


# Road-warrior VPN

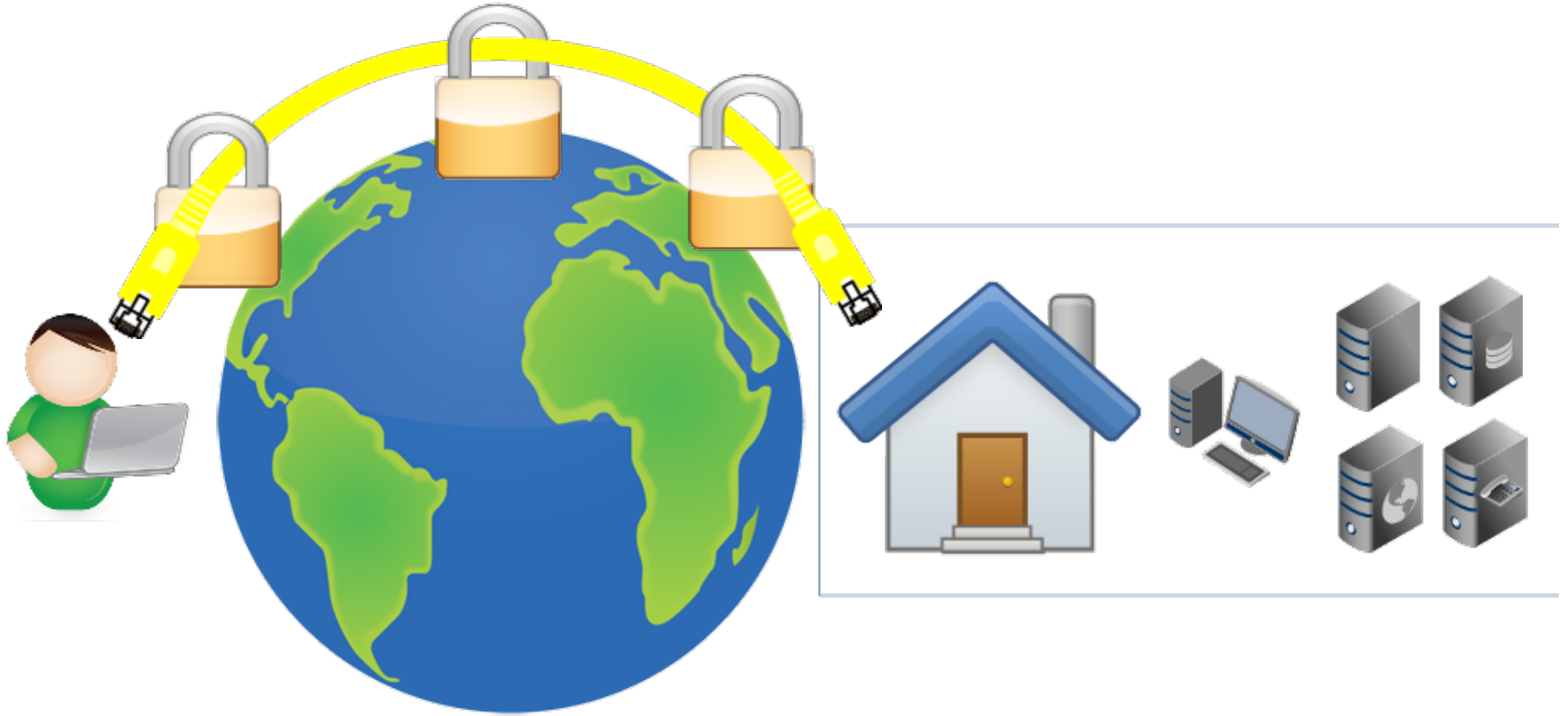
Анализ проблемы и обзор доступных в RouterOS решений

# Who am I ?

## Андрей Сыровенко

- Программист (C/C++, Python, Perl, JS, etc.)
  - IT Manager (умею руководить сисадминами)
  - Консультант
-  Фанат FreeBSD, который полагает, что RouterOS - то небольшое, что оправдывает существование Linux.
- E-mail / Hangouts: [andriys@gmail.com](mailto:andriys@gmail.com)
  - Skype: andriy\_syrovenko

# Road Warrior



# Road-warrior VPN: требования

- Надежность / защищенность
- Сценарии маршрутизации
  - Tunnel All
  - Split-Tunnel
- Split-DNS

# Road-warrior VPN: требования

- Server-dictated configuration
- Транспортные протоколы
  - Качество работы в условиях ненадежного Интернет-соединения
  - Firewall - friendliness
  - NAT - friendliness
- RADIUS

# Road-warrior VPN: Security

- Конфиденциальность
  - Шифрование трафика внутри VPN-туннеля
  - Затрудняет пассивное прослушивание / перехват трафика
- Аутентификация клиента
  - Контроль доступа
- Аутентификация сервера
  - Защита от MITM-атак

# Client Authentication

- Password-based
  - Простота в использовании и сопровождении
  - Достаточная надежность
  - Можно использовать Two-factor / two-phase для большей надежности
- Certificate-based
  - Считается более защищенной
  - Требуется создание и поддержка PKI (Public Key Infrastructure)

# Server Authentication

MITM (Man-in-the-middle)





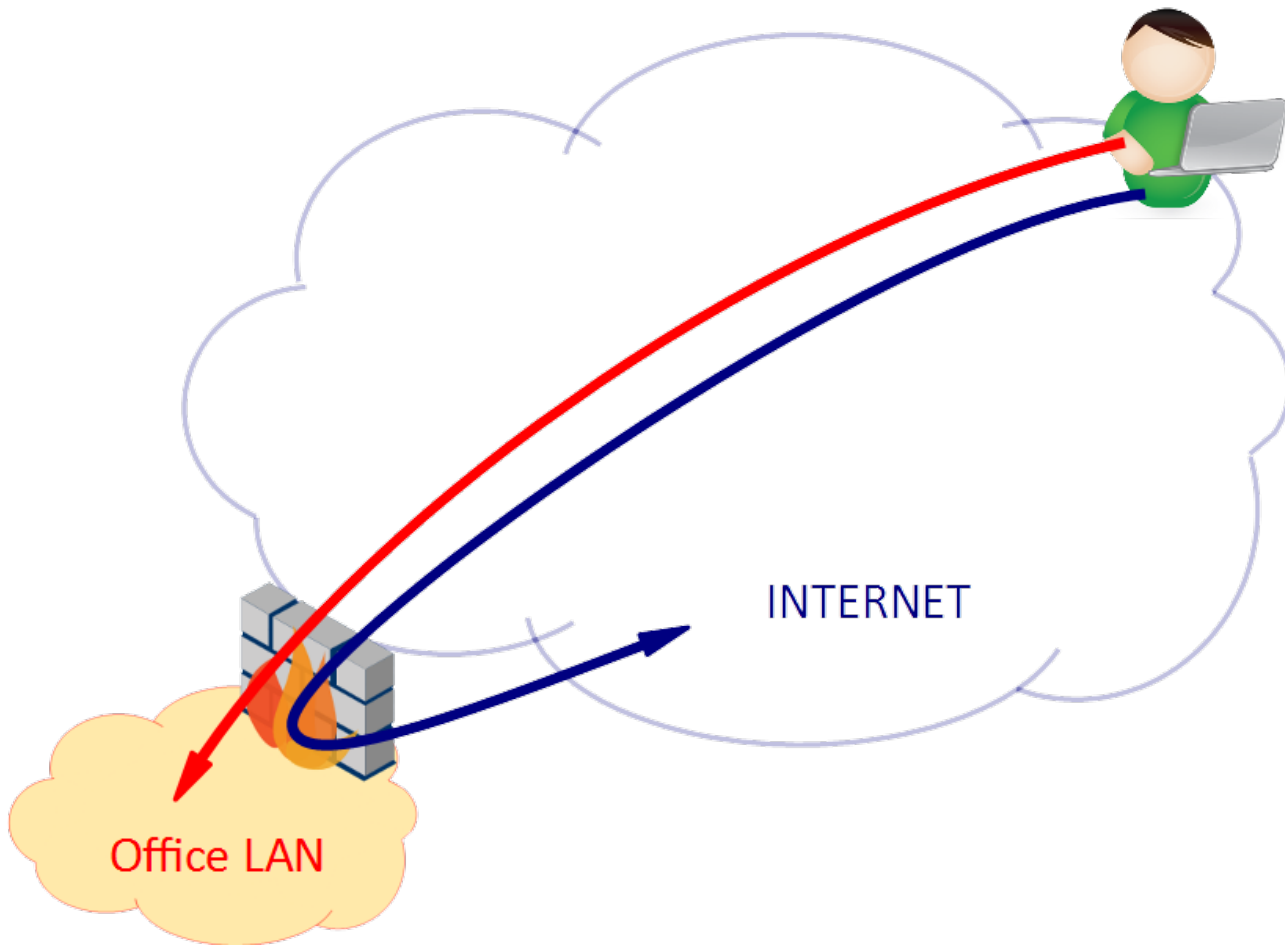
# Server Authentication

- Защита от MITM-атак
- Shared-secret based
  - Секрет, который не совсем секрет
  - Хорошо работает только для небольшого количества пользователей
- Certificate-based
  - Одинаково хорошо работает при любом количестве пользователей
  - Можно обойтись без собственной PKI

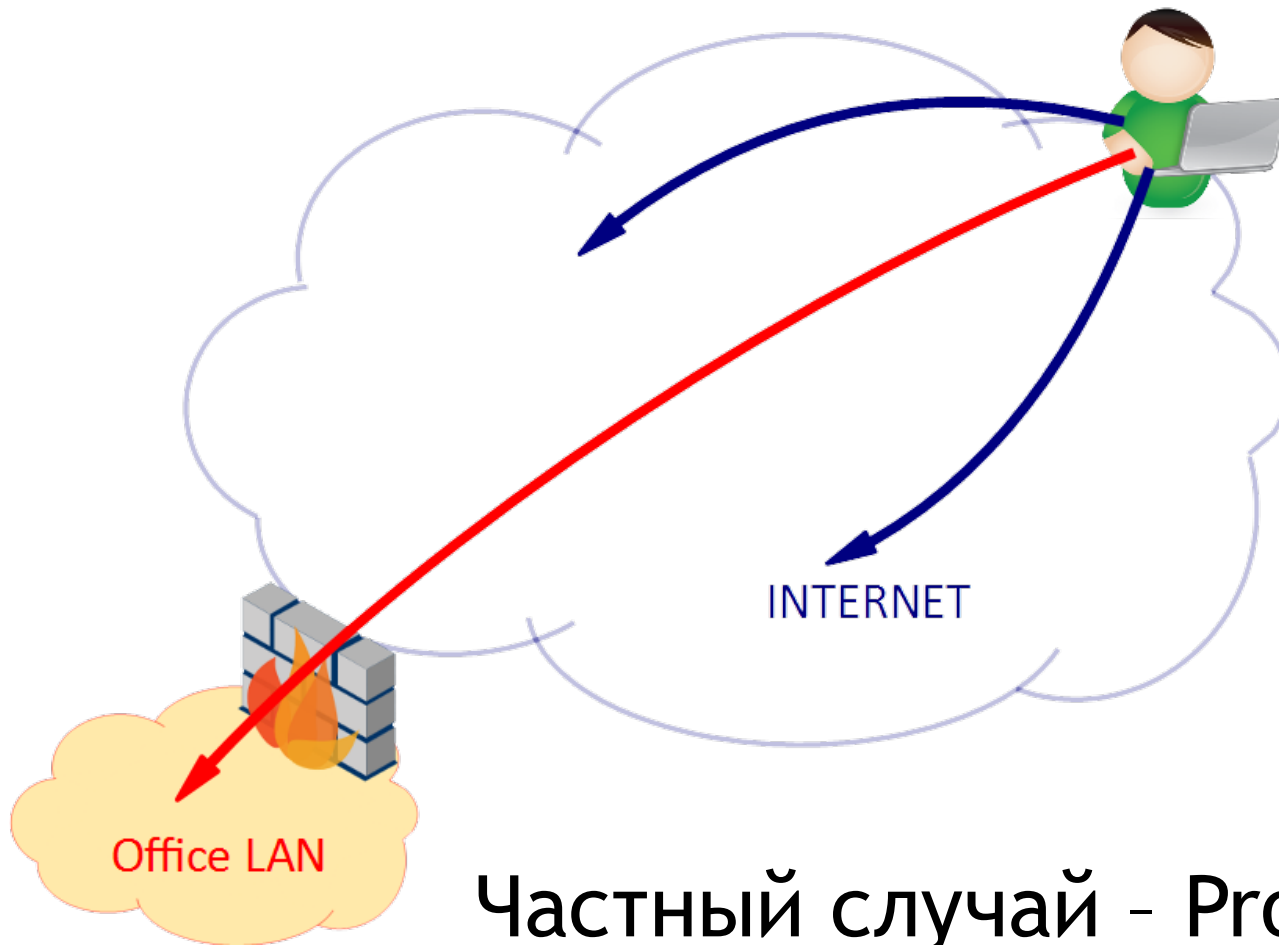
# Road-warrior VPN: требования

- Надежность / защищенность
- Сценарии маршрутизации
  - Tunnel All
  - Split-Tunnel
- Split-DNS

# Tunnel All



# Split-Tunnel



Частный случай - Proxy  
ARP

# Road-warrior VPN: требования

- Server-dictated configuration
- Транспортные протоколы
  - Качество работы в условиях ненадежного Интернет-соединения
  - Firewall - friendliness
  - NAT - friendliness
- RADIUS

# Server-Dictated Configuration

- Минимально необходимо:
  - Server-allocated client IP address
- Было бы не плохо:
  - Адреса DNS и WINS серверов
  - Domain name
  - Список туннелируемых сетей (Split-Tunnel)

# Транспортные протоколы

- TCP
  - NAT - friendly
  - Firewall - friendly
    - Особенно при использовании порта 443/tcp
  - Практически бесполезен в условиях плохого Интернет-соединения:
    - TCP-over-TCP “meltdown” problem
    - VoIP - задержки и высокий джиттер

# Транспортные протоколы

- UDP
  - Как правило NAT - friendly
    - Исключение - IPsec NAT-T в RouterOS
  - Иногда блокируется в сетях гостиниц и гостевых сетях предприятий
  - Хорошо работает в том числе и на плохих Интернет-соединениях



# Транспортные протоколы

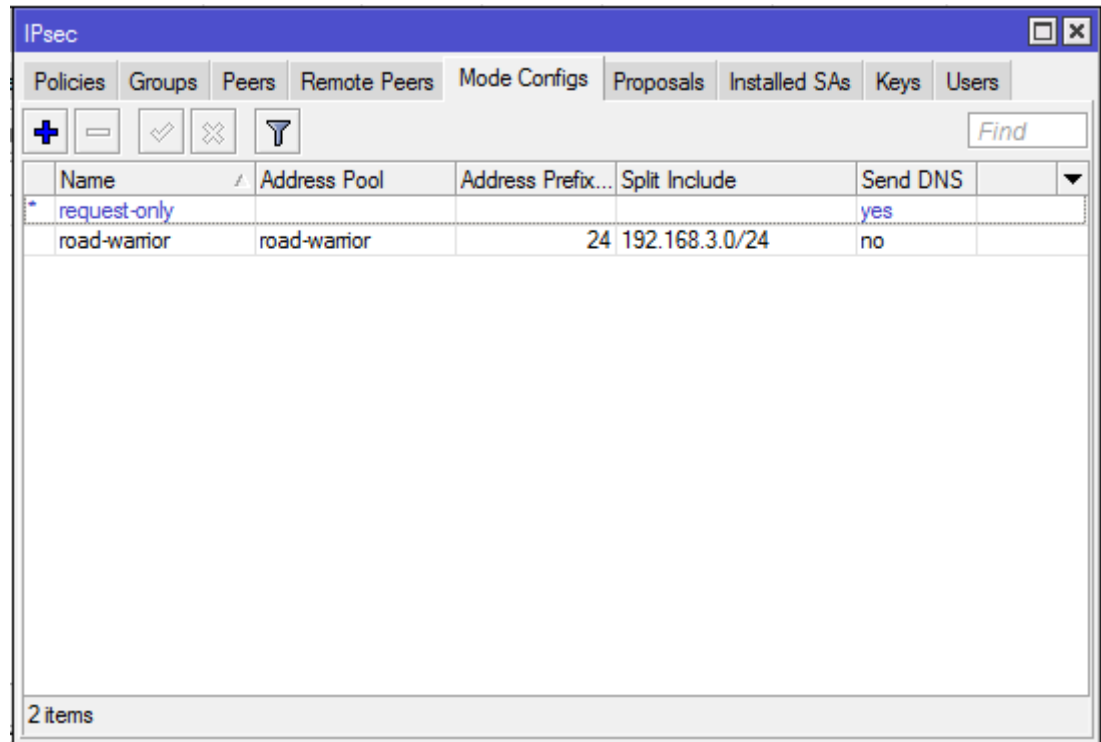
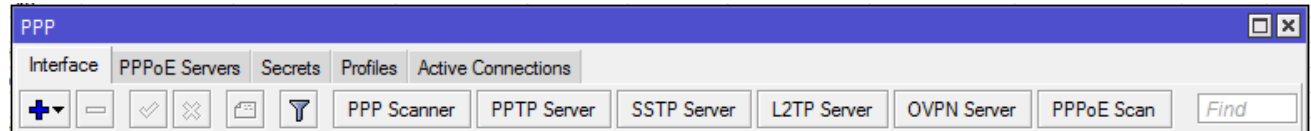
- ESP
  - Плохо сочетается с NAT
  - Иногда блокируется в сетях гостиниц и гостевых сетях предприятий
  - Хорошо работает в том числе и на плохих Интернет-соединениях

# Поддержка RADIUS

- Единая БД пользователей для нескольких устройств доступа
- Интеграция с существующими системами
  - ActiveDirectory, LDAP
- Дополнительная функциональность
  - Two-factor / two-phase authentication
  - Password expiration
  - Self-care

# RouterOS

- PPP
  - PPTP
  - L2TP
  - L2TP/IPsec
  - SSTP
- OpenVPN
- IPsec (IKEv1)



# PPTR, L2TP (без IPsec)

- Взламываются методом пассивного прослушивания
- <https://www.cloudcracker.com/>
  - \$200
  - 24 часа

# L2TP/IPsec

- Поддержка в клиентских ОС
  - Windows - встроенный клиент ✓
  - Mac OS X - встроенный клиент ✓
  - Android - встроенный клиент ✓
  - iOS - встроенный клиент ✓
- L2TP/IPsec PSK использует Shared Secret ✗
- L2TP/IPsec RSA как правило подразумевает IKEv2 (не поддерживается в RouterOS) ✗

# L2TP / IPsec

	Протокол	RouterOS	Клиент
Password-base Client Authentication	✓	✓	✓
Certificate-base Client Authentication	✗	✗	✗
RADIUS		✓	
Tunnel All	✓	✓	✓
Split-Tunnel	✓	✗	✓
Split-Tunnel (Proxy ARP)	✓	✓	✓
Сервер сообщает адреса DNS/WINS	✓	✓	✓
Сервер сообщает список Split-Tunnel сетей	✗	✗	✗
TCP	✓	✓	✓
UDP	✓	✓	✓
ESP			

# SSTP

- Поддержка в клиентских ОС
  - Windows - встроенный клиент ✓
  - Mac OS X - не поддерживается ✗
  - Android - не поддерживается ✗
  - iOS - не поддерживается ✗
- Certificate-based Server Authentication ✓

# SSTP

	Протокол	RouterOS	Клиент
Password-base Client Authentication	✓	✓	✓
Certificate-base Client Authentication	✗	✗	✗
RADIUS		✓	
Tunnel All	✓	✓	✓
Split-Tunnel	✓	✗	✓
Split-Tunnel (Proxy ARP)	✓	✓	✓
Сервер сообщает адреса DNS/WINS	✓	✓	✓
Сервер сообщает список Split-Tunnel сетей	✓	✗	✓
TCP	✗	✗	✗
UDP			



# OpenVPN

- Клиентское ПО
  - Windows - доступно бесплатно ✓
  - Mac OS X - доступно бесплатно ✓
  - Android - доступно в Play Market бесплатно ✓
  - iOS - доступно в App Store бесплатно ✓
- Certificate-based Server Authentication ✓

# OpenVPN

	Протокол	RouterOS	Клиент
Password-base Client Authentication	✓	✓	✓
Certificate-base Client Authentication	✓	✓	✓
RADIUS		✓	
Tunnel All	✓	✓	✓
Split-Tunnel	✓	✓	✓
Split-Tunnel (Proxy ARP)	✓	✓	✓
Сервер сообщает адреса DNS/WINS	✓	✗	✓
Сервер сообщает список Split-Tunnel сетей	✓	✗	✓
TCP	✓	✗	✓
UDP			

# IPsec

- Количество возможных вариантов конфигурации невероятно велико
- Далее рассмотрим такие варианты:
  - IPsec PSK
  - IPsec PSK + XAuth
  - IPsec RSA
  - IPsec RSA + XAuth
  - IPsec RSA Hybrid

# IPsec

- Клиентское ПО

- Windows - доступно бесплатно

- (Shrew Soft VPN Client)

- Mac OS X - встроенный клиент

- Также существует неофициальная сборка

- Shrew Soft VPN Client

- Android - встроенный клиент




- iOS - встроенный клиент

# IPsec

	Протокол	RouterOS	Клиент
RADIUS		✗	
Tunnel All	✓	✓	✓
Split-Tunnel	✓	✓	✓
Split-Tunnel (Proxy ARP)	✗	✗	✗
Сервер сообщает адреса DNS/WINS	✓	✓	✓
Сервер сообщает список Split-Tunnel сетей	✗	✗	✗
TCP	✓	✓✗*	✓
UDP	✓	✓	✓
ESP			

\* Нет полноценной поддержки NAT-T

# IPsec

- IPsec RSA + XAuth
  - Не поддерживается RouterOS 
- IPsec PSK
  - Не поддерживает аутентификацию клиента 
  - PSK == Pre-Shared Secret 

# IPsec PSK + XAuth







- Поддержка клиентским ПО
  - Shrew Soft VPN Client ✓
  - Mac OS X IPsec Client ✓
  - Android IPsec Client ✓
  - iOS IPsec Client ✓
- PSK == Pre-Shared Secret ✘

# IPsec RSA

- Поддержка клиентским ПО
  - Shrew Soft VPN Client ✓
  - Mac OS X IPsec Client ✓
  - Android IPsec Client ✓
  - iOS IPsec Client ✓
- Certificate-base Client Authentication
  - Требуется создание PKI



# IPsec RSA Hybrid

- Поддержка клиентским ПО
  - Shrew Soft VPN Client 
  - Mac OS X IPsec Client 
  - Android IPsec Client 
  - iOS IPsec Client 
- Certificate-base Server Authentication 
- Password-based Client Authentication 

**Примеры из личного опыта**

# Пожелания к Mikrotik

- Хотелось бы увидеть в будущих версиях RouterOS:
  - Полноценную поддержку IPsec NAT-T
  - Поддержку RADIUS в IPsec
  - Поддержку UDP-транспорта в OpenVPN
  - ...

# Вопросы и комментарии

**Благодарю за внимание!**