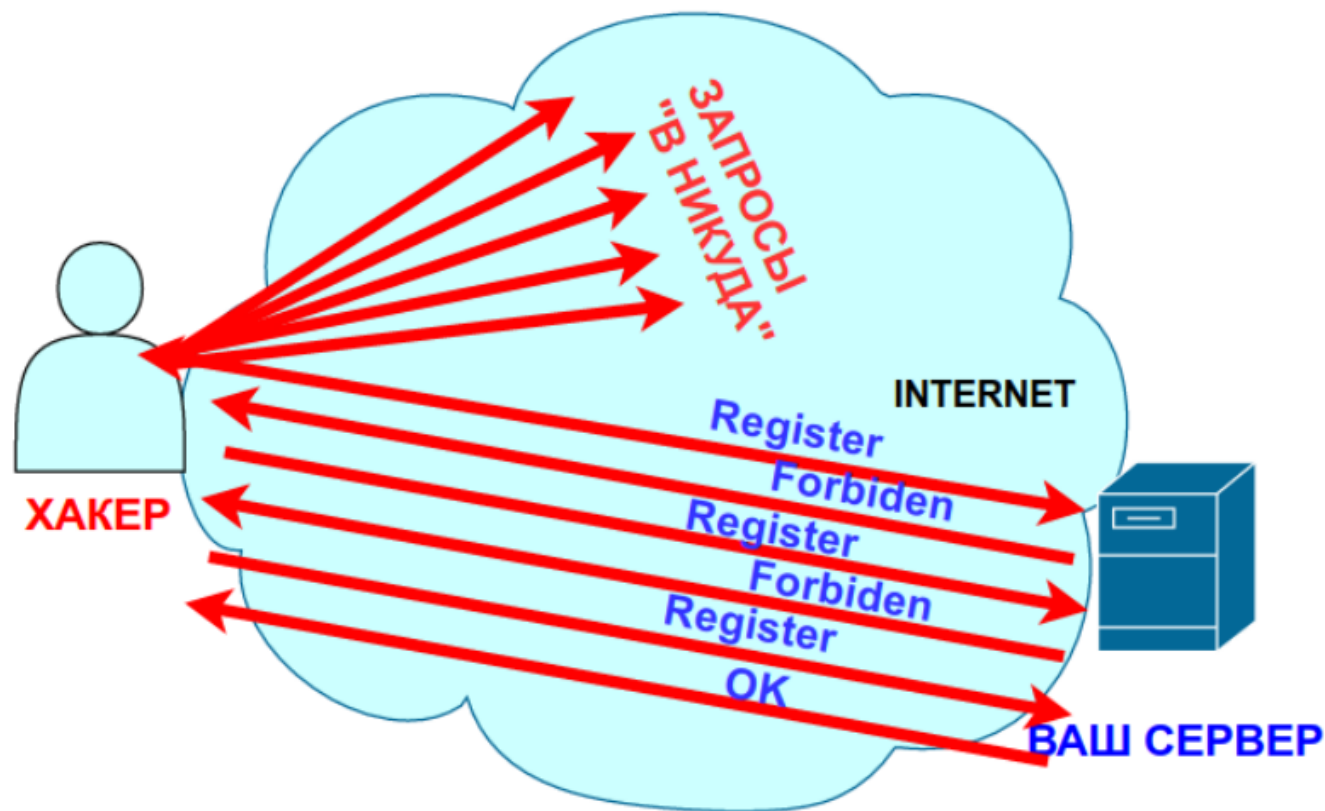


Основные способы защиты на Mikrotik

- **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



T.8 800 333 44 56



sales@avantelecom.ru



www.avantelecom.ru

Список и правило

The screenshot shows the Mikrotik WinBox interface. On the left, the 'Firewall' menu is expanded. The main window displays a list of firewall rules. The right pane shows the configuration for a selected rule, with the 'Chain' set to 'forward' and the 'Action' set to 'drop'.

Name	Address	Timeout
gringo	1.0.0.0/8	
gringo	7.0.0.0/8	
gringo	13.0.0.0/8	
gringo	14.0.0.0/8	
gringo	23.0.0.0/8	
gringo	24.0.0.0/8	
gringo	27.0.0.0/8	
gringo	32.0.0.0/8	
gringo	35.0.0.0/8	
gringo	36.0.0.0/8	
gringo	39.0.0.0/8	
gringo	40.0.0.0/8	
gringo	41.0.0.0/8	
gringo	42.0.0.0/8	
gringo	43.0.0.0/8	
gringo	45.0.0.0/8	
gringo	47.0.0.0/8	
gringo	49.0.0.0/8	
gringo	50.0.0.0/8	
gringo	52.0.0.0/8	
gringo	54.0.0.0/8	
gringo	58.0.0.0/8	
gringo	59.0.0.0/8	
gringo	60.0.0.0/8	
gringo	61.0.0.0/8	
gringo	63.0.0.0/8	
gringo	64.0.0.0/8	

142 items out of 1363 (1 selected)

Важно помнить о количестве правил и производительности устройства!



T.8 800 333 44 56



sales@avantelecom.ru



www.avantelecom.ru

Схема хонипот (honeypot)

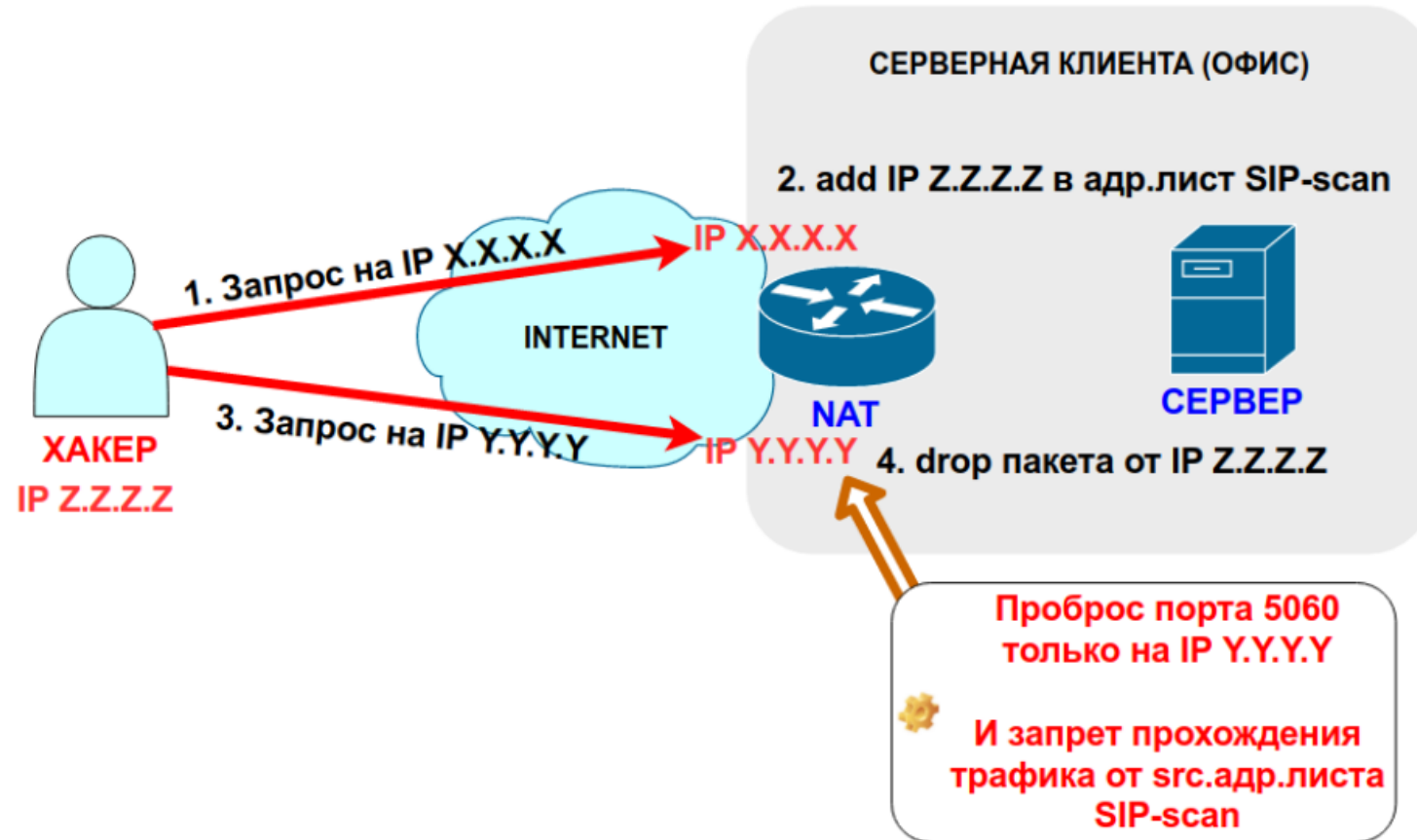


Схема хонипот (honeypot) - реализация

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 List ☒ **sip-scan**

Dst. Address List

Layer7 Protocol

Content *

Firewall Rule <>

General Advanced Extra Action Statistics

Action **drop**

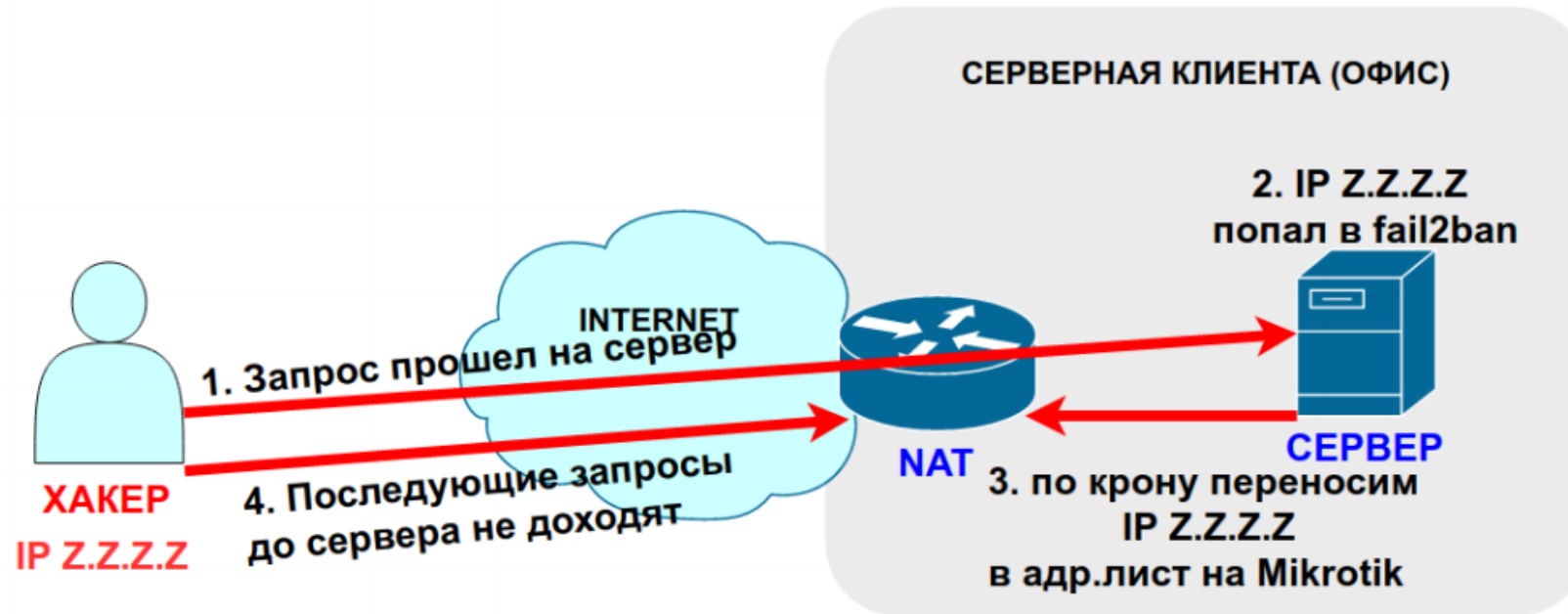
☐ Log

Log Prefix



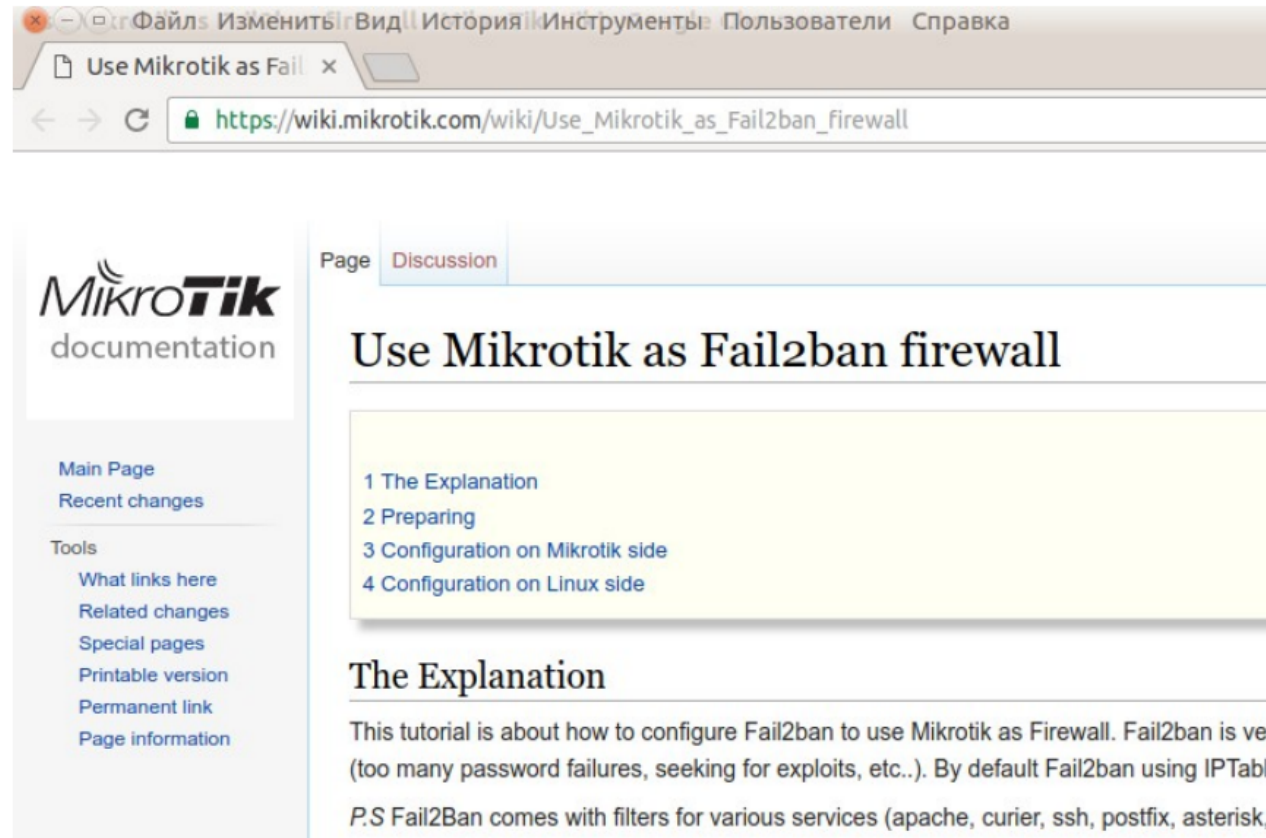
FAIL2BAN в связке с Mikrotik

Fail2ban с обратной связью



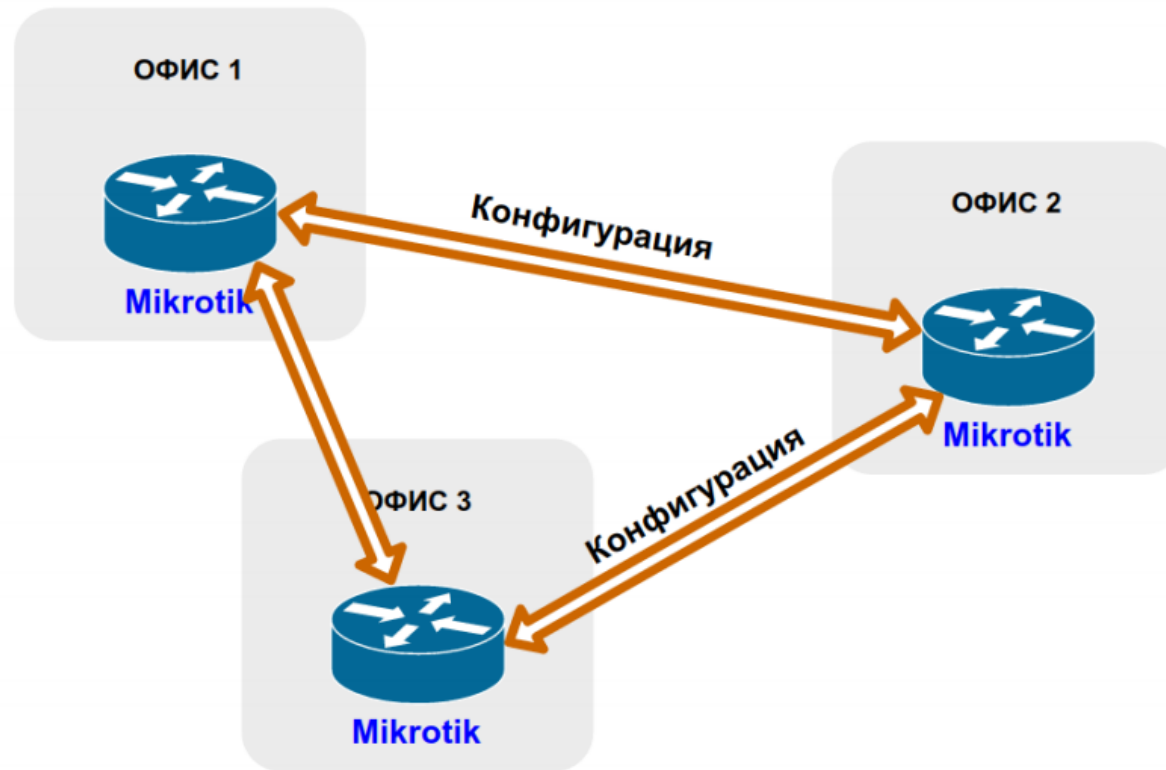
FAIL2BAN - реализация

Скрипт на оф. вики Mikrotik

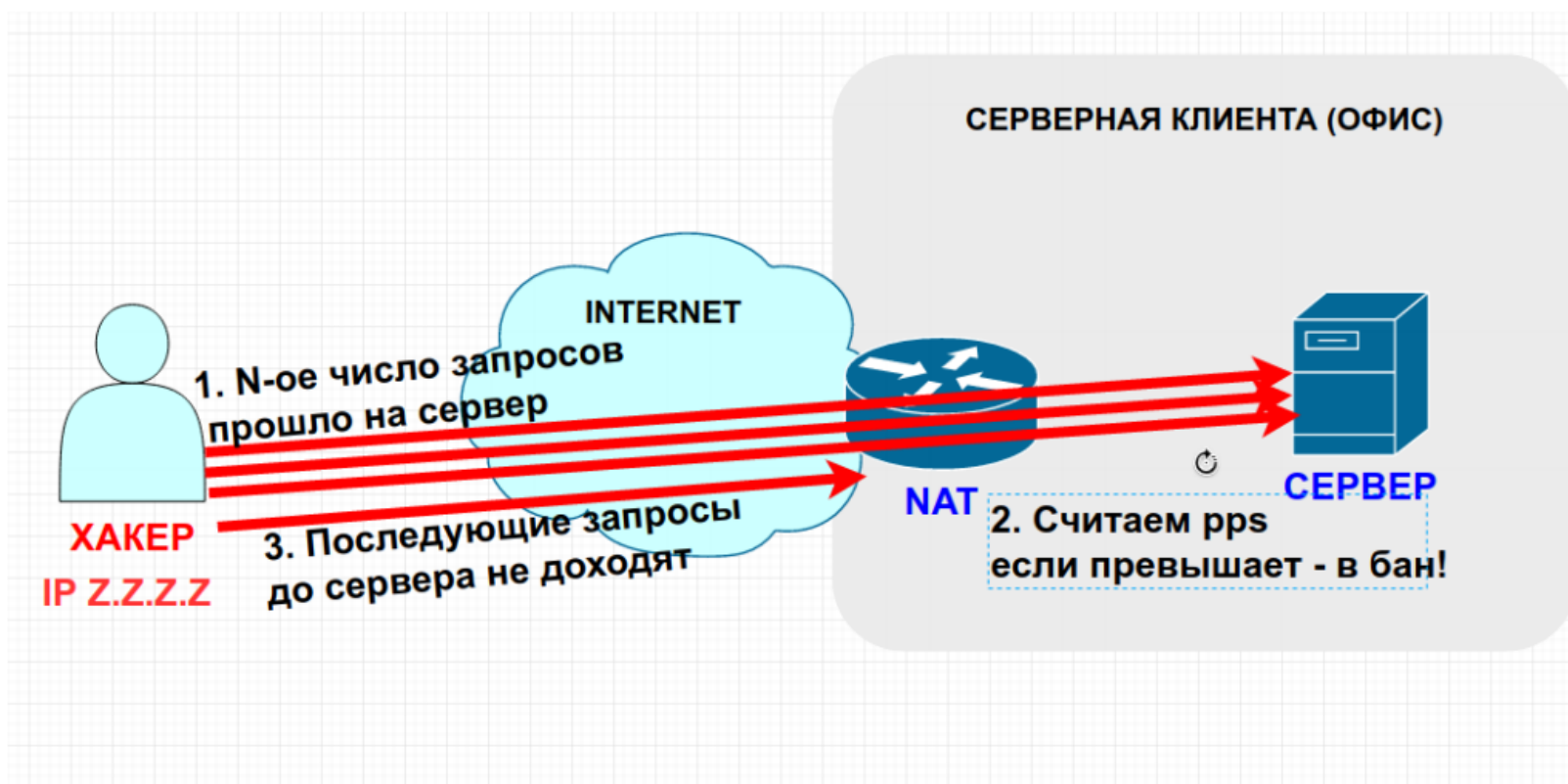


Адрес листы

**Копируем адрес листы с одного на другой
Микротик**

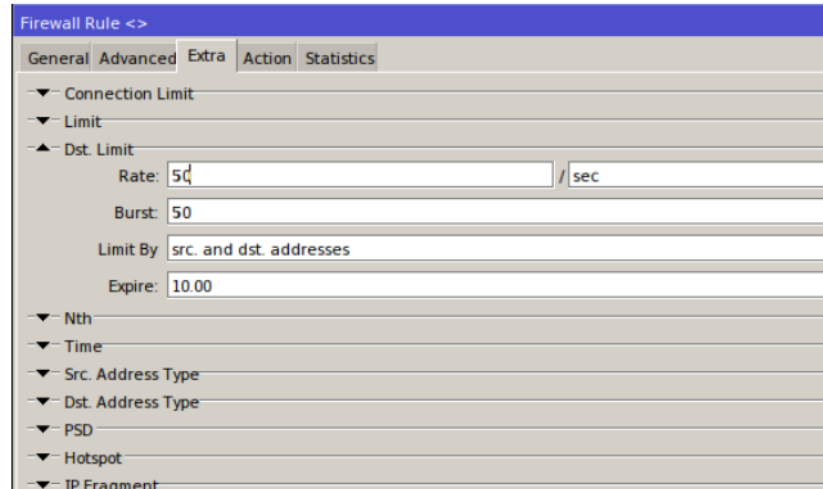


Ограничиваем pps



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

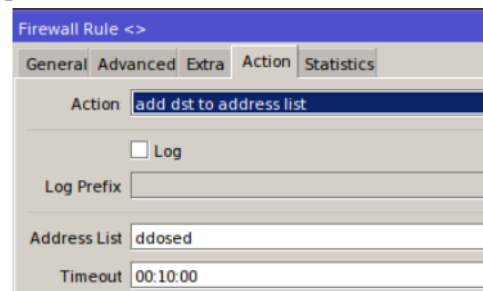
Dst. Address Type

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

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

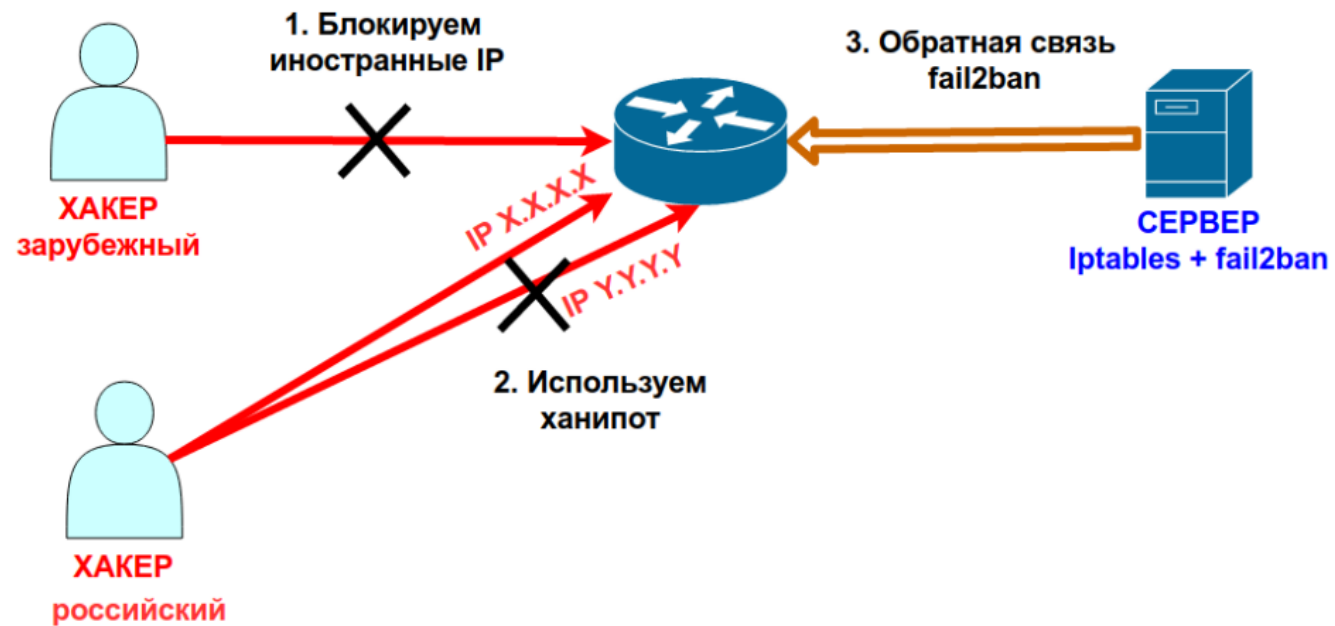


1. Анализ пакетов на содержание "403 Forbidden", считаем их
2. При определенном количестве добавляем IP Z.Z.Z.Z в адрес лист
3. Блокируем этот адрес лист



99 процентная связка защиты

Решаем 99% проблем



Та самая «галка» про анонимные звонки

Настройка телефона

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

