```
MMM      MMM       KKK                          TTTTTTTTTTT      KKK
MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK
```

```
 SSSSS     SSSSS    HH   HH
SS        SS        HH   HH
 SSSSS     SSSSS    HHHHHHH
     SS        SS   HH   HH
 SSSSS     SSSSS    HH   HH
```

[Vadim@Shepelev] > MikroTik User Meeting. Россия, Москва 2014

> О себе

Вадим

Работаю системным администратором более 5-ти лет

Первое знакомство с MikroTik ~2003 году, любовь с первого взгляда ;)

MTCNA, MTCTCE, MTCWE

В компании используется ~250 RouterBoard's

> В докладе будет рассмотрено:

- **Как управлять 10\20\50 роутерами одновременно;**
- **Как управлять десятками роутеров при помощи скриптов;**
- **Как осуществлять интеллектуальное резервное копирование;**
- **Как безопасно пользоваться ресурсами локальной сети из Интернет, не настраивая VPN и DST-NAT;**
- **Как безопасно использовать MikroTik в качестве SOCKS прокси.**

Общая информация об SSH

> Общая информация об SSH

Аутентификация:

- **По логину и паролю;**
- **По логину и ключу:**
  - **Используется пара ключей, публичный и приватный;**
  - **Приватный ключ может (а чаще всего должен) быть защищен паролем;**
  - **MikroTik поддерживает DSA ключи.**

> Общая информация об SSH

Преимущества аутентификации по ключу:

- **Удобство:**
  - **можно подключаться к роутеру без ввода пароля**
  - **можно давать клиентам свой публичный ключ, без боязни засветить пароль**
  - **не нужно помнить огромное количество уникальных паролей**
- **Возможность автоматизации при помощи скриптов;**
- **Безопасность:**
  - **проблематично брутфорсить)**
  - **утеря роутера или бинарного бекапа не столь фатальны.**

> Общая информация об SSH

Задача:

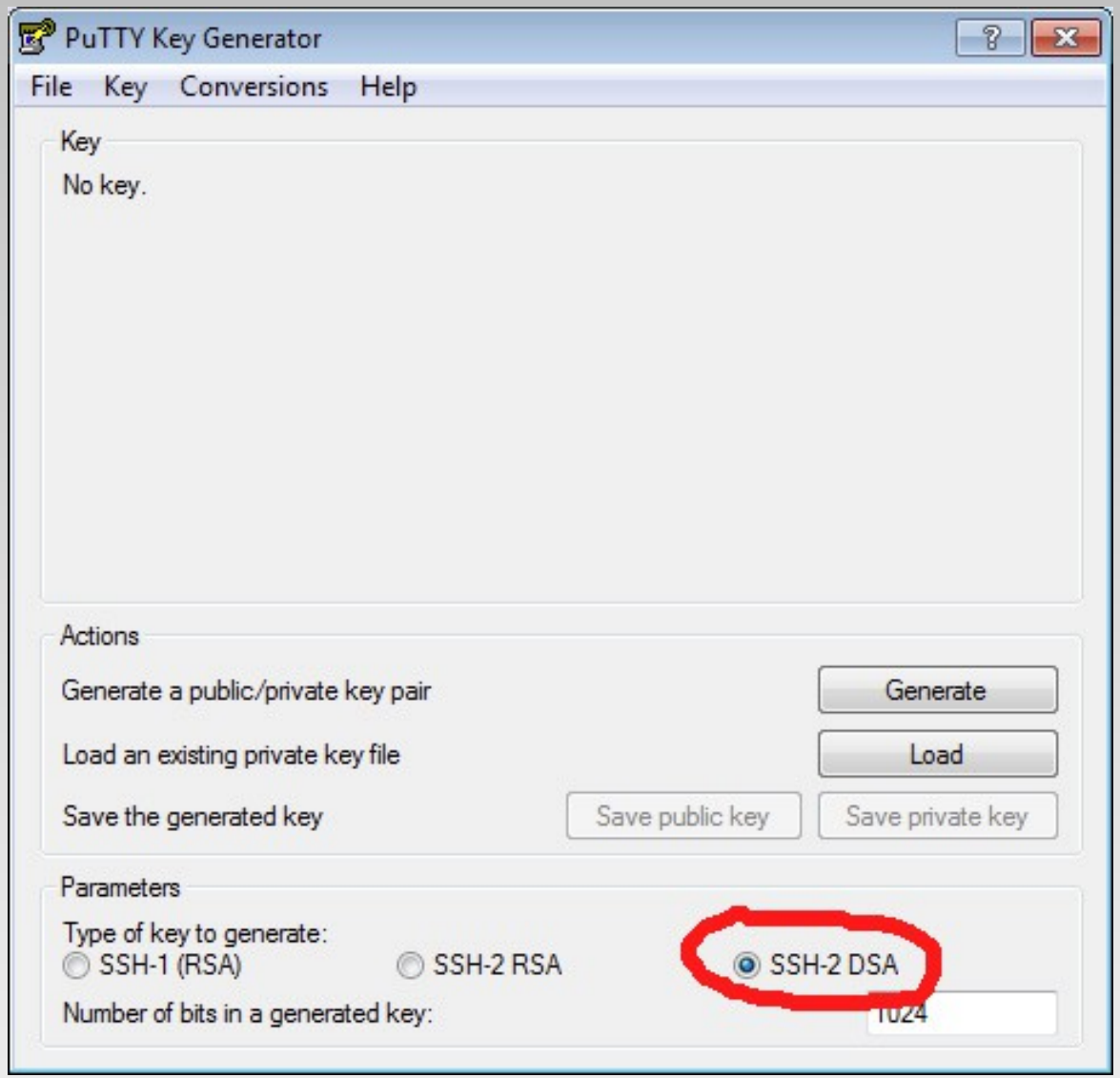
Сгенерировать пару ключей (публичный и приватный)

> Общая информация об SSH

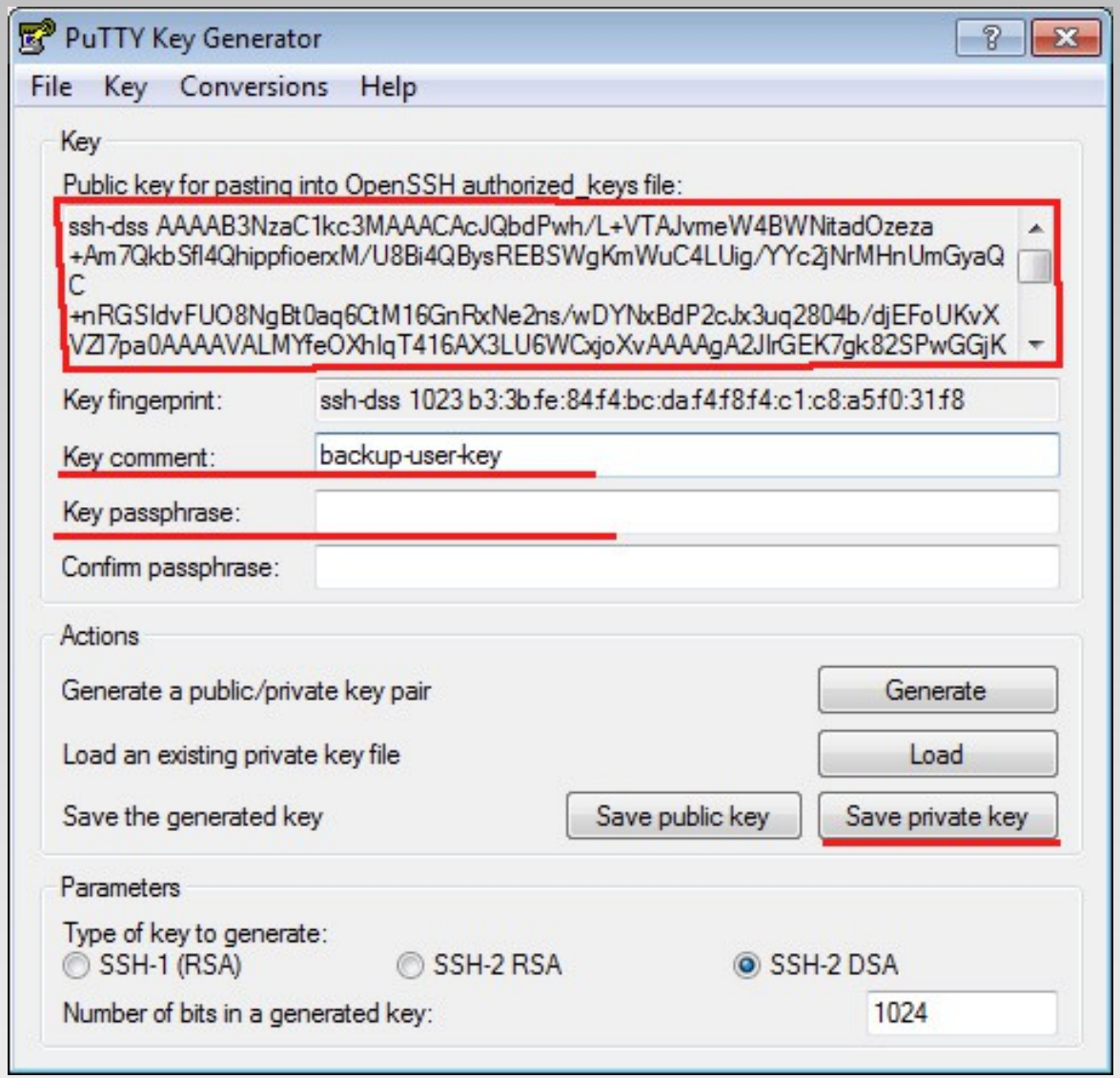
Создание ключей в Windows.

Для создания ключей можно использовать PUTTYGEN.EXE из комплекта PuTTY
http://www.chiark.greenend.org.uk/~sgtatham/putty/

> Общая информация об SSH



> Общая информация об SSH



> Общая информация об SSH

Создание ключей в *nix.

Ключи создаются командой (должен быть установлен OpenSSH):

ssh-keygen -t dsa -C _комментарий_

Публичный и приватный ключ создадутся в каталоге ~/.ssh

> Общая информация об SSH

В итоге мы получили:

- **Файл приватного ключа, который будет храниться на локальном компьютере;**
- **Публичный ключ, который нужно импортировать на подконтрольные маршрутизаторы.**

> Общая информация об SSH

Кое что о безопасности:

- **Берегите приватный ключ!**
- **По возможности защищайте ключ паролем.**

> Общая информация об SSH

Агенты ключей:

- **Хранят ключи и пароли к ним;**
- **Пароль вводится при запуске агента;**
- **При подключении по ssh к удаленному серверу агент автоматически осуществляет аутентификацию, вводить пароль на ключ не нужно.**

Примеры агентов:

- ***nix - ssh-agent;**
- **Windows - PAGEANT.EXE из комплекта PuTTY.**

SSH и автоматизация

> SSH и автоматизация

Для овладения навыками автоматизации крайне желательно иметь представления о написании скриптов для MikroTik, а так же импорте и экспорте конфигураций.

Рекомендую ознакомиться с:

- **http://wiki.mikrotik.com/wiki/Manual:Scripting**
- **http://wiki.mikrotik.com/wiki/Scripts**
- **http://wiki.mikrotik.com/wiki/Manual:Configuration_Management**

> SSH и автоматизация

Задача:

Одновременно на нескольких MikroTik создать пользователя и импортировать ему публичный ключ.

> SSH и автоматизация

Внимание! После импорта ключа пользователю, зайти под этим пользователем по SSH возможно только по ключу!

Команда

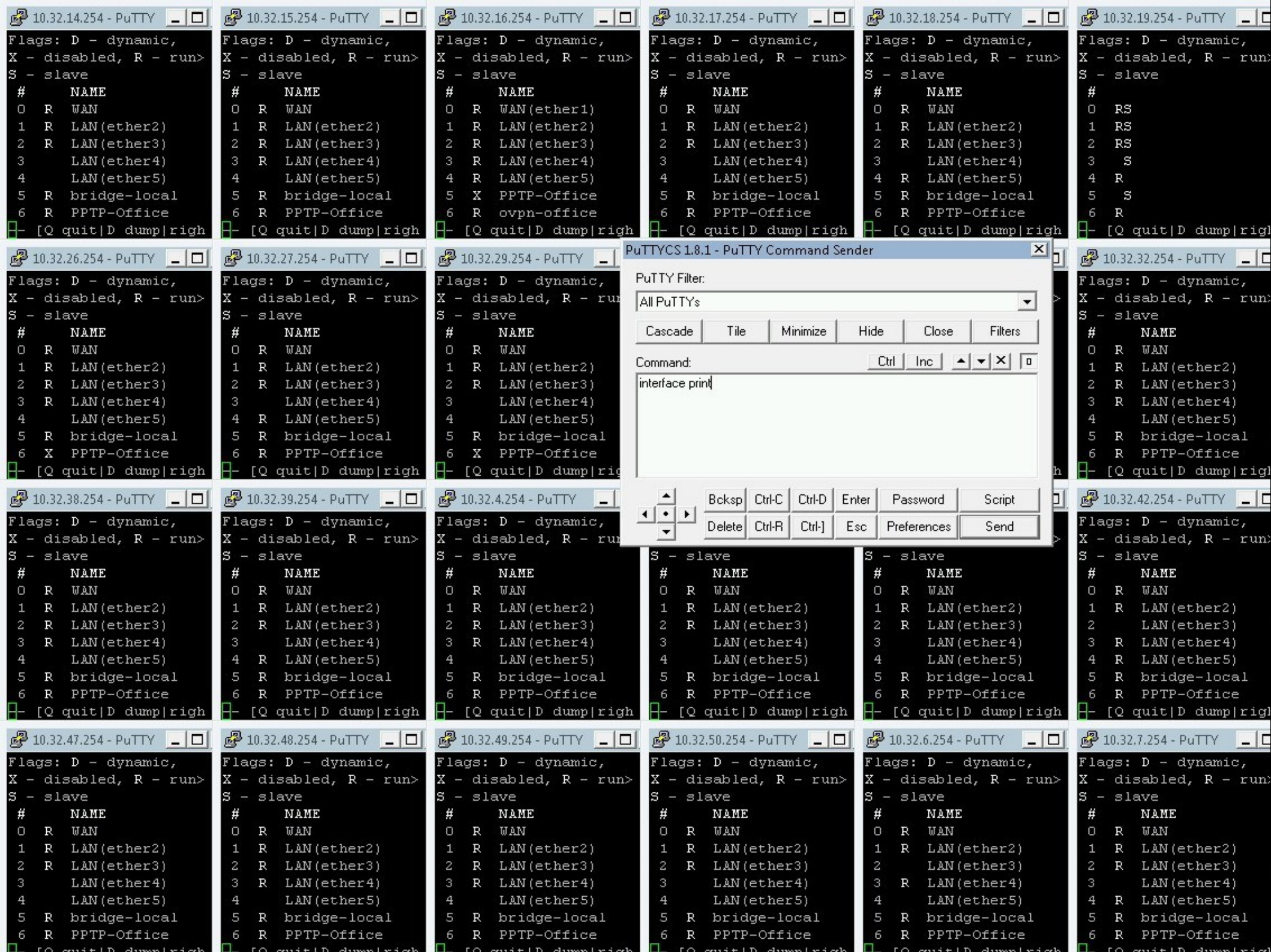
/ip ssh set always-allow-password-login=yes

возвращает возможность заходить по SSH, используя пароль.

> SSH и автоматизация

Для решения подходит следующий инструментарий:

- **Под Windows PuTTY + PuTTYCS (PuTTY Command Sender) (http://www.millardsoftware.com/puttycs);**
- **Есть аналог под *nix - clusterssh.**


10.32.14.254 - PuTTY
10.32.15.254 - PuTTY
10.32.16.254 - PuTTY
10.32.17.254 - PuTTY
10.32.18.254 - PuTTY
10.32.19.254 - PuTTY
10.32.26.254 - PuTTY
10.32.27.254 - PuTTY
10.32.29.254 - PuTTY
10.32.32.254 - PuTTY
10.32.38.254 - PuTTY
10.32.39.254 - PuTTY
10.32.4.254 - PuTTY
10.32.42.254 - PuTTY
10.32.47.254 - PuTTY
10.32.48.254 - PuTTY
10.32.49.254 - PuTTY
10.32.50.254 - PuTTY
10.32.6.254 - PuTTY
10.32.7.254 - PuTTY
Flags: D - dynamic,
X - disabled, R - run>
S - slave
NAME
0 R WAN
1 R LAN(ether2)
2 R LAN(ether3)
3 LAN(ether4)
4 LAN(ether5)
5 R bridge-local
6 R PPTP-Office
[Q quit|D dump|righ
PuTTYCS 1.8.1 - PuTTY Command Sender
PuTTY Filter:
All PuTTYs
Cascade
Tile
Minimize
Hide
Close
Filters
Command:
Ctrl
Inc
interface print
Bcksp
Ctrl-C
Ctrl-D
Enter
Password
Script
Delete
Ctrl-R
Ctrl-]
Esc
Preferences
Send

> SSH и автоматизация

Пример CMD файла для подключения ко множеству роутеров:

start PUTTY.EXE -ssh admin@10.32.1.254

start PUTTY.EXE -ssh admin@10.32.2.254

...

start PUTTY.EXE -ssh admin@10.32.50.254

start PuTTYCS.exe

> SSH и автоматизация

У PuTTY есть опции запуска, *например:*

***-load "имя_сессии"* - запустить PuTTY с параметрами, которые ранее были сохранены как сессия (можно сохранить множество настроек, от пути до файла закрытого ключа, логина, кодировки, настройки туннелей, etc до удаленного хоста и порта);**

-P _порт_- указать порт, к которому следует подключаться;

-l _логин_ - использовать указанный логин;

-pw _пароль_ - использовать указанный пароль (крайне не безопасно)

-i _путь_до_ключа_ - указать приватный SSH ключ, который нужно использовать.

> SSH и автоматизация

/user add name=automate_user group=full password=somePasswd comment="User for automate"

/file print file=dsa_pub.txt

:delay 3

/file set dsa_pub.txt contents="ssh-dss AAAAB3NzaC1kc3MAAACAcJQbdPwh/L+VTAJvmeW4BWNitadOzeza+Am7QkbSfl4QhippfioerxM/U8Bi4QBysREBSWgKmWuC4LUig/YYc2jNrMHnUmGyaQC+nRGSIdvFUO8NgBt0aq6CtM16GnRxNe2ns/wDYNxBdP2cJx3uq2804b/djEFoUKvXVZl7pa0AAAAVALMYfeOXhIqT416AX3LU6WCxjoXvAAAAgA2JIrGEK7gk82SPwGGjK9tz/wdMvTV5D/SxWcl8fwoE6PbvQqxOdG32DDU1VrpMvAQUOIJ5pueNYy/iQyZy9THfS/mPknzsZbK4wFjfWJ1Khyhtbs9gxPYCKMwFi3KoTeeA3MltEFmUx537Hn3rZduifZpWhEXifjWwc7rbiE97AAAAgGg6eMcTbNQIykO8YYJlQ5NqNT+jiomxcFbbRFJuYHFN7I1B5nBsQn7S8aIgjm6OJ/V1FKOeBzxQ7efTmBJH2nNsw6J4x70Y346omv4NvpAx139FMpd8Z6aoAmKgvZJuuWM1AExfZnAl6dRSLOEYul0c2aBvCgua90vP8dLfsRW8 backup-user-key"

:delay 3

/user ssh-keys import user=automate_user public-key-file=dsa_pub.txt

> SSH и автоматизация

Для чего еще это может быть полезно?

- **Работа с несколькими роутерами в интерактивном режиме, проверка и перенастройка параметров SNMP, Traffic Flow, Wireless, SMB, etc...**
- **Создание и удаление пользователей.**
- **Проверка связи до какого-то узла сразу с нескольких маршрутизаторов (traceroute, ping).**

> SSH и автоматизация

Задача:

Регулярно обновлять WEB Proxy Acess List на 50-ти маршрутизаторах.

> SSH и автоматизация

Если делать это вручную, то можно "поехать"...

> SSH и автоматизация

> SSH и автоматизация

Для решения подходит следующий инструментарий:

- **PSCP.EXE - Утилита командной строки для копирования файлов, в качестве транспорта используется SSH;**
- **PLINK.EXE - Утилита командной строки, позволяющая подключаться по SSH и запускать команды на удаленном устройстве.**

Обе утилиты входят в комплект PuTTY.

> SSH и автоматизация

Пример .RSC файла, который очистит access list web proxy и запишет его заново:

/ip proxy access { :foreach r in=[find] do={ remove $r }}

/ip proxy access

add action=allow disabled=no dst-host=mikrotik.com dst-port=""

add action=allow disabled=no dst-host=.mikrotik.com dst-port=""*

add action=allow disabled=no dst-host=routerboard.com dst-port=""

add action=allow disabled=no dst-host=.routerboard.com dst-port=""*

...

add action=deny disabled=no dst-port=""

> SSH и автоматизация

Пример CMD файла для копирования и применения .RSC файла на множество роутеров:

```
@set username=admin
@set filename=new_proxy_access_list.rsc


@set ip=10.32.1.254
PSCP.EXE %filename% %username%@%ip%:/
PLINK.EXE %username%@%ip%:/ import file-name=%filename%
...
@set ip=10.32.50.254
PSCP.EXE %filename% %username%@%ip%:/
PLINK.EXE %username%@%ip%:/ import file-name=%filename%
```

> SSH и автоматизация

Задача:

Регулярно, по расписанию, менять пароль на гостевую WiFi сеть и отправлять его администратору на email.

> SSH и автоматизация

Пример sh скрипта для смены пароля на WiFi сеть:

```
#!/bin/sh

pass=`/usr/bin/pwgen -s -v 12 1`

ssh -l admin -i ~/.ssh/id_dsa 192.168.1.253 "interface wireless security-profiles set WiFi-Guest wpa2-pre-shared-key=$pass"

ssh -l admin -i ~/.ssh/id_dsa 192.168.2.253 "interface wireless security-profiles set WiFi-Guest wpa2-pre-shared-key=$pass"

...
ssh -l admin -i ~/.ssh/id_dsa 192.168.10.253 "interface wireless security-profiles set WiFi-Guest wpa2-pre-shared-key=$pass"

echo "$pass" | mutt vs@foto-glaz.ru -s "New Pass for WiFi-Guest Net"
```

> SSH и автоматизация

Для чего еще может это быть полезно?

- **Регулярно обновлять IP листы**
- **Записи DNS Static**
- **Mangle**
- **Wireless Access List**
- **etc...**

MikroTik, SSH и языки программирования

> MikroTik, SSH и языки программирования

Задача:

- **Настроить резервное копирование конфигураций роутеров MikroTik;**
- **Делать резервные копии, только если конфигурация роутера изменилась;**
- **Обеспечить версионность резервных копий;**
- **Не производить запись на Flash память роутеров без необходимости;**
- **Отправлять по email отчеты об изменениях в конфигурации;**

> MikroTik, SSH и языки программирования

Эту и более сложные задачи позволят решить языки программирования + библиотека для работы с SSH.

Например, можно использовать:

- **Python + paramiko**
- **Ruby + Net::SSH**

> MikroTik, SSH и языки программирования

Логика работы скрипта:

- **Прочитать список IP из файла;**
- **Подключиться к роутерам по SSH (аутентификация по паролю или ключу);**
- **Если резервная копия ранее не создавалась, создать каталог вида IP-Identity-серийный_номер\ДАТА и записать в него бинарный бекап и export;**
- **Если ранее уже была создана резервная копия, сверить последний export с текущим, что на роутере (причем flash память роутера не используется). Если обнаружена разница, создать резервную копию в подкаталоге IP-Identity-серийный_номер\ДАТА;**
- **Отправить на email оповещения об ошибках и информацию об изменении конфигурации со списком изменений.**

> MikroTik, SSH и языки программирования

Скрипт можно найти по адресу:

https://github.com/0x566164696D/mt_backup_ng

bit.ly/1hbd8rs

> MikroTik, SSH и языки программирования

Для чего еще это может быть полезно?

- **Автоматизировать настройку однотипных устройств для удаленных филиалов.**
- **Написать ПО для управления конфигурациями парка роуртеров, что-то типа Puppet (получение конфигурации - анализ - действие).**

SSH туннели

> SSH туннели

Задача:

- **Получить доступ к своему рабочему компьютеру по RDP из любого места в Интернет;**
- **Без использования VPN;**
- **Без использования DST-NAT;**
- **Безопасно.**

> SSH туннели

Решением может служить SSH туннель.

Логика работы:

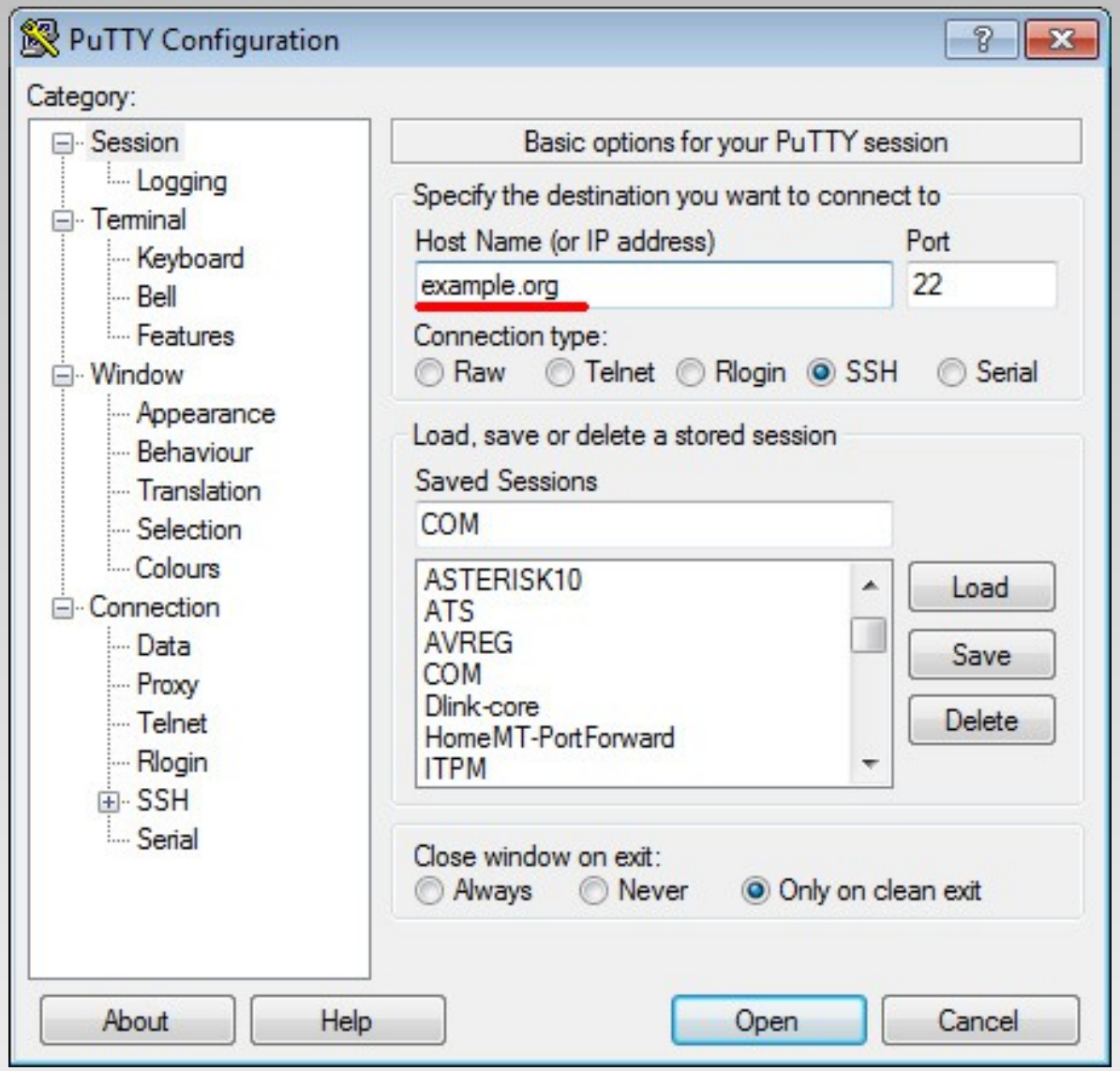
- **После подключения по SSH, на localhost откроется порт, данные с которого будут проброшены на удаленный хост, в другой локальной сети, за MikroTik;**
- **Данные передаются в зашифрованном виде внутри ssh;**
- **Соединения с хостами в удаленной локальной подсети устанавливаются "от лица" роутера.**

> SSH туннели

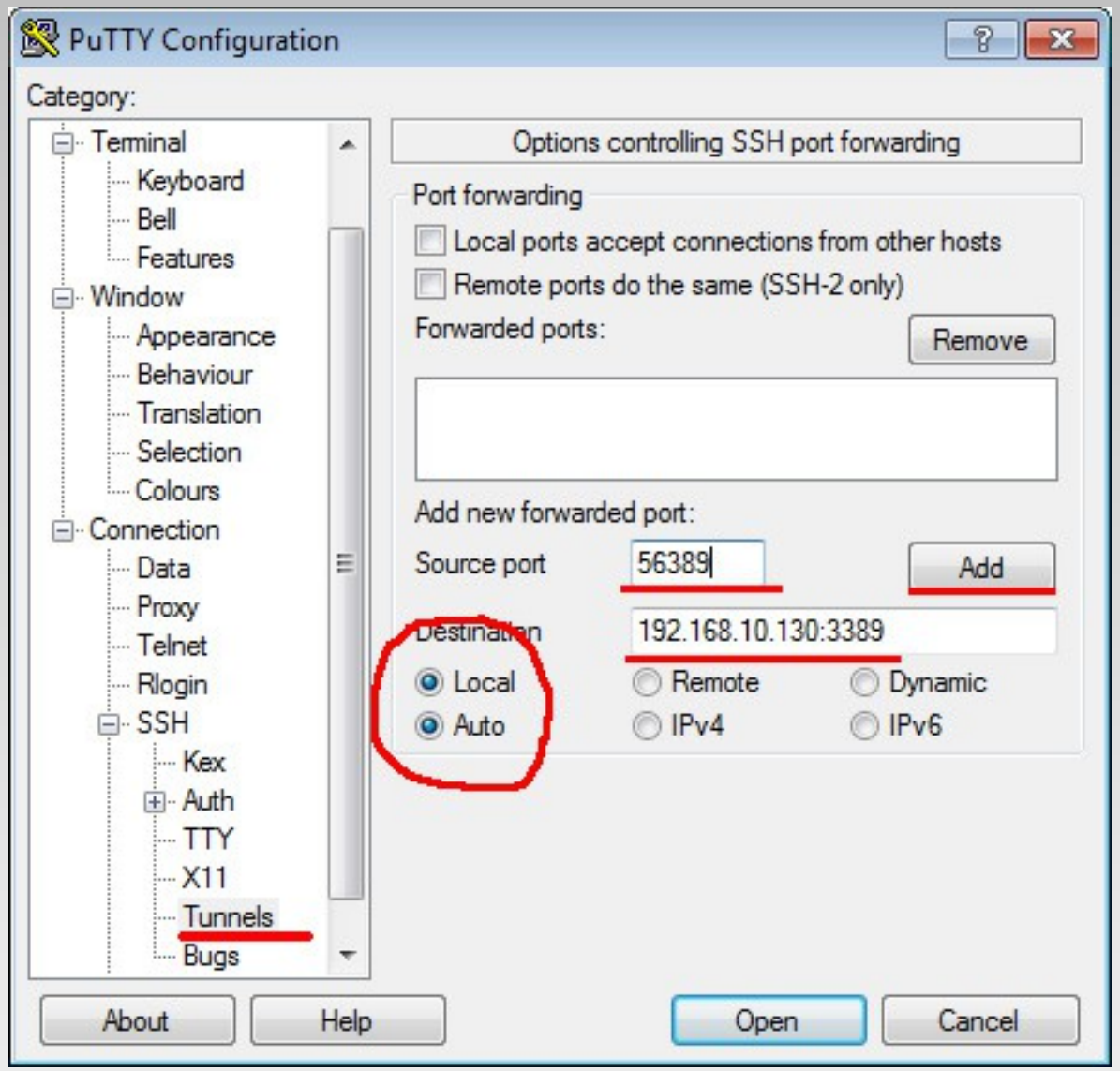
Особенности данного решения:

- **Простота настройки.**
  - **MikroTik настраивать не нужно.**
- **Безопасно:**
  - **SSH - проверенный временем инструмент.**
  - **Данные передаются внутри SSH в зашифрованном виде.**
- **Работает быстрее VPN (субъективно)**

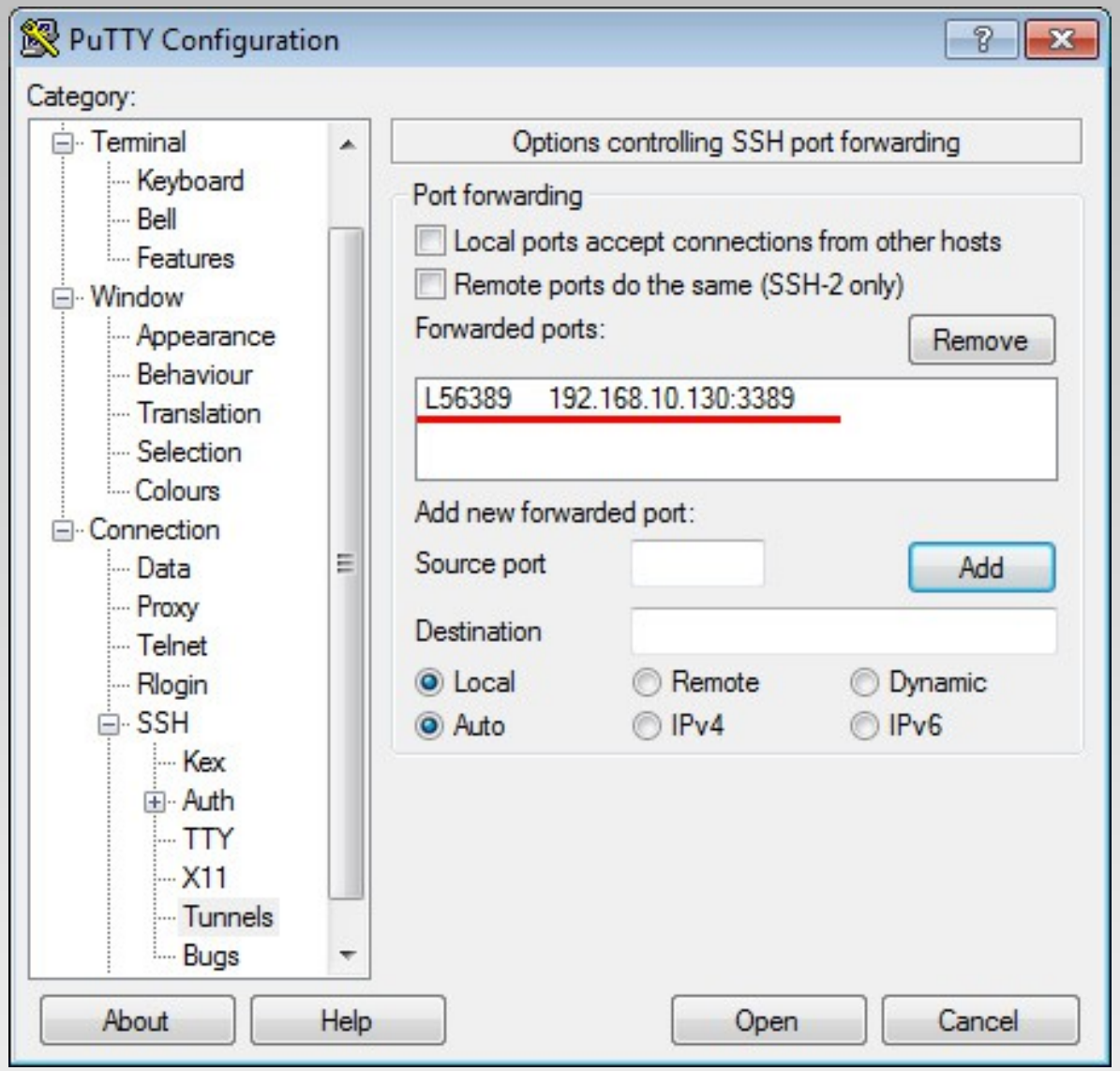
> SSH туннели


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
example.org
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
COM
ASTERISK10
ATS
AVREG
COM
Dlink-core
HomeMT-PortForward
ITPM
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

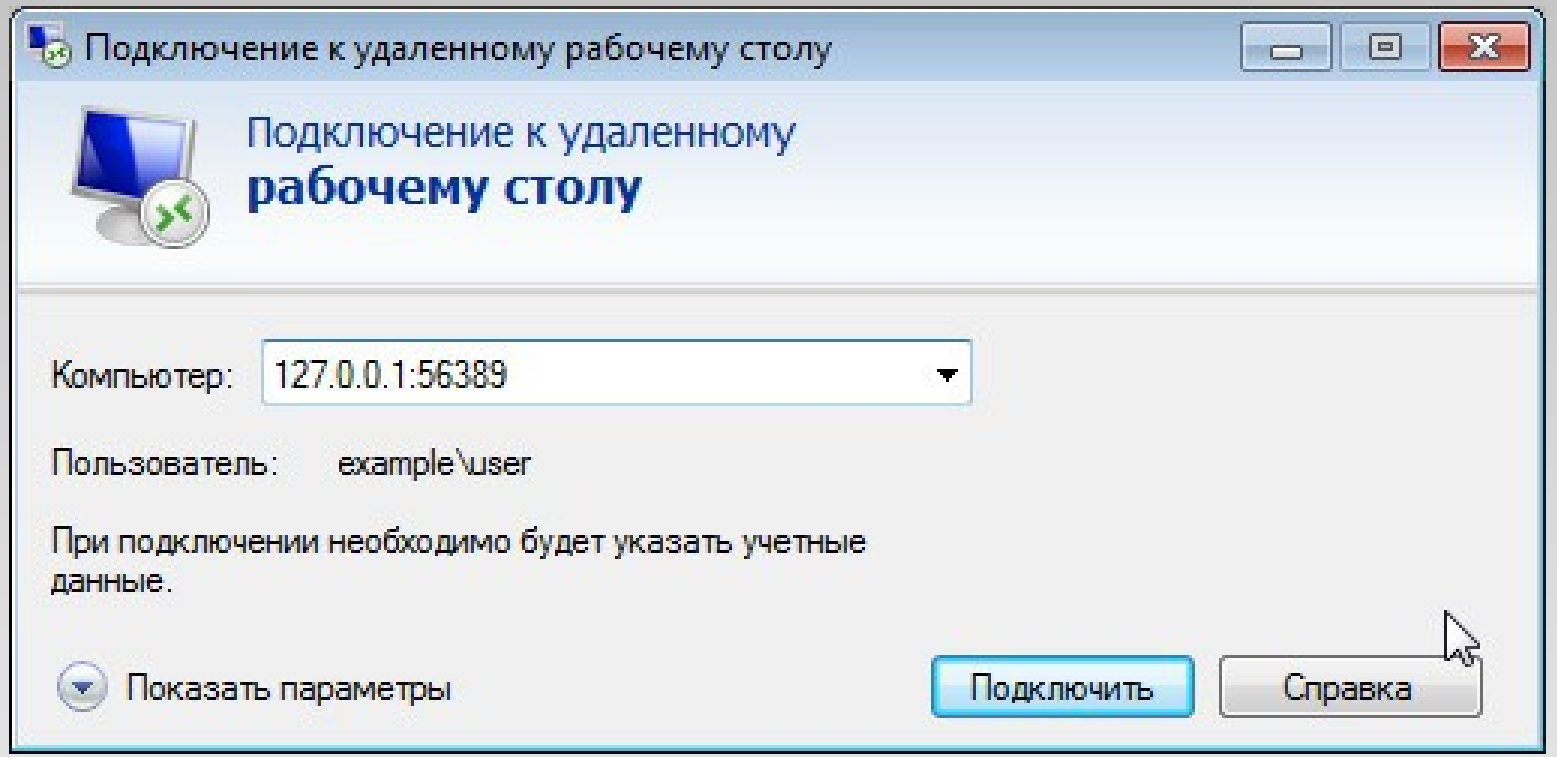
> SSH туннели


PuTTY Configuration
Category:
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
Add new forwarded port:
Source port
56389
Add
Destination
192.168.10.130:3389
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Help
Open
Cancel

> SSH туннели


PuTTY Configuration
Category:
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
L56389 192.168.10.130:3389
Add new forwarded port:
Source port
Add
Destination
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Help
Open
Cancel

> SSH туннели


Подключение к удаленному рабочему столу
Подключение к удаленному
рабочему столу
Компьютер:
127.0.0.1:56389
Пользователь:
example\user
При подключении необходимо будет указать учетные данные.
Показать параметры
Подключить
Справка

> SSH туннели

Переброс локального порта на удаленную машину через ssh в *nix:

ssh -L локальный_порт:удаленный_адрес:удаленный_порт логин@IP_роутера

ssh -L 56389:192.168.56.1:3389 user@example.org

> SSH туннели

Для чего еще это может быть полезно?

Параноидальный доступ к другим службам MikroTik (Winbox, FTP, WWW)

> SSH туннели

Задача:

- **Получить доступ к сайтам, которые кто-то заблокировал ;)**
- **Использовать удаленный MikroTik в качестве http\https прокси;**
- **Без настройки Web Proxy;**
- **Без настройки на SOCKS proxy;**
- **Безопасно.**

> SSH туннели

Решение:

- **В OpenSSH встроен функционал SOCKS проксирования и MikroTik поддерживает его;**
- **Можно настроить SSH туннель таким образом, чтобы удаленный роутер был SOCKS proxy сервером;**
- **Все данные передаются внутри SSH в защифрованном виде;**
- **В логах WEB сервера будет записан адрес "роутера-прокси".**

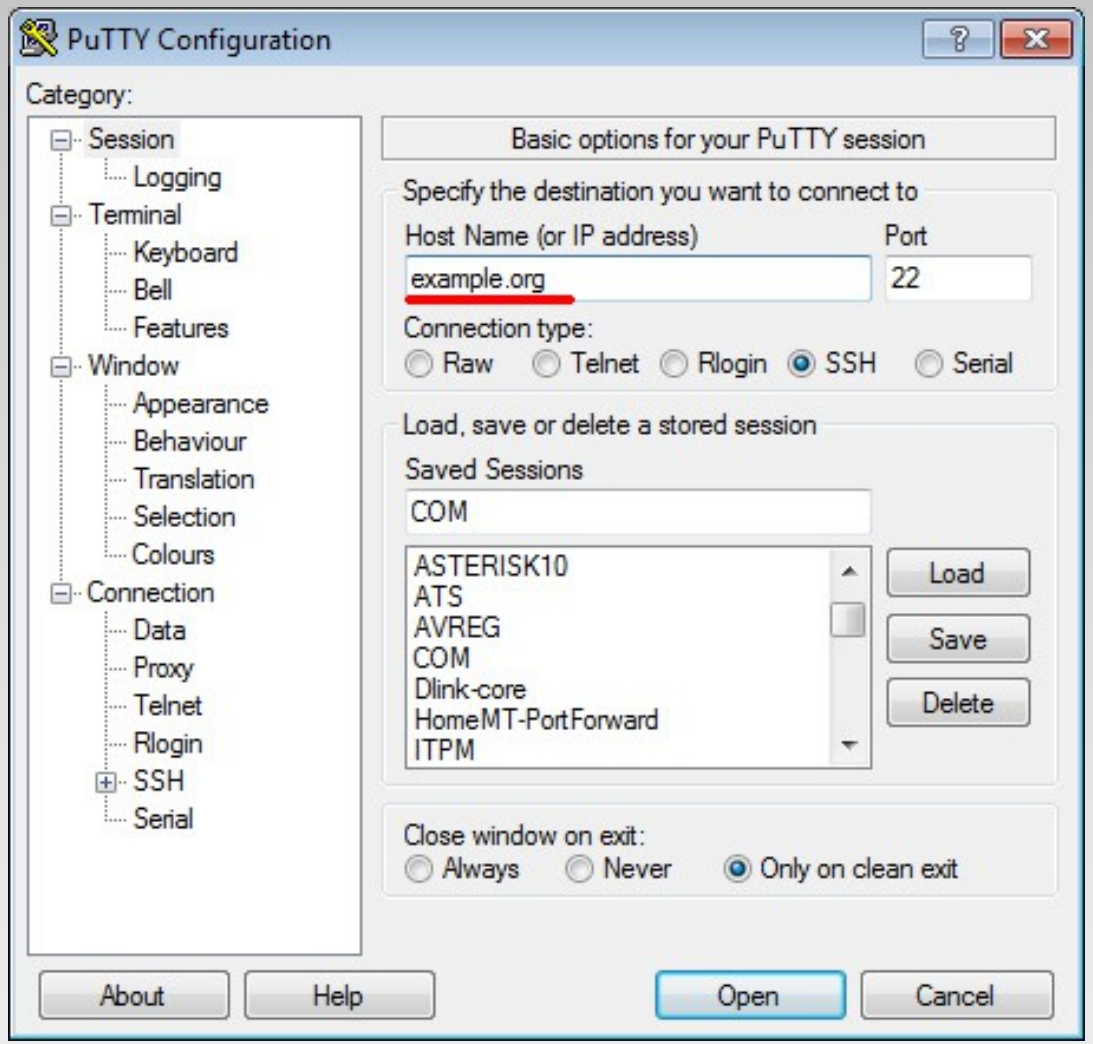
> SSH туннели

Что такое SOCKS?

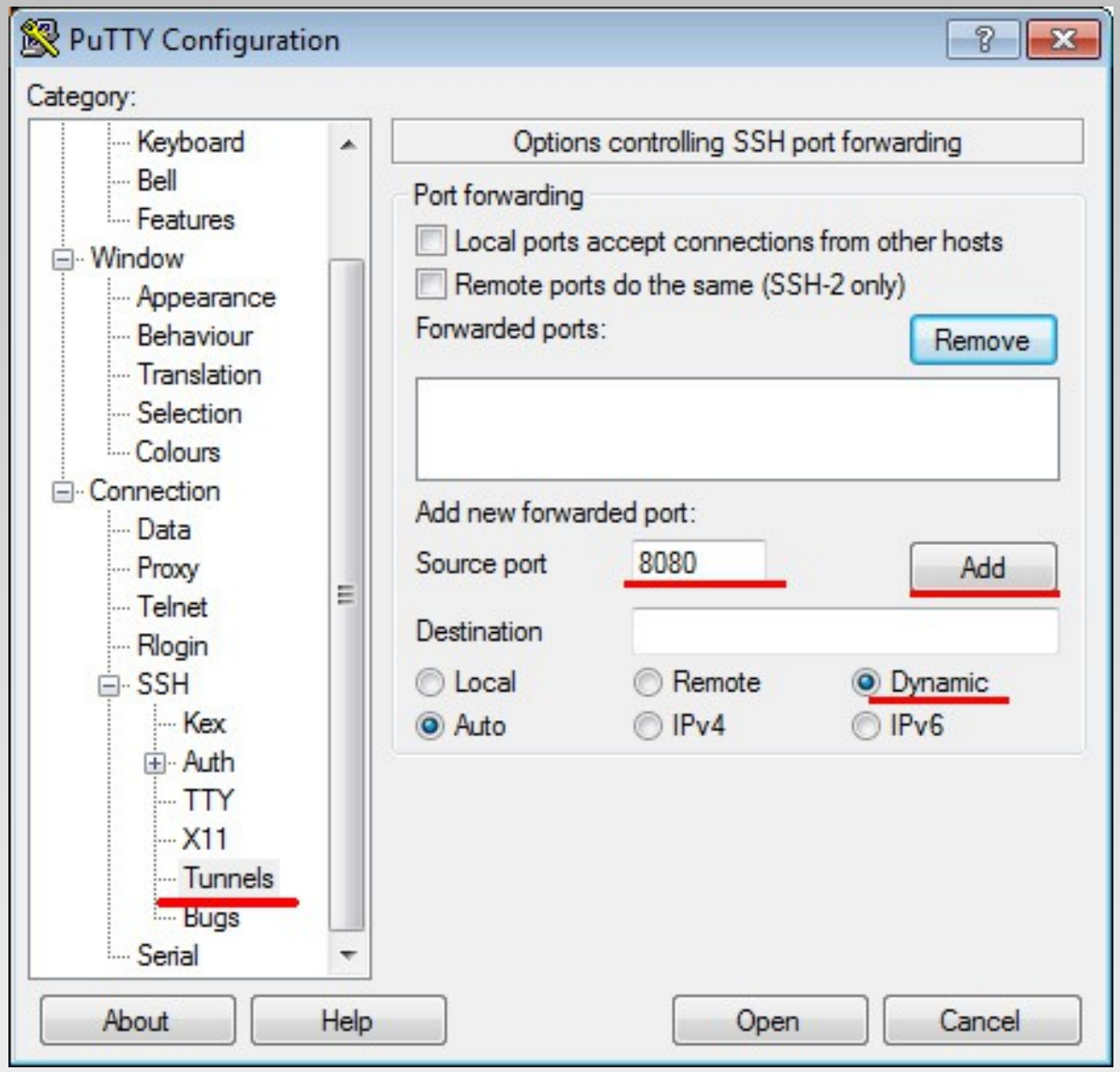
- **SOCKS (SOCKet Secure). Сетевой протокол, изначально использовавшийся для преодоления firewall;**
- **Позволяет пропускать внутри себя почти любые протоколы (HTTP, HTTPS, FTP, SMTP, POP3, IRC, etc);**
- **В отличие от HTTP proxy не добавляет никаких данных\заголовков в пакеты.**
- **Работает по TCP, но позволяет внутри себя передавать TCP и UDP (SOCKS 5)**

> SSH туннели

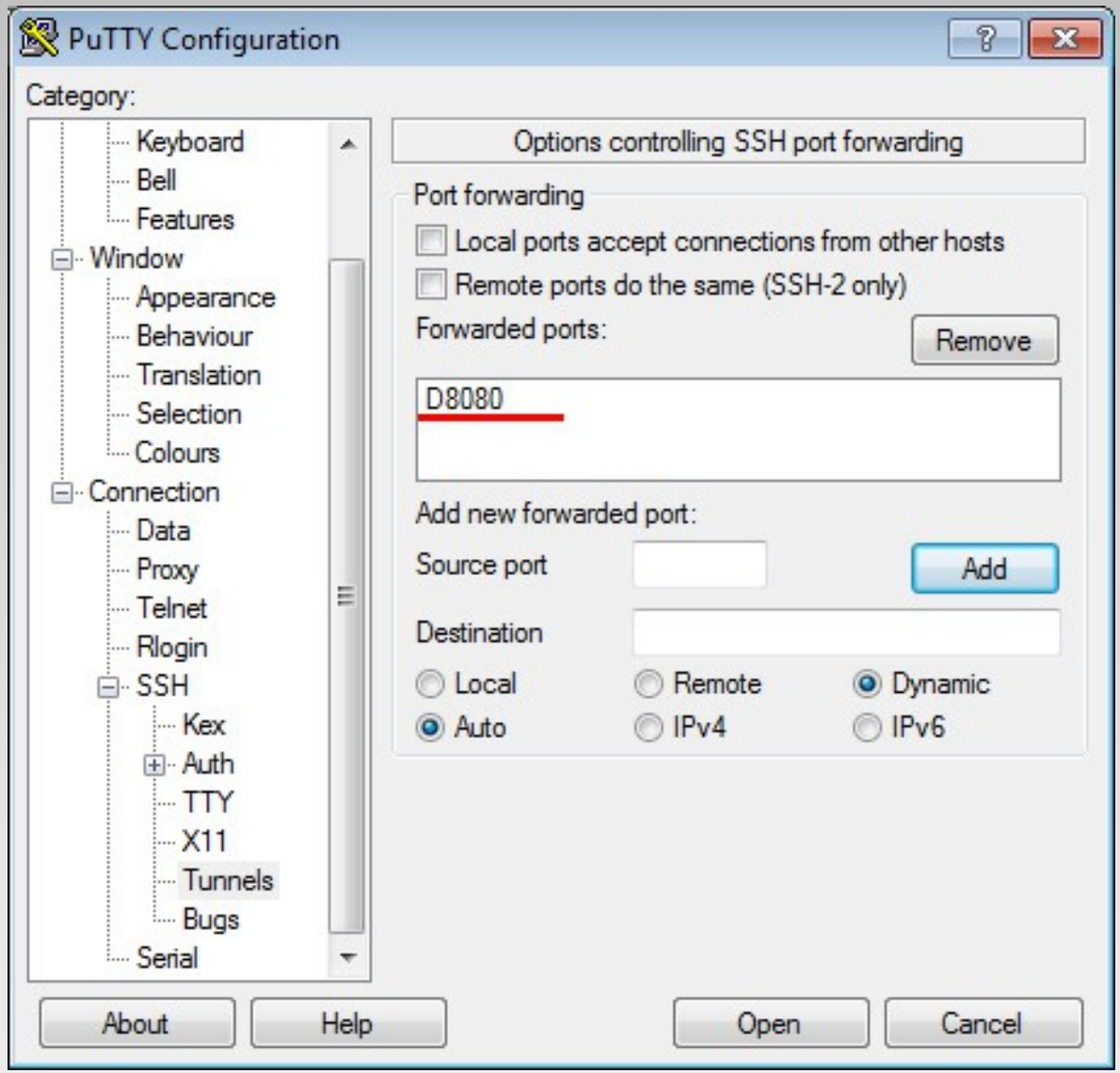
Под Windows настроить можно через PuTTY.



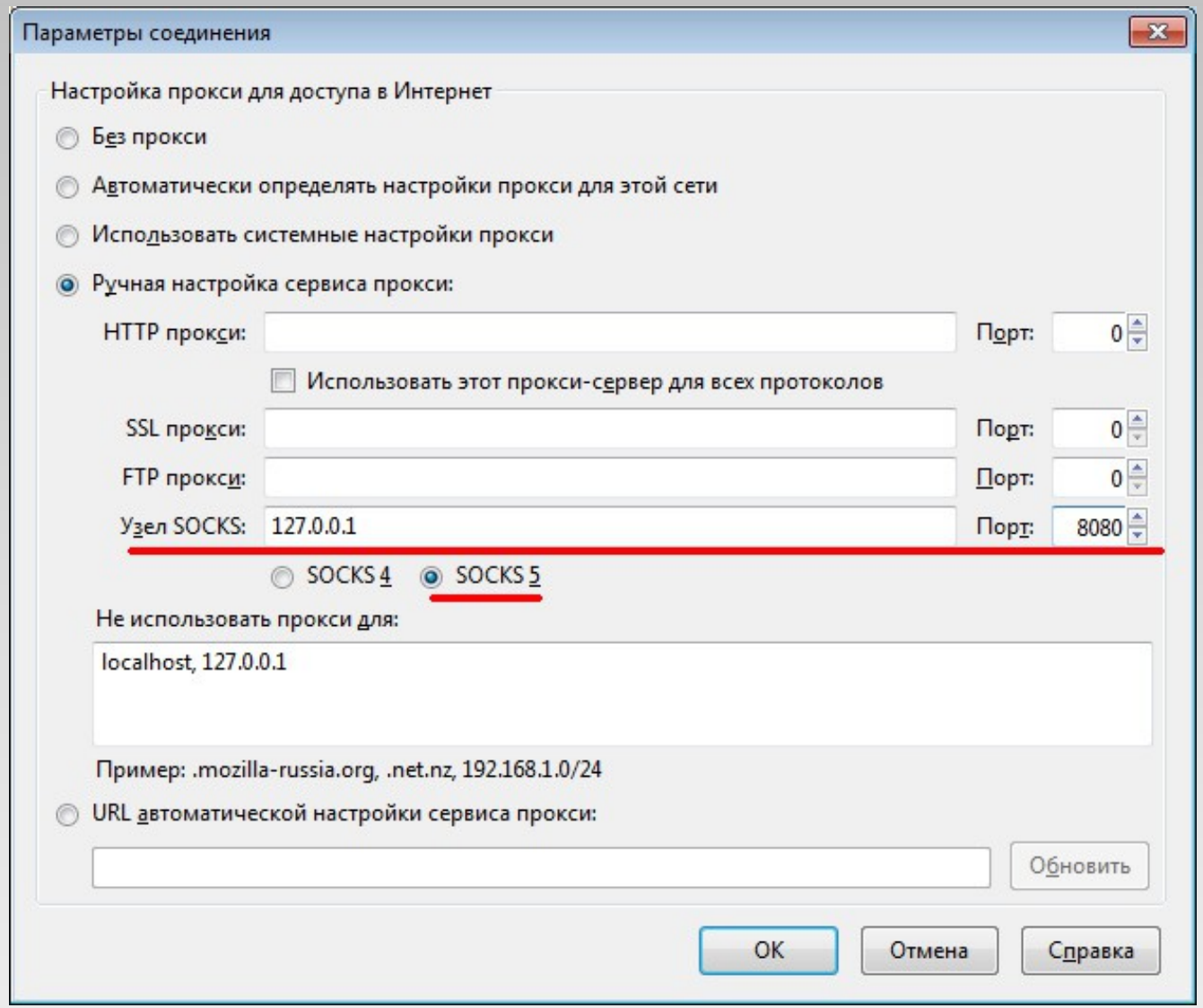
> SSH туннели


PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Serial
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
Add new forwarded port:
Source port
8080
Add
Destination
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Help
Open
Cancel

> SSH туннели


PuTTY Configuration
Category:
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Tunnels
Bugs
Serial
Options controlling SSH port forwarding
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH-2 only)
Forwarded ports:
Remove
D8080
Add new forwarded port:
Source port
Add
Destination
Local
Remote
Dynamic
Auto
IPv4
IPv6
About
Help
Open
Cancel

> SSH туннели


Параметры соединения
Настройка прокси для доступа в Интернет
Без прокси
Автоматически определять настройки прокси для этой сети
Использовать системные настройки прокси
Ручная настройка сервиса прокси:
HTTP прокси:
Порт:
0
Использовать этот прокси-сервер для всех протоколов
SSL прокси:
Порт:
0
FTP прокси:
Порт:
0
Узел SOCKS:
127.0.0.1
Порт:
8080
SOCKS 4
SOCKS 5
Не использовать прокси для:
localhost, 127.0.0.1
Пример: .mozilla-russia.org, .net.nz, 192.168.1.0/24
URL автоматической настройки сервиса прокси:
Обновить
OK
Отмена
Справка

> SSH туннели

SOCKS проксирование через ssh в *nix:

ssh -D локальный_порт логин@IP_роутера

ssh -D 8080 user@example.org

> SSH туннели

Через SOCKS можно проксировать практически любое TCP или UDP приложение, используя "соксификатор".

Например:
SocksCap
widecap
Proxyfier
socksify

А еще можно делать цепочки SOCKS серверов)

> SSH туннели

Для чего еще это может быть полезно?

- **Получение доступа к оборудованию в удаленной подсети, если на нем не настроена маршрутизация\шлюз по умолчанию.**
- **Безопасная работа в Интернет из гостиницы, ресторана и подобной публичной сети, где возможна атака man in the middle.**

> Вопросы?

vs@foto-glaz.ru