MikroTik как инструмент защиты информации.

IPSec, плюс

2-факторная аутенитификация

на слабом железе.

Обо Мне

- ✓ Руководитель ИТ-службы
- ✓ MikroTik certified engineer, consultant
- ✓ MikroTik Trainer
- ✓ Сертификаты: ccna, mtcna, mtcre, mtcwe, Eltex - коммутация, ФЗ-152
- ✓ Работаю с микротик с 2008

Проблемы Безопасности

- Длинные пароли не спасают. Уязвимости MIkroTik, Linux, Windows не зависящие от парольной защиты
- Вектор атак сместился на протоколы и сервисы

«CIA Vault 7 – информация о взломах»

https://wikileaks.org/ciav7p1/

Преимущества 6.40.4

- Добавлено "none-dynamic" and "none-static" в качестве address-list timeout !
- Добавлен «interface-list» в профили (с 6.39)
- Добавлен DHCP-Client script (с 6.39)
- IPv6 Firewall в default

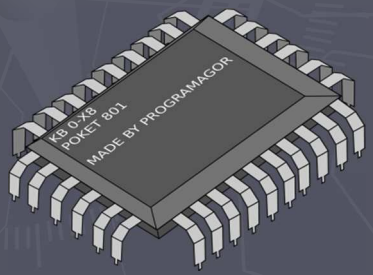
IPSec не для всех

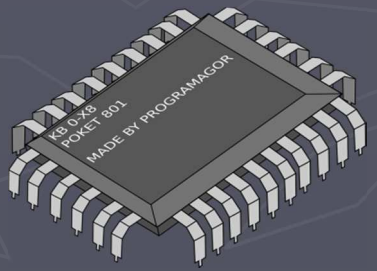
Аппаратное ускорение для отдельных моделей и алгоритмов:

1. **RB1100AHx4**
2. **hEX v3 *(RB750Gr3)***
3. **Все CCR**
4. **RB1100AHx2**
5. **RB850Gx2**

1. **AES-CBC 128, 192, 256**
2. **sha1, sha256.**

Все остальные нагружают CPU!

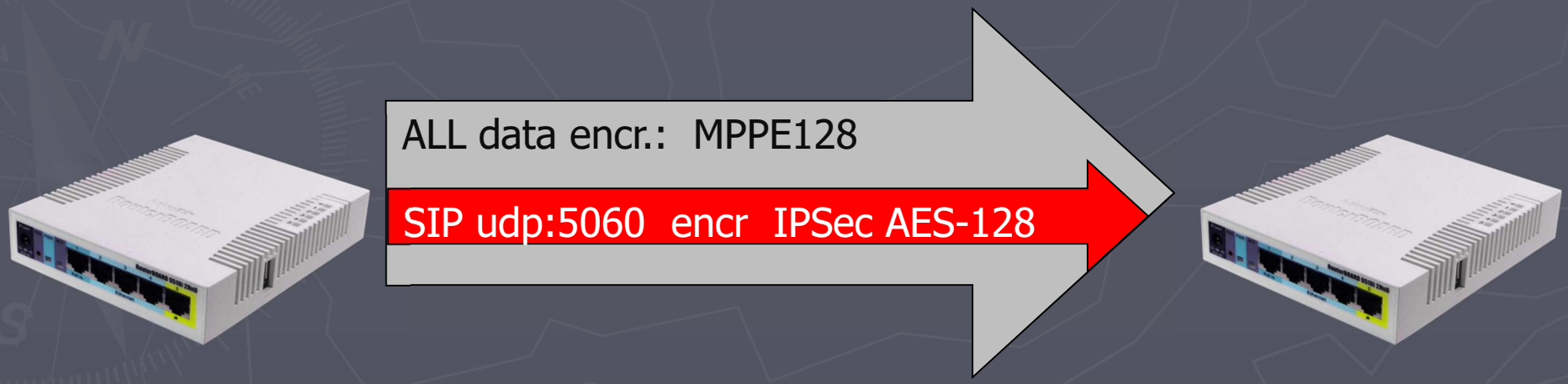




Что делать с RB951/2011?

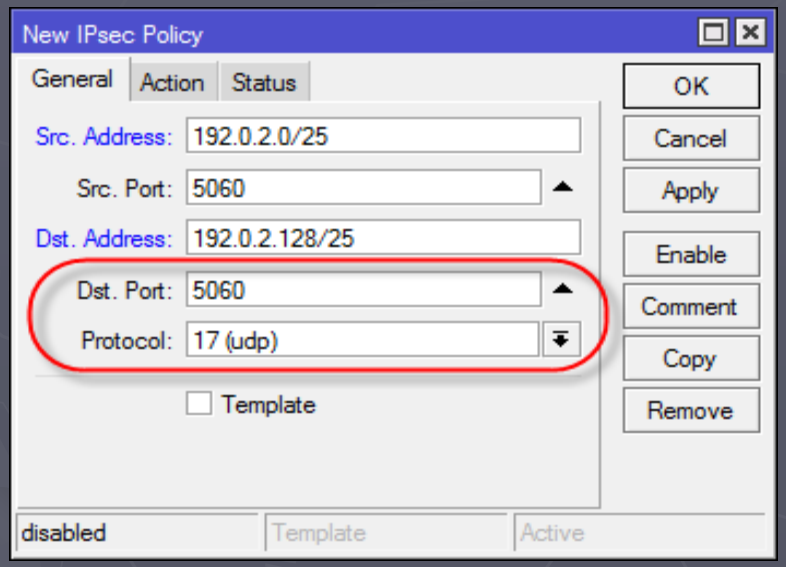
реальный кейс «за три копейки» по требованию СБ

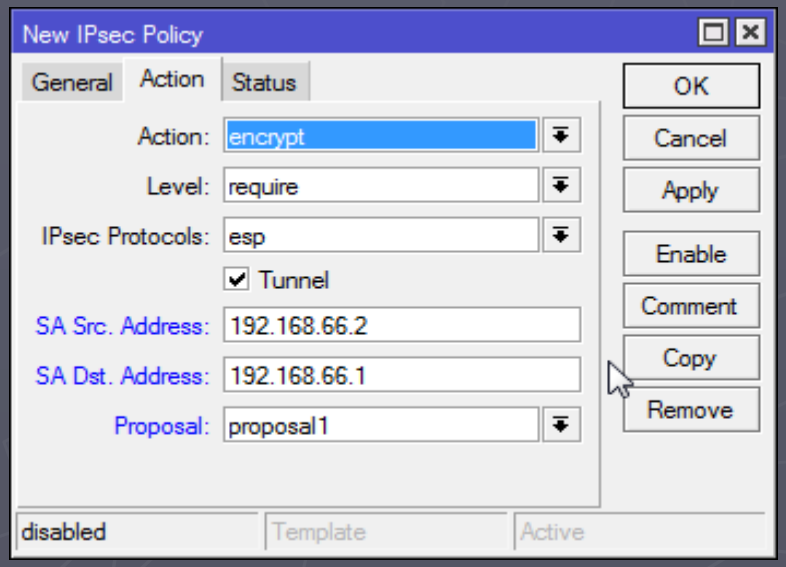
- ✓MPPE128
- ✓IPSec выборочно по протоколам+портам
- ✓Комбинация 1 и 2 способа



Что делать с RB951/2011?

Создаем выборочную IPSec Policy для SIP

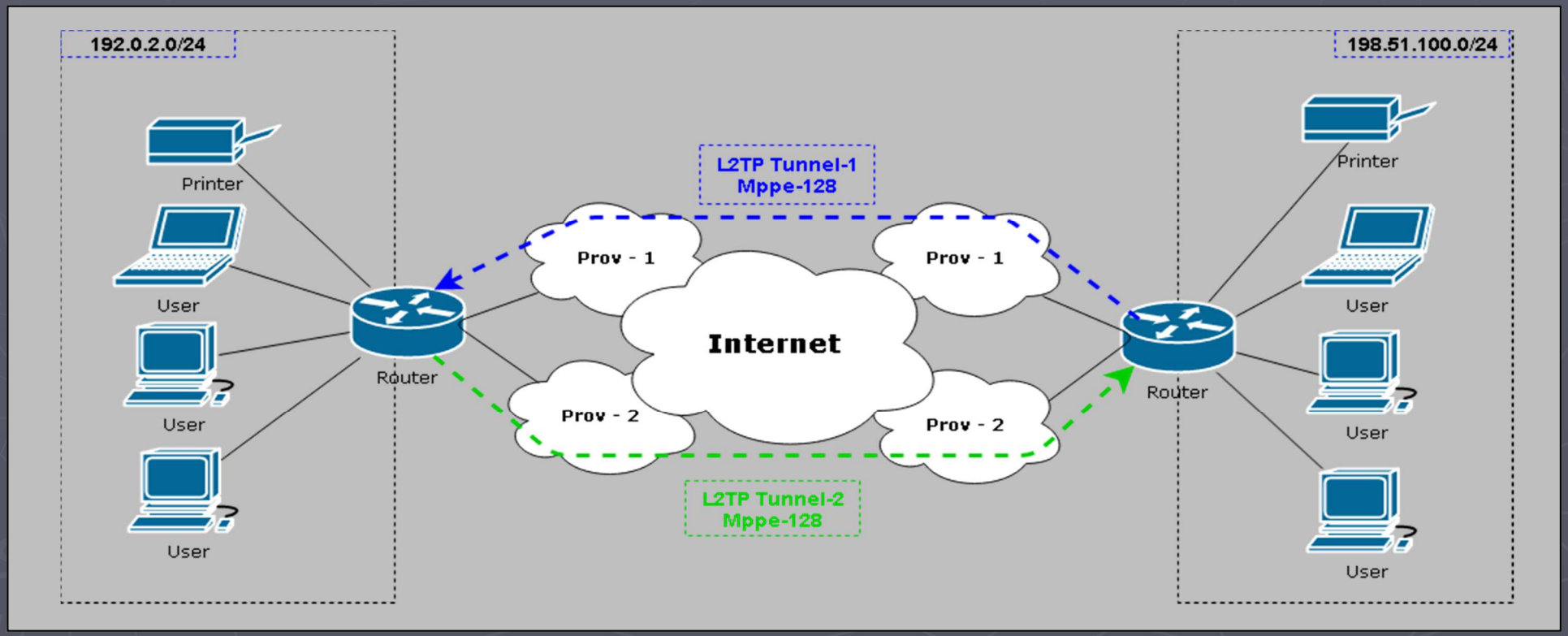




Ассиметричный роутинг

Запросы идут по одному линку

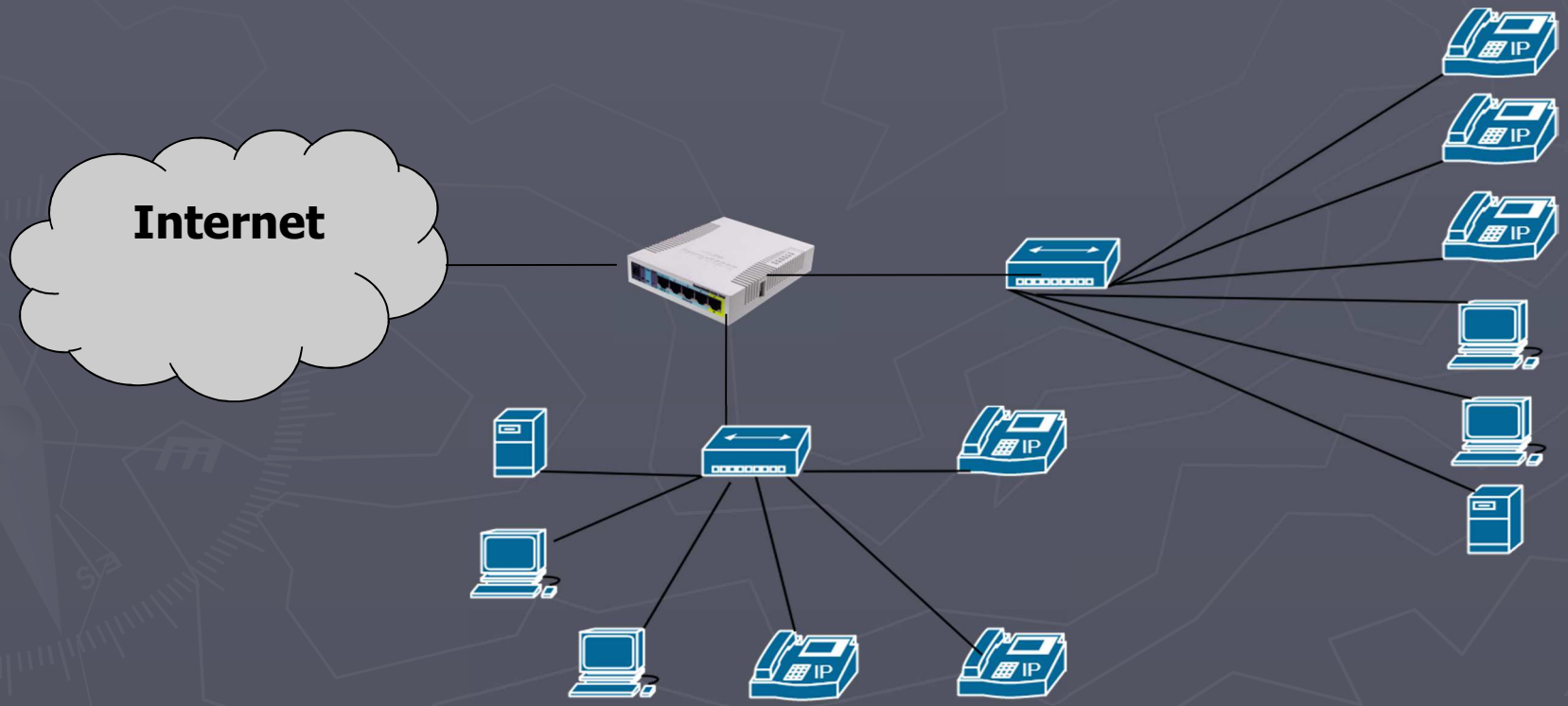
Ответы возвращаются по другому



Защита SIP внутри LAN

Сеть была построена на простых SOHO свитчах

Не поддерживающих VLAN

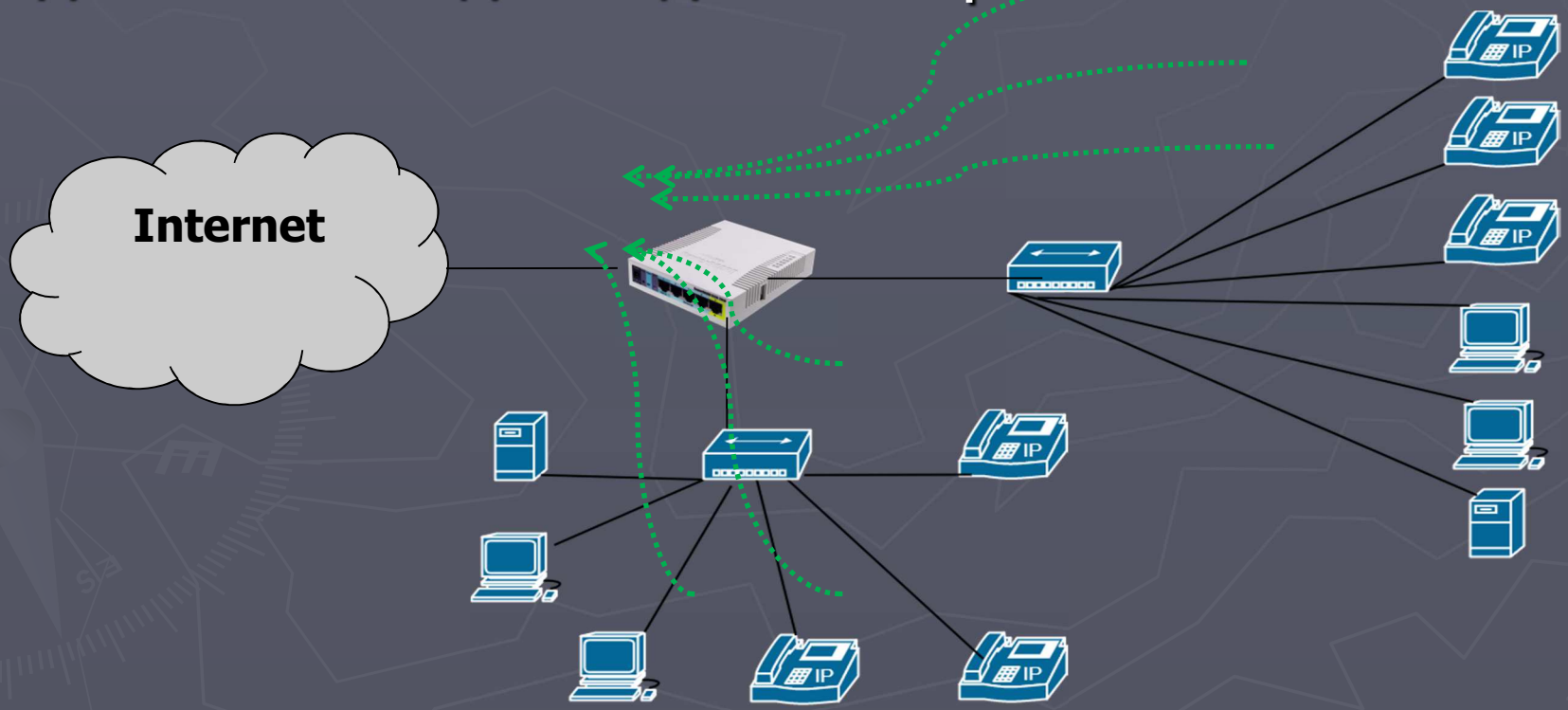


Защита SIP внутри LAN

Телефоны имеют встроенный PPPoE-клиент

Был создан локальный PPPoE-сервер с MPPE128

Выделена IP-подсеть для телефонов



Итоги первого этапа

- Внутри LAN SIP зашифрован MPPE128
- VoIP-подсеть закрыта фаерволом
- Транзит критичного трафика зашифрован по AES-256, прочий MPPE128
- Сэкономлены ресурсы CPU RB951
- При переходе на более мощное «железо» нужно лишь подправить IPSec Policy

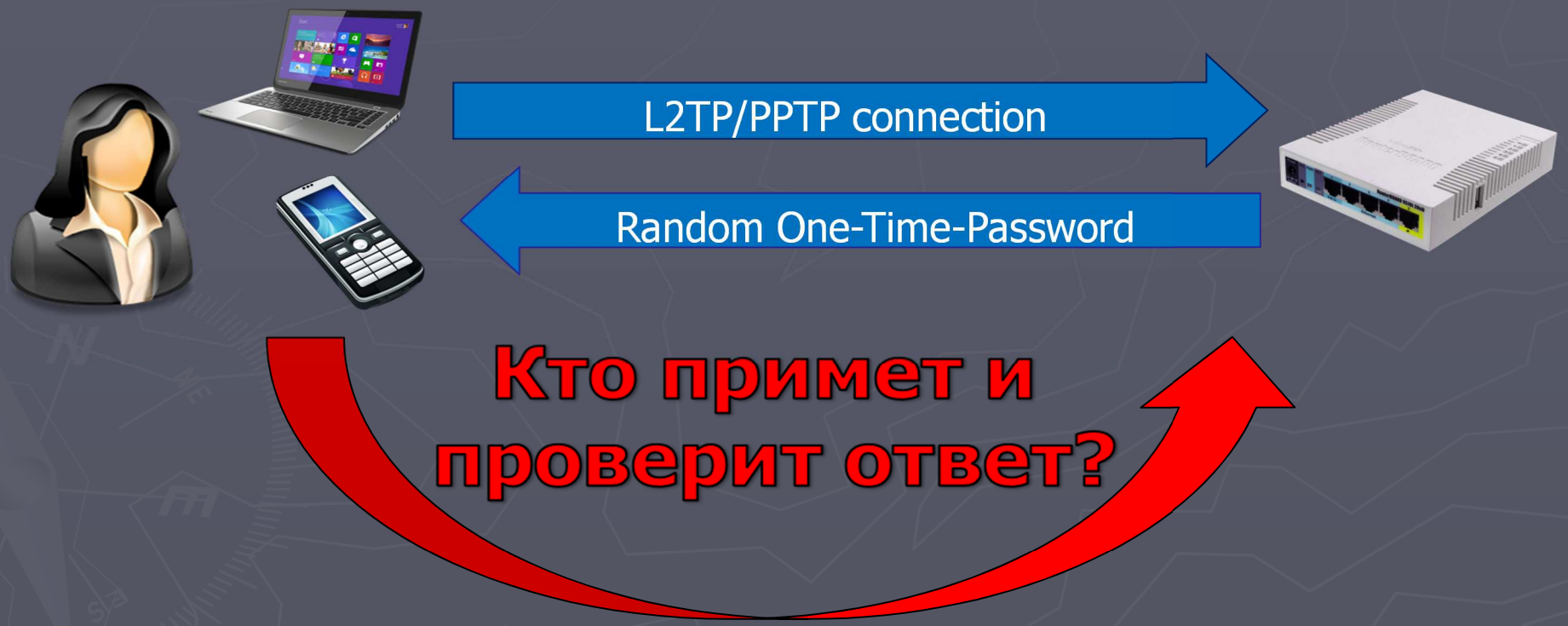
Двухфакторная аутентификация

- ✓ Без использования внешних аутентификаторов
- ✓ Средствами самого маршрутизатора
- ✓ Без затрат со стороны подключенного клиента
- ✓ Для PC и мобильных устройств

Варианты 2ФА (2FA)

- ✓ Токен, криптографический носитель
- ✓ Одноразовый пароль (OTP) доставляемый на уникальный приёмник – сотовый телефон
- ✓ Пароль зависимый от времени - Time-Based OTP (TOTP) RFC 6238

Главная проблема OTP



Фаервол проверит пароль

Пароль передается в виде URL.

Наподобие confirm-URL при регистрации на сайте

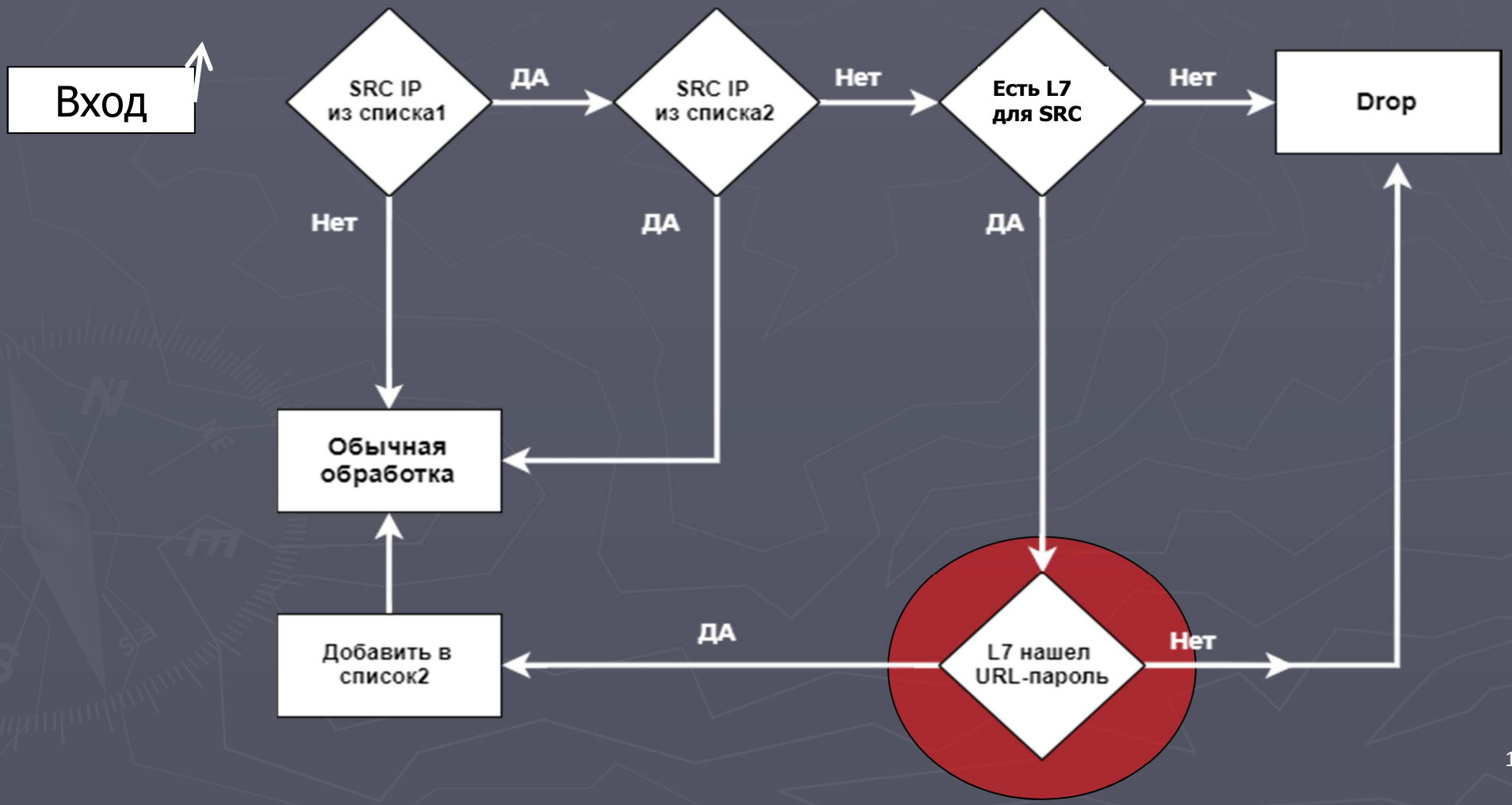
Два списка адресов:

серый – подключенный

белый – подтвержденный

Из серого списка дальше фаервола не пройти.

Фаервол проверит пароль



Фаервол проверит пароль

Пример URL-пароля: http://gw.local/otp/987123

Чтобы URL был обработан до Layer7-filter , необходимо:

DNS

Работающая служба HTTP (Proxy)

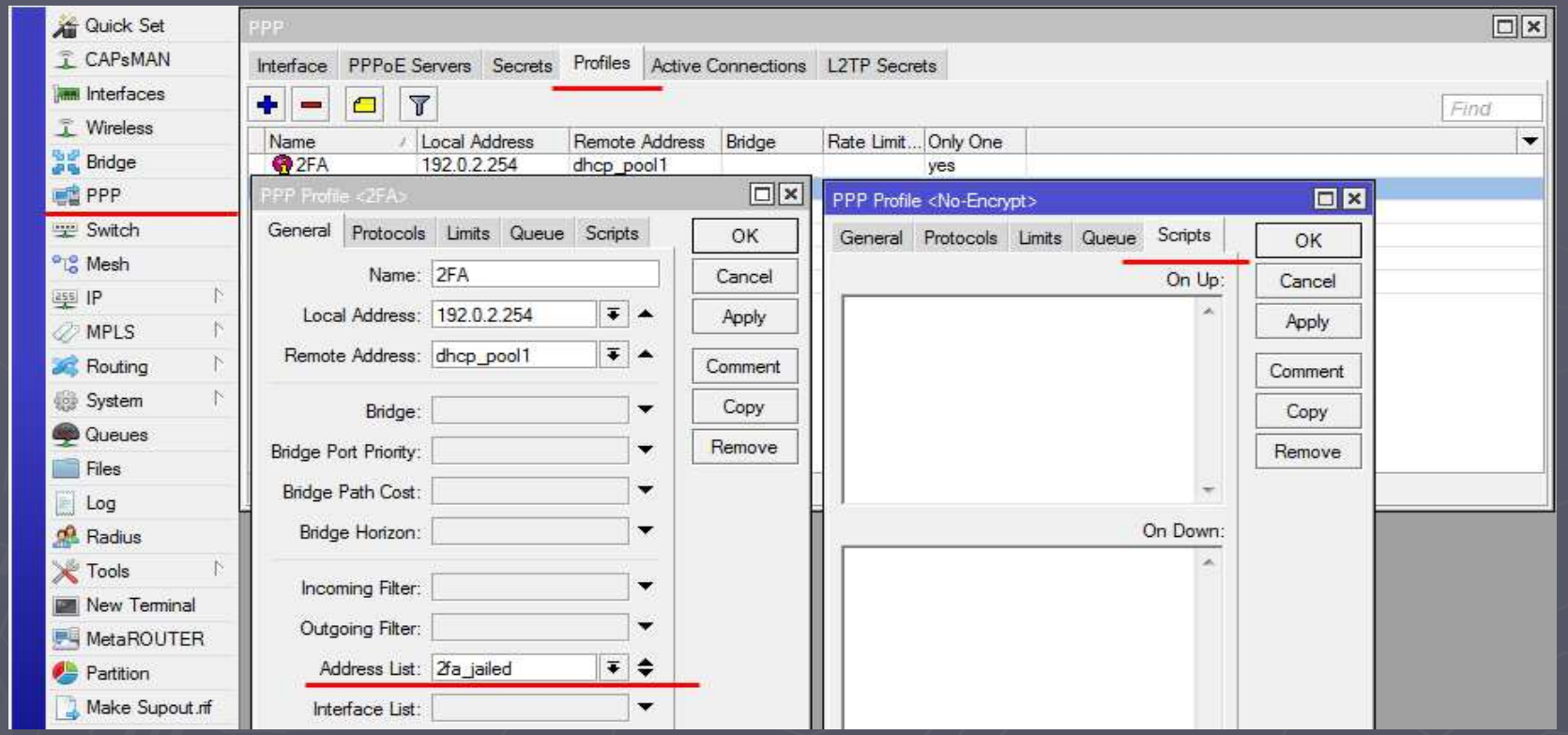
Правила фаервола в INPUT

Правила фаервола в PREROUTING (DNAT)

Правила доступа внутри HTTP-Proxy

Своя цепочка для добавления правил Layer7-filter

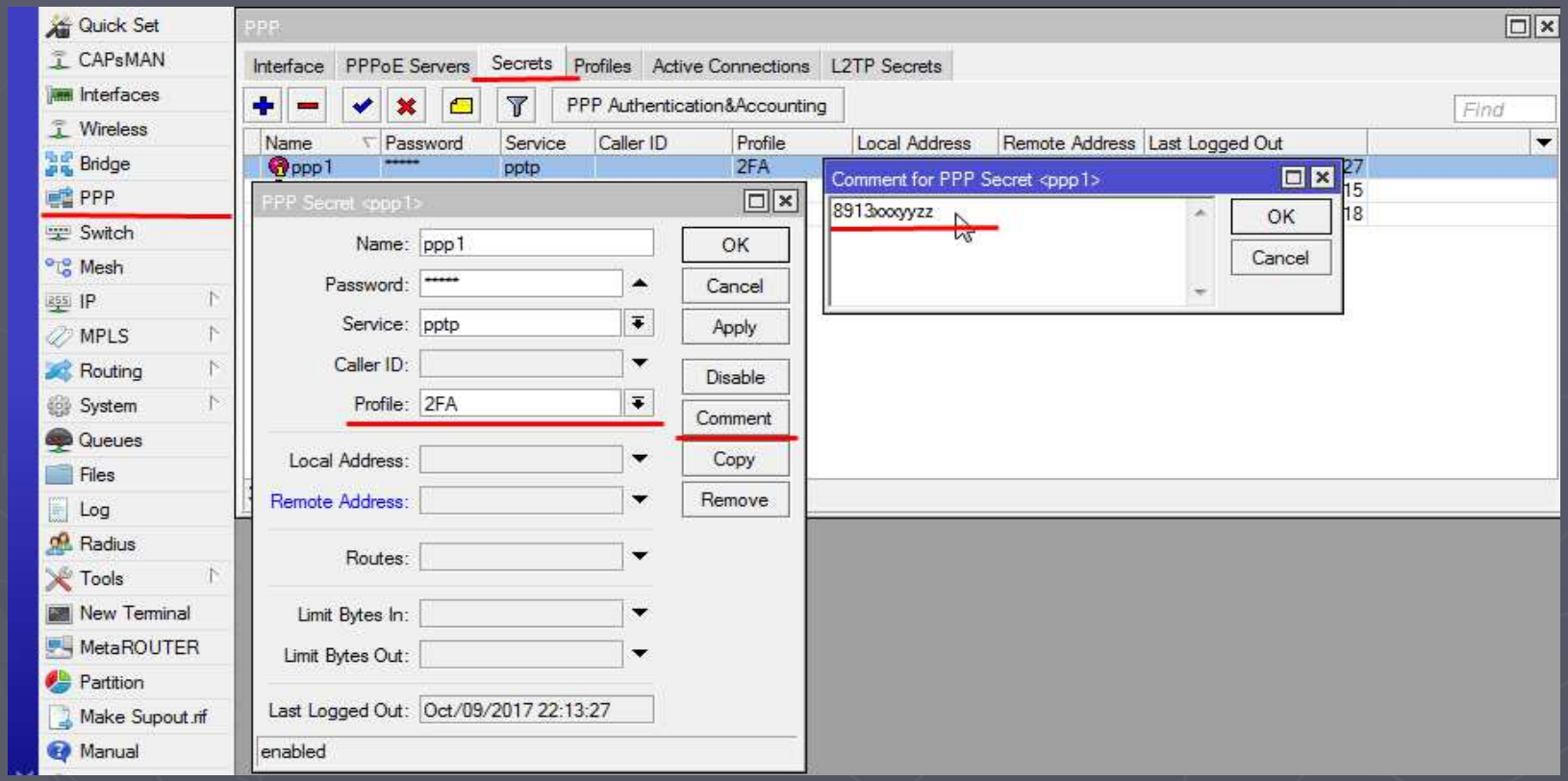
Готовим профиль



Address-List – туда автоматически добавляется IP клиента

Scripts – исполняются при подключении/отключении

Готовим пользователей



В поле комментария указываем номер телефона для СМС

Скрипт “on-up”

1. Генерирует случайный пароль ;
2. Отправляет СМС на номер из “comment” ;
3. Создаёт именной фильтр Layer7 и вносит пароль в regexp;
4. Создаёт правило фаервола со ссылкой на фильтр Layer7 для remote-IP клиента ;

Скрипт “on-up”

RouterOS передаёт переменную $remote-address – IP-адрес назначенный VPN- клиенту

```
:local listname "2fa_jailed"
:local viamodem false
:local modemport "usb2"
:local recnum1 [/ip fi address-list find address=($"remote-address") list=$listname]
/tool fetch url="https://www.random.org/strings/\?num=1&len=7&digits=on&unique=on&format=plain&rnd=new"  \ mode=https keep-result=yes dst-path=($"remote-address")
:local vpass  [pick [/file get ($"remote-address") contents] 0 6];
/ip fir address-list set $recnum1 comment=$vpass
:local vphone [/ppp secret get [find name=$user] comment]
:local msgboby ("Your code: ".$vpass."\n Or open link http://gw.local/otp/".$vpass."/")
if $viamodem do={ \
/tool sms send phone-number=$vphone message=$msgboby port=$modemport } \
else={ \
/tool e-mail send server=$ServIP  from=user@domain to=mail2sms@mcommunicator.ru  subject=("@”.$vphone) \ body=$msgboby }
```

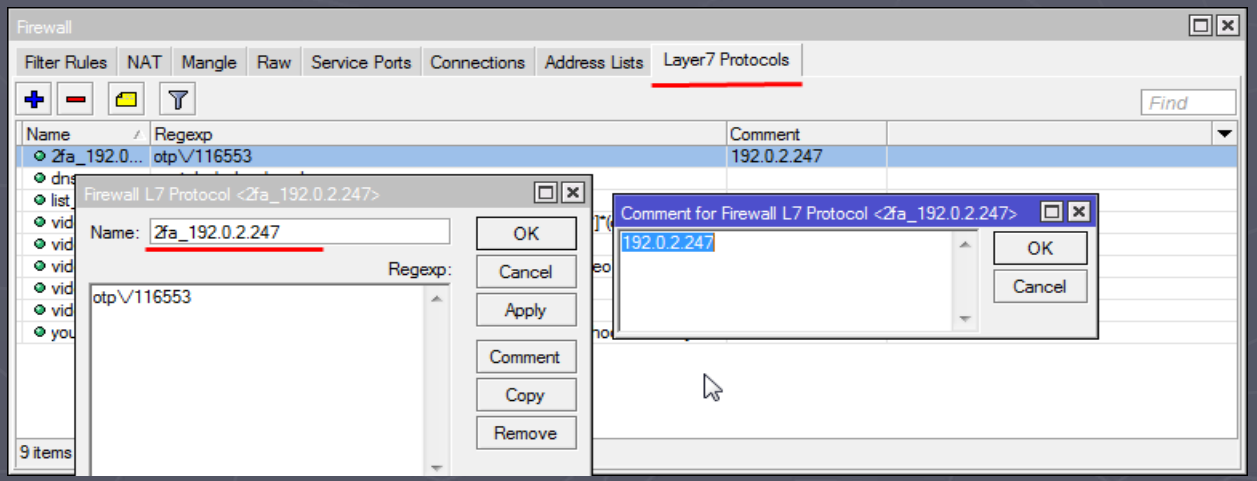
Скрипт “on-up”

Создается именной фильтр Layer7 и правило со ссылкой на него:

:local vregexp ("otp\\/".$vpass)

:local vcomment ("2fa_".($"remote-address"))

/ip firewall layer7-protocol add name=($"vcomment") comment=($"remote-address") regexp=($"vregexp")



Firewalling

/ip firewall filter add action=add-src-to-address-list address-list=2fa_approved address-list-timeout=none-dynamic \ chain=input_2fa dst-port=80,443,3128 layer7-protocol=($"vcomment") protocol=tcp src-address=($"remote-address") \ dst-limit=1,1,src-address/1m40s

Скрипт “on-down”

1. Удаляет IP клиента из белого списка;
2. Удаляет правило фаервола для IP клиента;
3. Удаляет именной фильтр Layer7;

Листинг не привожу, он тривиален. Обычный remove [find…]

Системные настройки

Создается статическое имя DNS

```
/ip dns static add address=192.0.2.1 name=gw.local ttl=1m
```

Настраивается INPUT:

```
/ip firewall filter
add action=accept chain=input dst-port=53 in-interface=all-ppp protocol=udp src-address-list=2fa_jailed
add action=jump chain=input in-interface=all-ppp jump-target=input_2fa src-address-list=2fa_jailed
add action=accept chain=input dst-port=3128 in-interface=all-ppp protocol=tcp src-address-list=!2fa_approved
add action=reject chain=input in-interface=all-ppp reject-with=icmp-network-unreachable src-address-list=!2fa_approved
```

Настраивается FORWARD:

```
add action=reject chain=forward in-interface=all-ppp reject-with=icmp-network-unreachable \
   src-address-list=!2fa_approved
```

Создается цепочка INPUT_2FA для помещения туда фильтров Layer-7 regexp:

```
add action=return chain=input_2fa in-interface=all-ppp src-address-list=2fa_approved
```

Системные настройки

Настраивается DST-NAT на перехват HTTP-запросов от VPN-клиентов:

```
/ip firewall nat
add action=redirect chain=dstnat_redir dst-port=80,443 protocol=tcp src-address-list=!2fa_approved to-ports=3128
add action=jump chain=dstnat dst-port=80,443 in-interface=all-ppp jump-target=dstnat_redir protocol=tcp  \
src-address-list=2fa_jailed
add action=redirect chain=dstnat in-interface=all-ppp src-address-list=!2fa_approved
```

Настраивается HTTP-PROXY:

```
/ip proxy
set enabled=yes port=3128
/ip proxy access
add action=deny redirect-to=gw.local./mikrotik_logo.png src-address=192.0.2.0/24
```

Создается редирект на лого MikroTik при успешной авторизации и доступе к прокси

Генерация паролей

1. Через API сервиса RANDOM.ORG. Просто и доступно. Позволяет получать буквенные, цифровые и буквенно-цифровые пароли необходимой длины

2. Через реализацию генерации псевдослучайной последовательности цифр средствами RouterOS. Требует дополнительного программирования, ограничена скриптовым языком и сильно зависит от счётчиков роутера.

Доставка паролей

1. Через USB-модем huawei e173 или аналогичный.

Плюсы: быстрее, проще в настройке

Минусы: однопоточность. Не подходит для нагруженного VPN-сервера.

2. Через сервис email2sms сотового оператора.

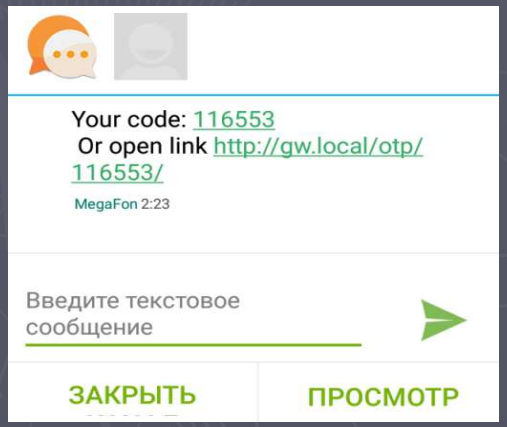
Плюсы: многопоточный.

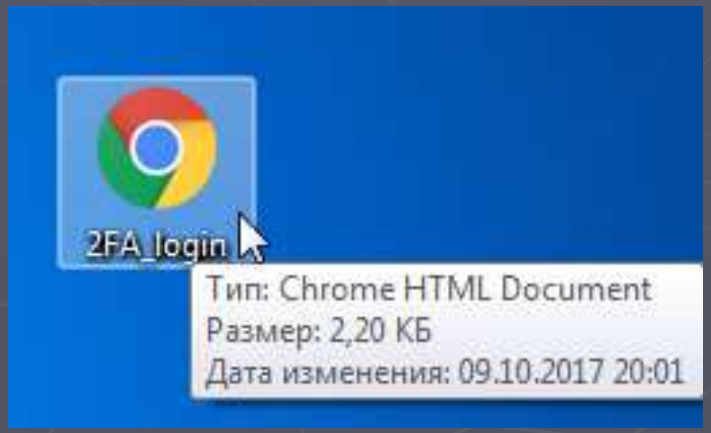
Минусы: меделннее, требует допсоглашений с оператором

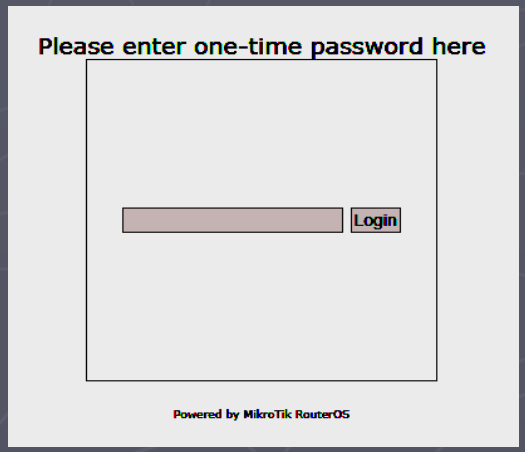
Ввод паролей

1. Для телефона в составе СМС сразу приходит ссылка-пароль, которую можно открыть.

2. На компьютере сохраняется простая HTML-страничка содержащая окно ввода и кнопку перехода







Ввод паролей

При успешной аутентификации появляется лого

Ввод паролей

Минимальная HTML-страничка ввода пароля:

```
<html>
<head> <title>SMS OTP login</title> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> </head>
<body>
<form name="login" action="location.href='http://gw.local/otp/'+document.getElementById('text').value"  method="post"
 <input id="text" type="text"/>
<input type="button" value="Login" onclick="location.href='http://gw.local/otp/'+document.getElementById('text').value"/>
</form>
</body>
</html>
```

Итоги второго этапа

- Внедрена 2FA на основе OTP;
- Пользователи VPN могут быть разделены на группы с 2FA и без неё;
- Механизм работает с динамическими IP
- Работает на любом роутере MikroTik

Заказчик доволен

Ссылки

- http://wiki.mikrotik.com – Документация
- https://www.random.org – Генератор чисел
- http://mcommunicator.ru – email2sms МТС
- https://arxiv.org/pdf/1309.5344.pdf - Статистика по 2FA