# Двухфакторная аутентификация для VPN MikroTik через Asterisk

# Обо мне:

| | |
|---|---|
| **ФИО** | **Козлов Роман** |
| Контакты | t.me/soriel |
| Возраст | 37 |
| Сертификаты Mikrotik | MTCNA*, MTCRE*, MTCWE*, MTCTCE*, MTCUME*, MTCINE*, MTCIPv6E*, MTCSE*, MTCSWE*, Trainer* |
| Компания | IntegraSky |
| Должность | Технический директор |
| Технологии и профессиональные интересы | Сети, wifi, виртуализация, сервера, linux, безопасность, windows и etc |
| Дополнительно | |

# О чем доклад

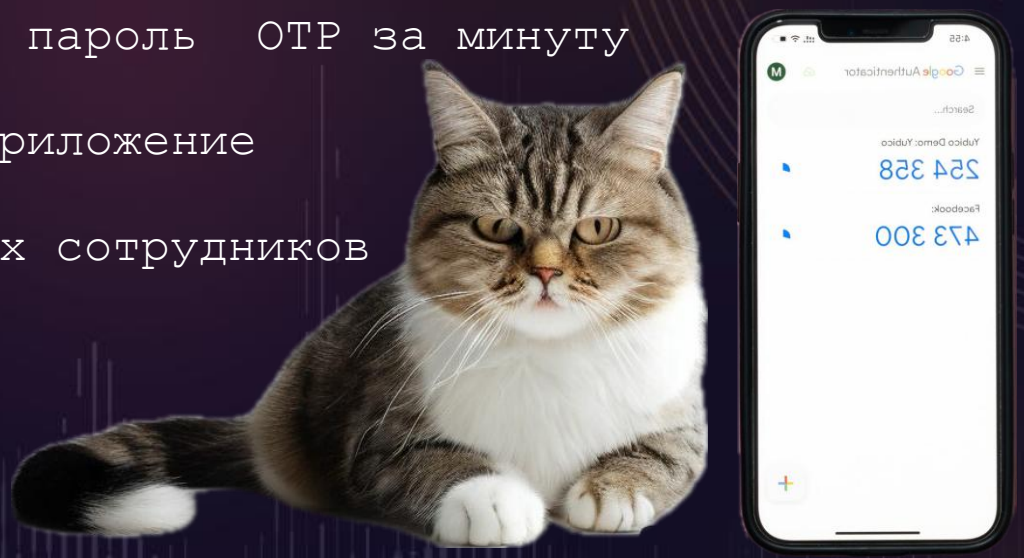
- Зачем нам понадобилась 2FA
- Почему не OTP
- Неудачная попытка написать сервис для 2FA на asterisk
  - Схема реализации
  - Почему не взлетело
- Простое и практически бесплатное решение для 2FA
  - Схема реализации
  - Плюсы реализации
- Выводы

# Зачем нам понадобилась 2FA

- Большой центр обработки звонков
- В смену работает от 150 до 600 человек в очереди
- Все работают удаленно и со личных рабочих станций
- Нет возможности на 100% контролировать “чистоту” рабочих станций
- Работаем с крупными заказчиками и любой инцидент связанный с безопасностью будет фатальным для нашей компании
- Используем для подключения различные клиент-серверные VPN с ограниченным доступом к ресурсам заказчика – SSTP, OpenVPN, l2tp + ipsec
- Используем RADIUS для хранения учетных данных

# Почему не OTP

- В MikroTik UserManager  есть встроенных механизм для реализации OTP(one time password) для VPN подключений
- Нужно устанавливать OTP клиент  на мобильные телефоны операторов
- Дополнительная нагрузка при обучении операторов
- Некоторые операторы не успевают ввести пароль  OTP за минуту
- Некоторые операторы забывают про OTP приложение
- В общем это сложно для неподготовленных сотрудников

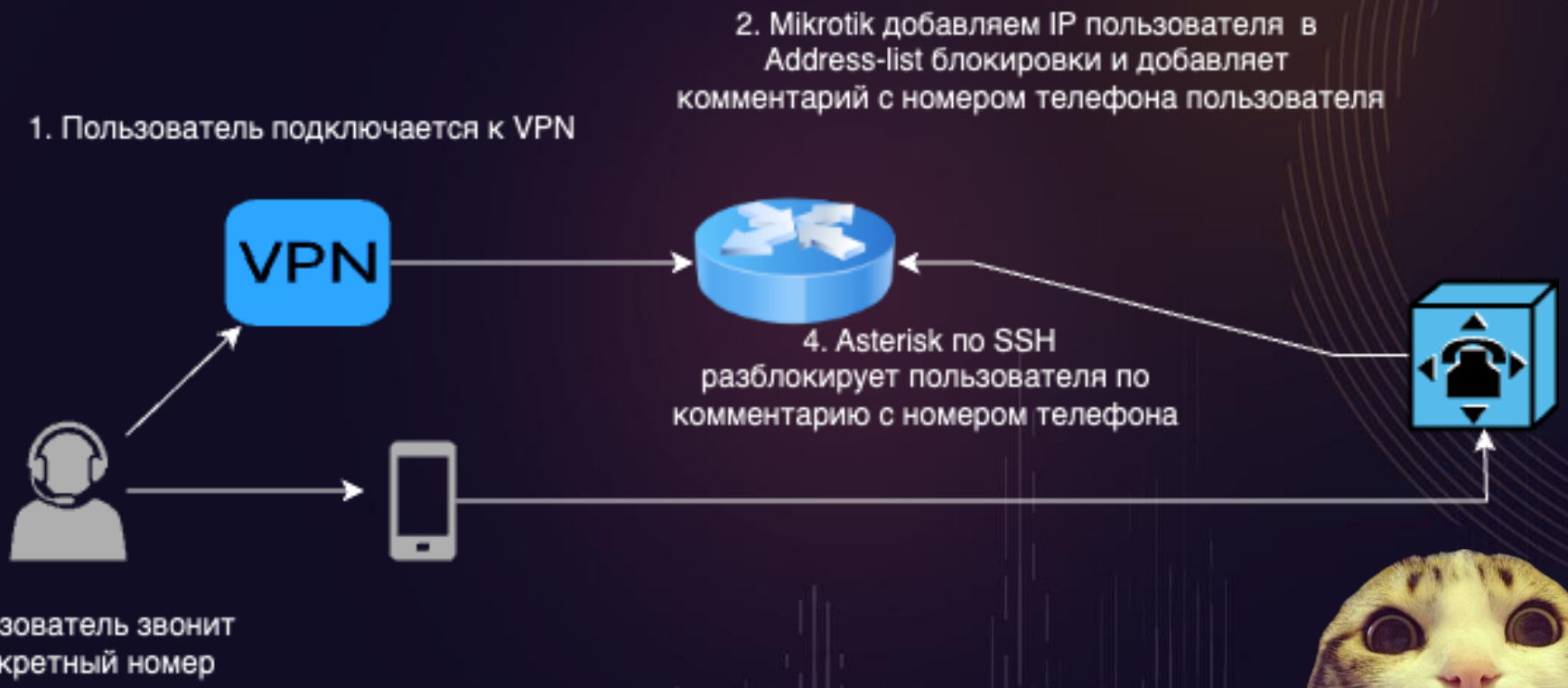


# Неудачная попытка написать сервис для 2FA на asterisk


# Почему не взлетело

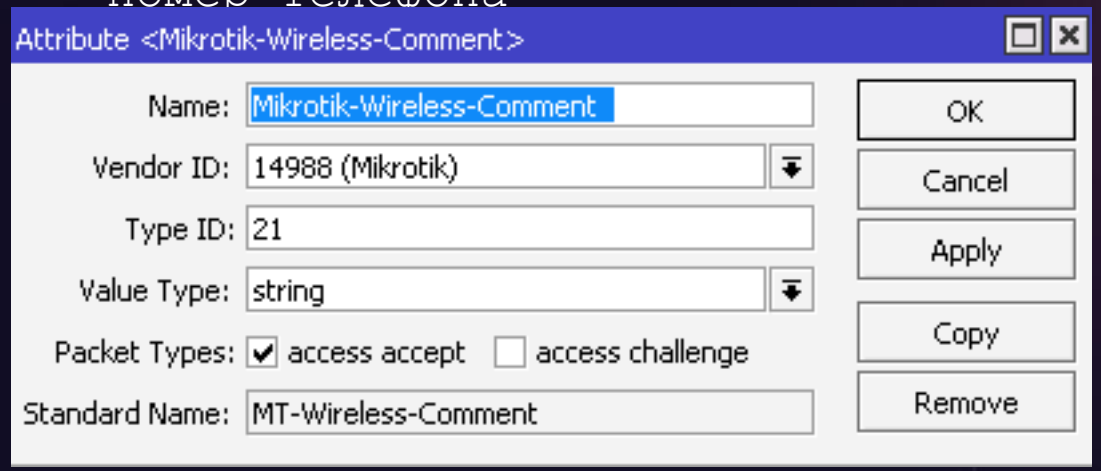
- Не типовая разработка для нашей компании
- Поддержка дополнительной базы данных и веб сервиса
- Платные звонки для компании
- Проблемы с повторной авторизацией
- Требуется дополнительная логика для наборов клавиш от пользователей
- Требуется доработка логики сервиса

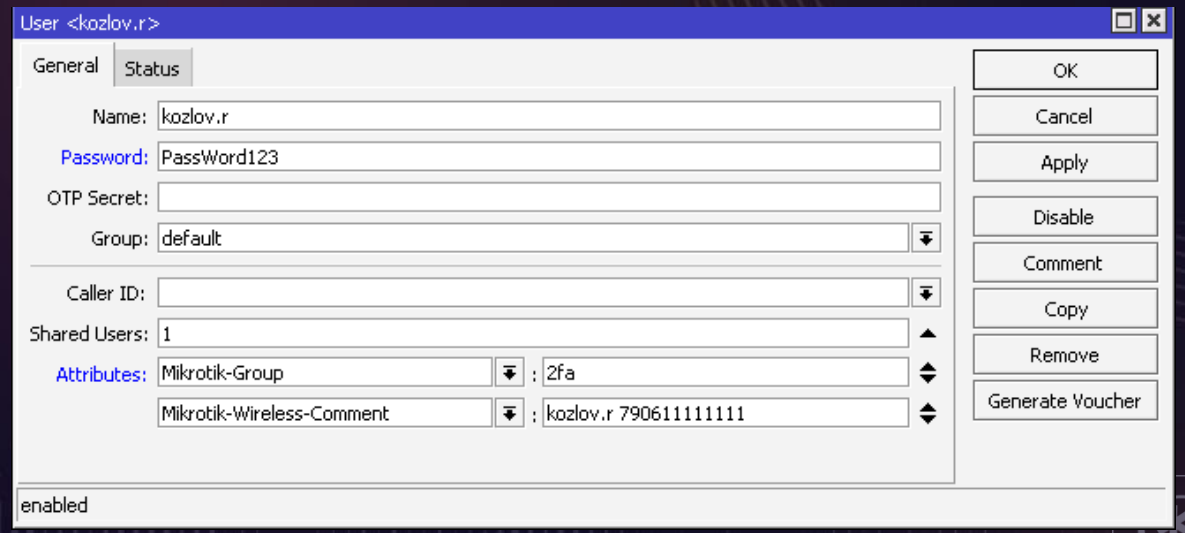
# Простое и практически бесплатное решение для 2FA




# Технические нюансы реализации

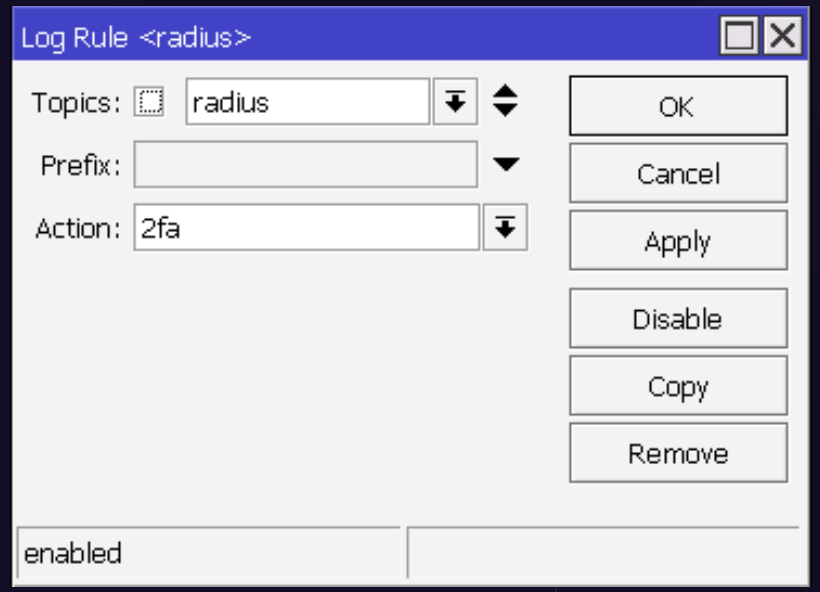
- Для добавления номера телефона в ip firewall address-list требуется получить его из дополнительных атрибутов
- Для этого используется Radius атрибут Mikrotik-Wireless-Comment 14988 (Mikrotik) / 21 / String
- Добавляем этот атрибут в Radius используя “Имя_пользователя Номер Телефона”

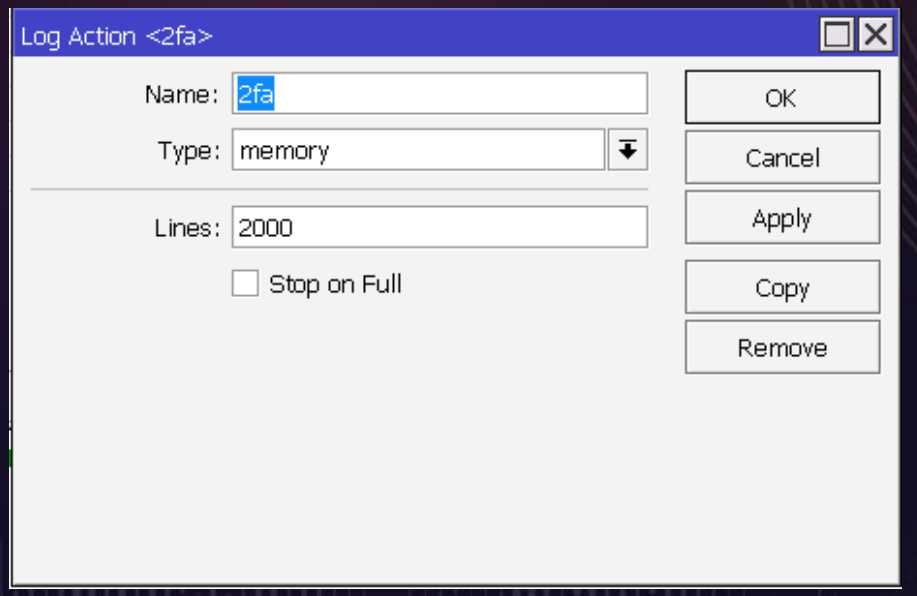


# Технические нюансы реализации

- Создаем лог для поиска атрибутов номера телефона
- /system logging action add memory-lines=2000 name=2fa target=memory
- /system logging add action=2fa topics=radius



# Технические нюансы реализации

- Действие по поиску номеров телефонов будет происходить через ppp profile
- При отключении ip удаляется из address-list блокировки
- Нужно настроить ssh авторизацию по ключам (приватный ключ нужно поместить на asterisk, публичный на mikrotik)
- Требуется номер телефона для звонков пользователей
- Можно сделать страницу для уведомления о блокировке для ваших пользователей (На mikrotik работает через web-proxy и только для HTTP, с альтернативным веб-сервером может быть HTTPS, но с ошибкой сертификата)

# Технические нюансы /ppp profilre on up

```
:local datetime [/system clock get date]
:local time [/system clock get time]
:local remoteAddr
:local callerid
:set remoteAddr $"remote-address"
:set callerid $"caller-id"
:local 2facomment;

:foreach line in=[/log find buffer=2fa (message~"MT-Wireless-Comment =")]
do={
  :do {:local content [/log get $line message];
  :local pos1add [:find $content " = " 0];
  :if ([:len $pos1add] != 0) do={
    :local pos2add [:len $content];
    if ([:len $pos2add] != 0) do={
      :set 2facomment [:pick $content ($pos1add+4) ($pos2add-1)];
      };
   };
 };
if ($2facomment ~ $user) do={
   delay 2;
   /ip firewall address-list add address=$remoteAddr list=vpnblocked
timeout=200d comment=$"2facomment"
   /log info "VPN-con $datetime $time Connected user: $"2facomment"
$"caller-id" $"remote-address""
   };
```

Локальные переменные

Цикл поиска номера телефона в log сообщениях от radius сервера

Добавление ip адреса в /ip firewall address-list с комментарием номер телефона
Лог сообщение info

# Технические нюансы /ppp profile on down

```
/ip firewall address-list remove numbers=[find where comment~$user
list=vpnblocked]

:local callerId

:local calledId

:set callerId $"caller-id"

:set calledId $"called-id"

:local datetime [/system clock get date]

:local time [/system clock get time]

/log info "VPN-con $datetime $time Disconnected user: $user
$callerId"
```

Удаление пользователя из address-list

Локальные переменные

Лог сообщение info

# Asterisk

Dialplan

```
[from-trunk]
exten => 749511111111,1,Goto(two-factor,s,1)


[two-factor]
exten => s,1,NoOp(START 2 factor auth from 7${CALLERID(num):-10})
same  => n,Set(CLIENT=7${CALLERID(num):-10})
same  => n,GotoIf($[${REGEX("^7[0-9]{10,10}$" ${CLIENT})}]?remove:end)
same  => n(remove),System(/usr/local/bin/2factor-mikrotik.sh ${CLIENT})
same  => n(end),Busy()
```

Shell

/usr/local/bin/2factor-mikrotik.sh

```
#!/bin/bash
/usr/bin/ssh -oStrictHostKeyChecking=no pbx482@ip-mikrotik "/ip firewall address-list remove
numbers=[find where comment~\"$1\" list=vpnblocked]
```

# Технические нюансы firewall / web-proxy

- /ip firewall filter add action=reject chain=forward comment="Deny 2fa for vpnblacked" reject-with=icmp-admin-prohibited src-address-list=vpnblocked
- /ip firewall filter add action=reject chain=input comment="Deny 2fa for vpnblacked" reject-with=icmp-admin-prohibited src-address-list=vpnblocked
- /ip firewall filter add action=accept chain=input comment="Allow 2fa for vpnblacked" dst-port=8080 protocol=tcp src-address-list=vpnblocked
- /ip firewall nat add action=redirect chain=dstnat comment="Redirect to web-proxy for vpnblocked" dst-port=80 protocol=tcp src-address-list=vpnblocked to-ports=8080

- /ip proxy reset-html
- /ip proxy set cache-administrator=admin@example.com enabled=yes
- /ip proxy access add action=deny

# Итоги

- **Очень простая реализация:** не требует навыков программирования и не нужно поддерживать дополнительных сервис
- **Низкие ежемесячные расходы:** цена равна стоимости номера телефона в вашем регионе
- **Простота для пользователей:** не нужно устанавливать приложения и учиться ими пользоваться
- **Номера телефонов хранятся в radius** достаточно обновлять одну базу хранения учетных записей
- **Уведомление с номером телефона для звонка** пользователи не потеряют номер телефона для авторизации.
- **Никаких дополнительных установок на телефонном сервере:** скрипт однострочник и dialplan

# Спасибо за внимание!

Буду рад ответить на все ваши вопросы сейчас или свяжитесь со мной в будущем:

**Роман Козлов**
trainer@mikrotik-training.ru
mikrotik-training.ru
+7 495 256-9-256
tg://soriel

http://mkrtk.ru/asterkonf2fa