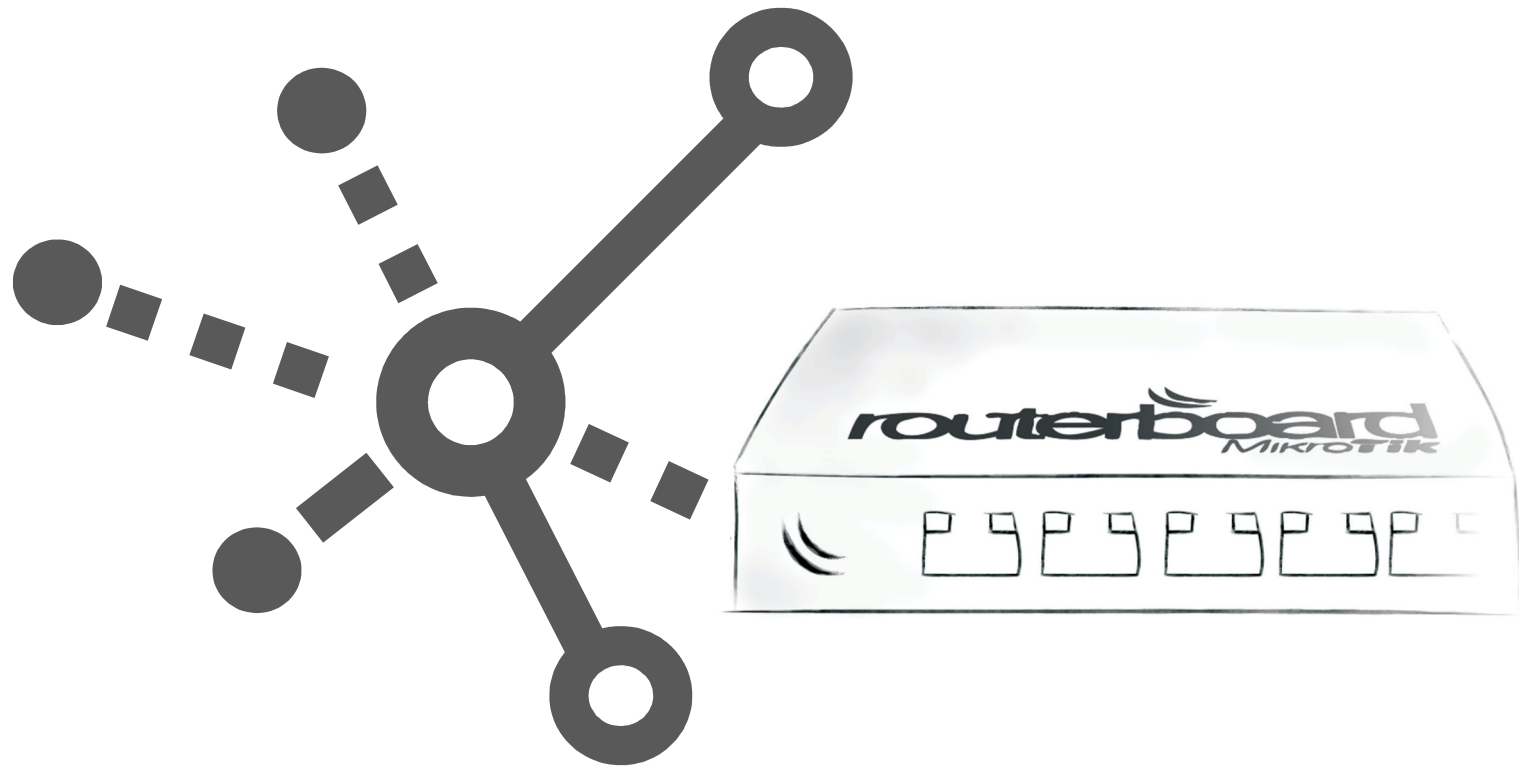


MUM Europe, Ljubljana 2016.03.25

Andis Arins / router.lv



How to choose the right VPN?

Presenter – Andis Arins



2

- MikroTik Consultant at www.router.lv
- MikroTik / Microsoft certified trainer
- Member of the board in Latvian Internet Association
- Review expert EU EC in future networking research

[andis\[at\]router.lv](mailto:andis[at]router.lv)

www.linkedin.com/in/andisarins

Focus of presentation



3

Virtual Private Networking aspects in perspective
of Security / Performance / Flexibility

Why you want one ?

What RouterOS can offer?

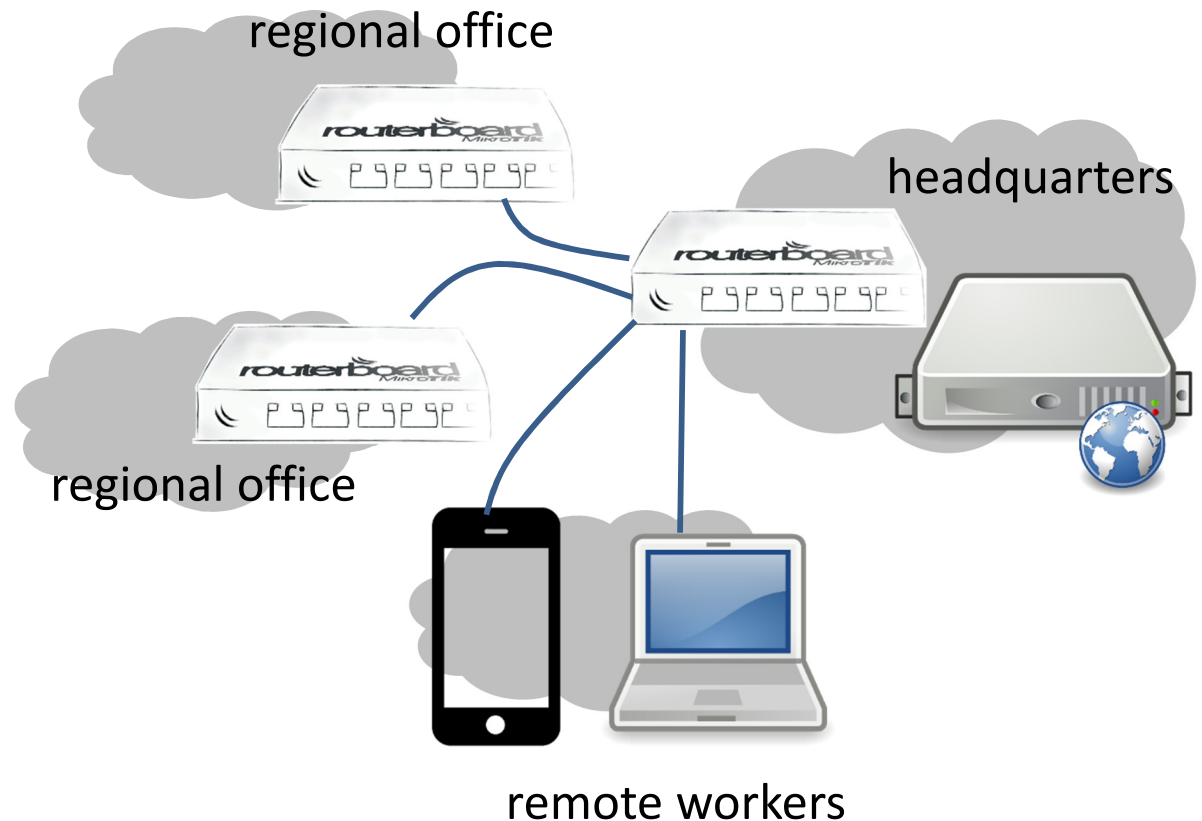
How to pick the best one for you ?

VPN user profiles



4

- road warriors
- corporate connections
- James Bonds

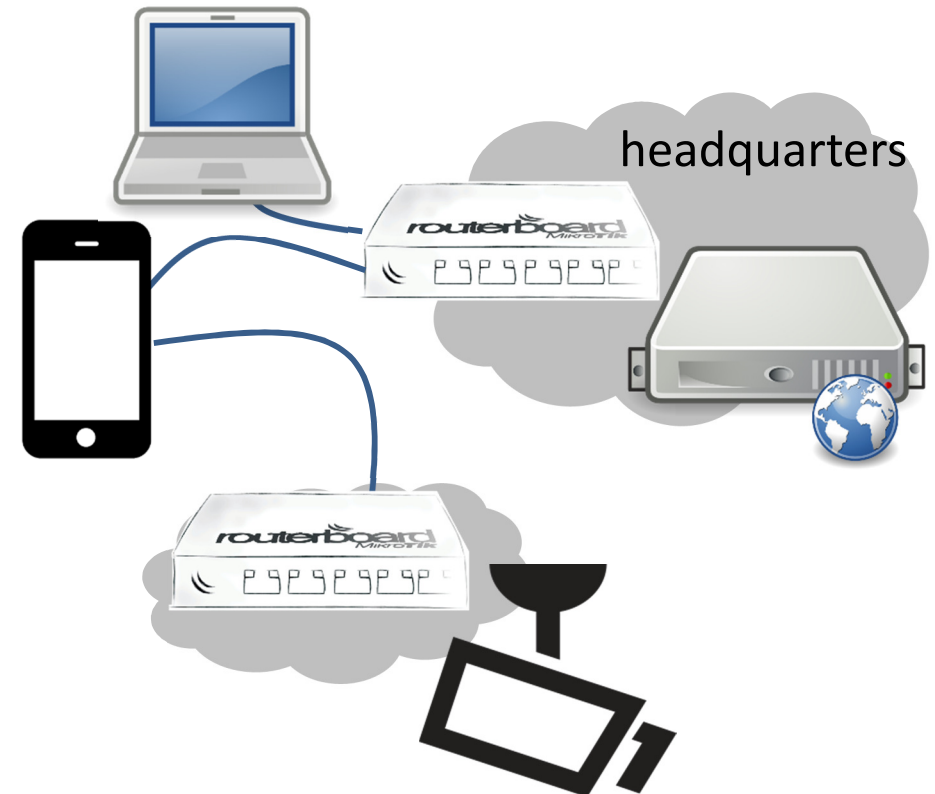


road warriors



5

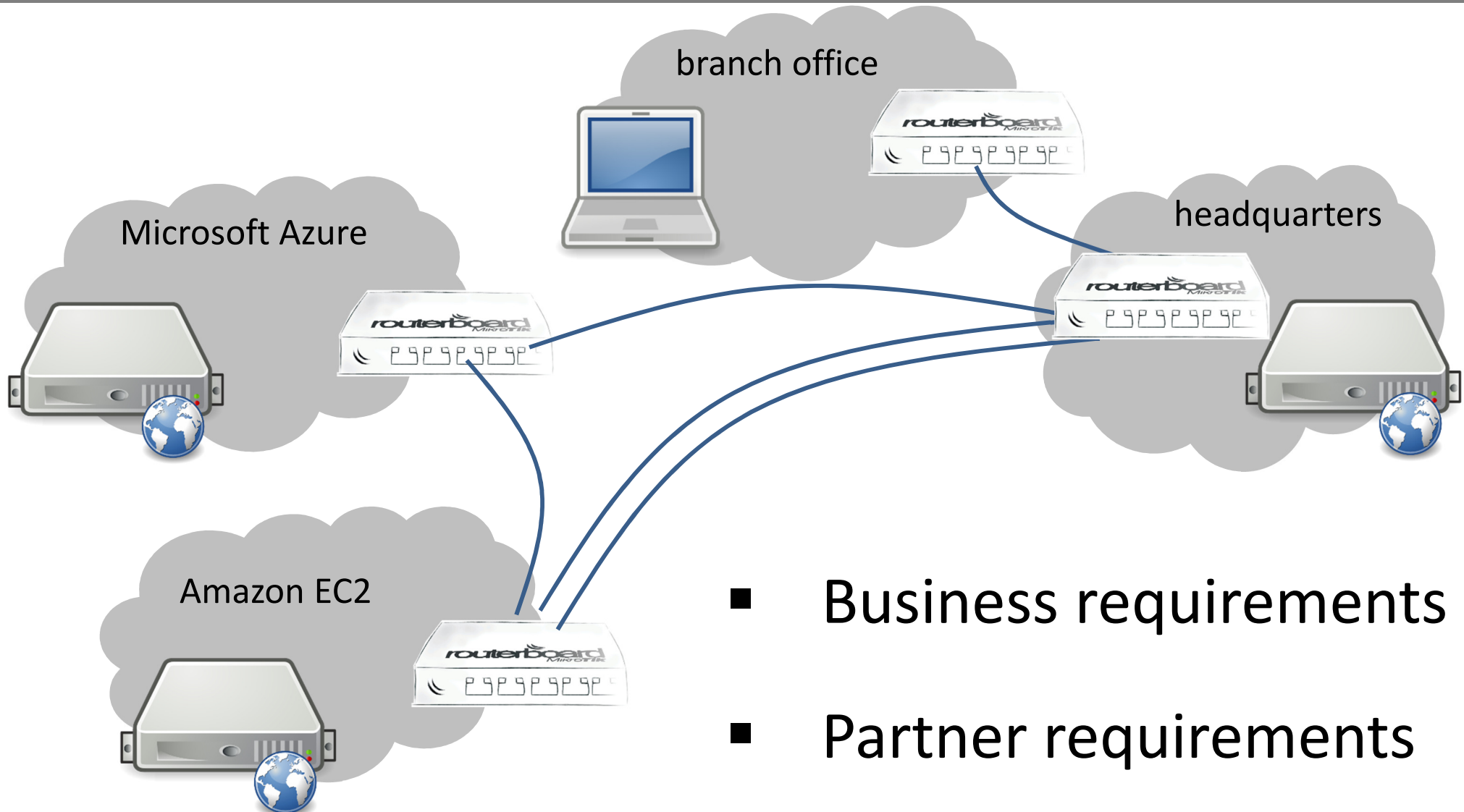
- working from anywhere
- unpredictable network conditions



Corporate connections



6

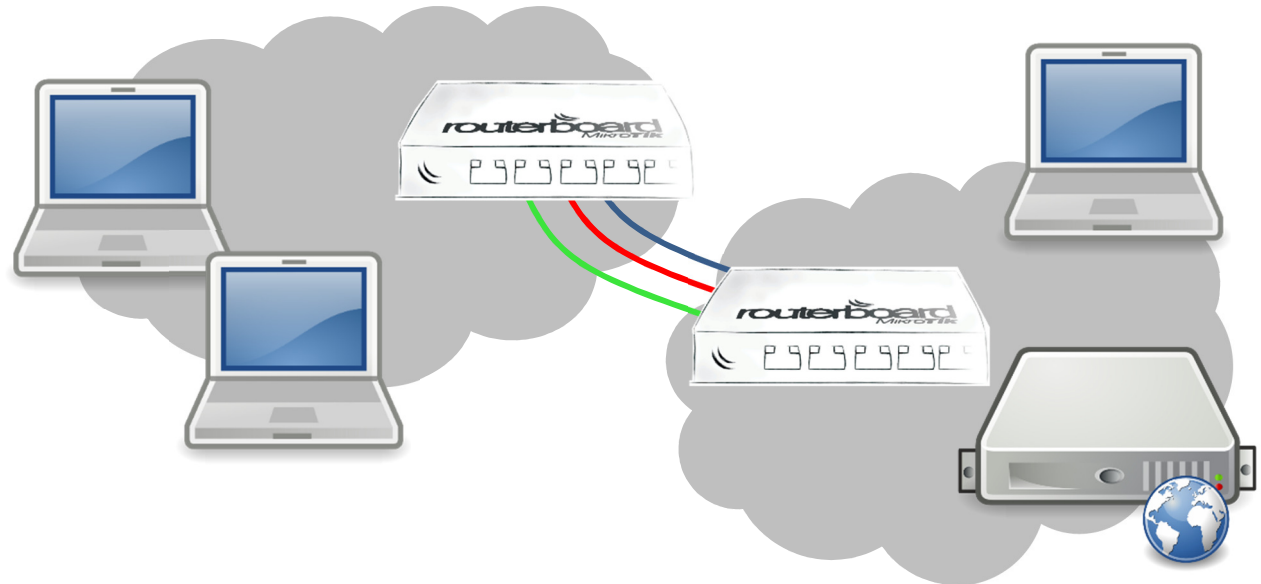


- Business requirements
- Partner requirements

Corporate connections



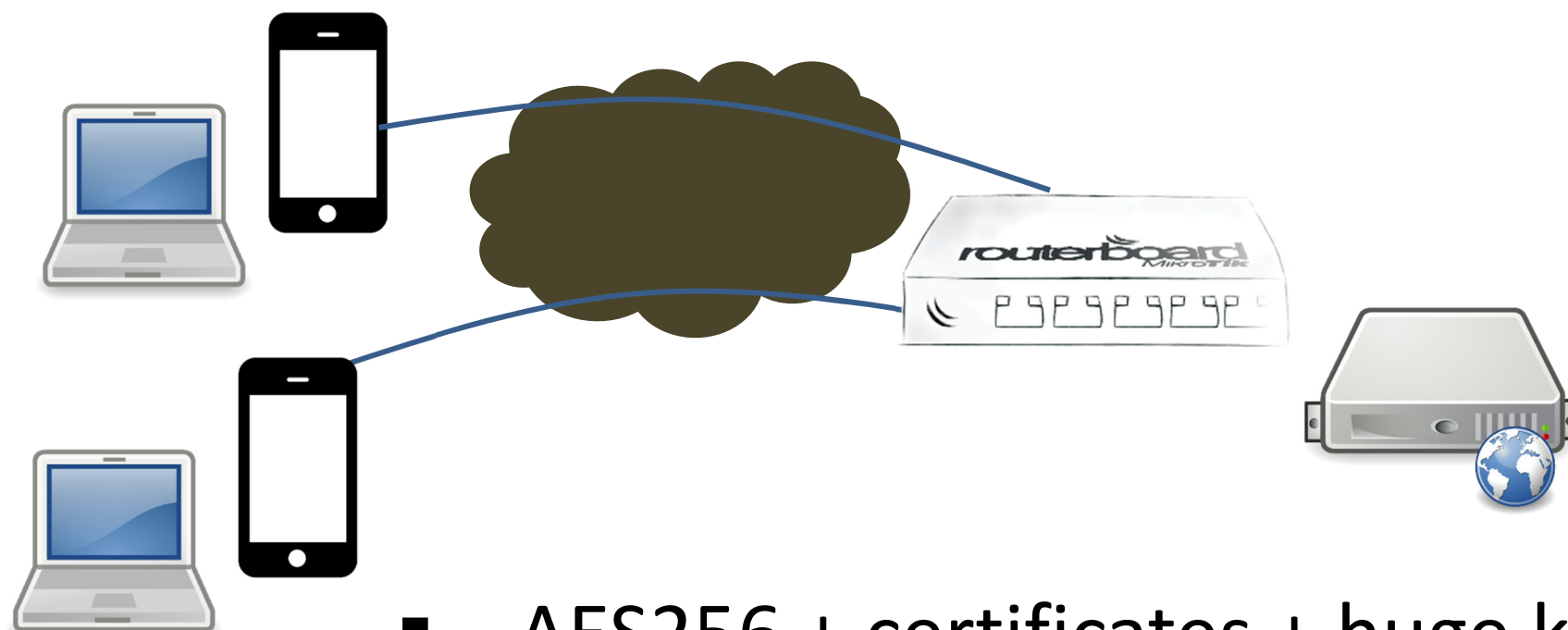
7



Serious encryption



8



- AES256 + certificates + huge keys stored in safe hardware
- VPN over VPN



- Authentication
- Access control
- Confidentiality
- Data integrity

RouterOS VPN portfolio



10

PPPoE - Point-to-Point Protocol over Ethernet

PPTP – Point to Point Tunneling Protocol

L2TP - Layer 2 Tunneling Protocol

SSTP – Secure Socket Tunneling Protocol

OVPN – Open Source VPN

IPSEC - Internet Protocol Security

EoIP – Ethernet over IP

Does encryption still work?



11

Core cryptography elements:

- Algorithm
- Key (size)



Security is Only as Strong as the Weakest Link



- **DES** (Data Encryption Standard) was once the standard crypto algorithm for encryption
- **MD5** has recently been found less secure than previously thought
- **RC4** (Rivest Cipher 4) - recent attacks :Royal Holloway, KU Leuven

AES (Advanced Encryption Standard) is the current preferred symmetric algorithm

IPSEC / SSTP between RouterOS / OVPN



Symmetric:

Key sizes of 128 bits (standard for SSL) are sufficient for most applications
Consider 256 bits for secure systems such as large financial transactions

Symmetric-key encryption protocols should include message authentication

Asymmetric:

2048 bits should be considered for highly protected applications.
2048 / 4096 ?

Don't use excessive key sizes unless you know you need them.

Point-to-Point Tunneling Protocol



14

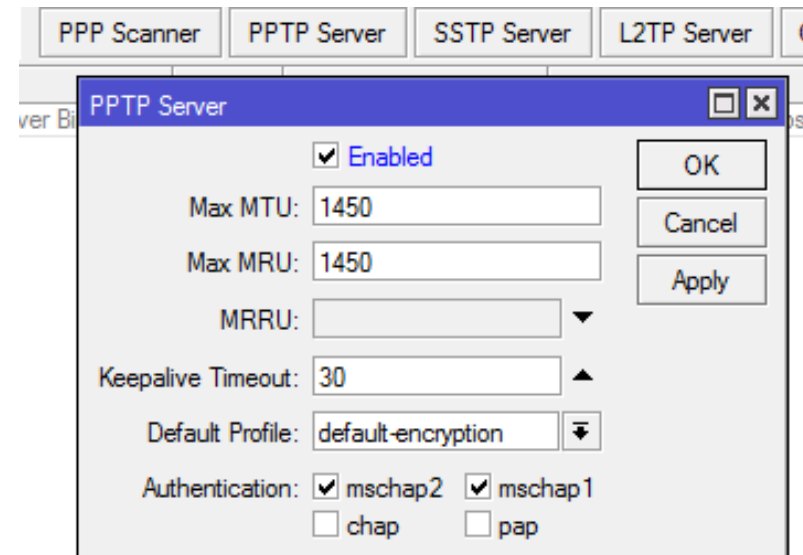
PPTP is available since the mid 1990s
requires /47 GRE and /6 TCP:1723

+ Pros

- client software on all platforms
- very easy to set up
- fast
- NAT friendly

- Cons

- not at all secure
- easy to block on firewalls



PPTP vulnerability



15

MPPE-128 encryption (which uses RC4 encryption with a 128bit key)

MITM attack to capture the handshake and any PPTP traffic after that
offline crack of the handshake and derive the RC4 key

no forward secrecy - cracking one PPTP session is sufficient to crack all
previous PPTP sessions using the same credentials.

<https://github.com/moxie0/chapcrack>

IP security (IPSec)



16

IPSec is set of encryption mechanisms,
two modes: transport/ tunnel
requires IKE /17 udp:500, ESP /50

+ Pros

- considered very secure
- works together with other tunnels
- faster than OVPN/SSTP
- hardware support

- Cons

- struggle with restrictive firewalls
- problems with NAT
- complicated setup

New IPsec Peer

Address: 0.0.0.0/0

Port: 500

Local Address:

Auth. Method: pre shared key

☐ Passive

Secret:

Policy Template Group: default

Exchange Mode: main

☒ Send Initial Contact

☐ NAT Traversal

My ID: auto :

Proposal Check: obey

Hash Algorithm: sha1

Encryption Algorithm: ☐ des ☒ 3des ☒ aes-128

☐ aes-192 ☐ aes-256 ☐ blowfish

☐ camellia-128 ☐ camellia-192 ☐ camellia-256

Mode Configuration:

DH Group: modp1024

Generate Policy: no

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: 120 s

DPD Maximum Failures: 5

L2TP/IPSec



17

The L2TP and IPsec protocols combine their best individual features to create a highly secure VPN client
requires IKE udp:500, ESP /50, udp:1701

+ Pros

- Clients in most modern OS
- faster than OVPN/SSTP
- Hardware support

- Cons

- struggle with restrictive firewalls
- larger overhead
- may be compromised by governments (unproven)

OpenVPN



18

fairly new open source technology that uses the OpenSSL
requires tcp:1194 (can be changed)

+ Pros

- Optional clients in most OS (OpenVPN Connect)
- Can bypass firewalls
- Open source
- NAT friendly

- Cons

- Needs third party software
- Certificates required

A screenshot of the 'OpenVPN Server' configuration window. The window has a title bar with 'OpenVPN Server' and standard window controls. The main area contains various configuration fields and checkboxes. At the top, there is a checkbox labeled 'Enabled' which is checked. Below it are fields for 'Port' (1194), 'Mode' (ip), 'Netmask' (24), 'MAC Address' (FE:52:A3:33:B2:22), 'Max MTU' (1500), 'Keepalive Timeout' (60), and 'Default Profile' (default). There are 'OK', 'Cancel', and 'Apply' buttons on the right. Below these fields, there is a 'Certificate' dropdown menu set to 'unknown'. Further down, there is a checkbox for 'Require Client Certificate' which is unchecked. Under 'Auth.', there are checkboxes for 'sha1' and 'md5' which are checked, and a 'null' option which is unchecked. Under 'Cipher.', there are checkboxes for 'blowfish 128', 'aes 128', 'aes 192', 'aes 256', and 'null'. 'blowfish 128' and 'aes 128' are checked, while the others are unchecked.

Secure Socket Tunneling Protocol



19

introduced by Microsoft in Windows Vista SP1, small chance to ever appear on Apple device. SSL v3 offers similar advantages to OpenVPN
requires tcp:443 (can be changed)

+ Pros

- very secure
- built-in client in MS Windows
- can bypass firewalls
- NAT friendly

- Cons

- RouterOS <-> MS Windows can use only RC4
- Proprietary standard owned by Microsoft so cannot be independently audited for back doors and suchlike
- Overhead of PPP

VPN hardware acceleration

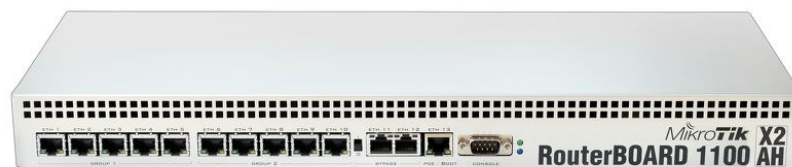


20

AES for IPSec, not for SSTP/OVPN



RB850



1100AHx2

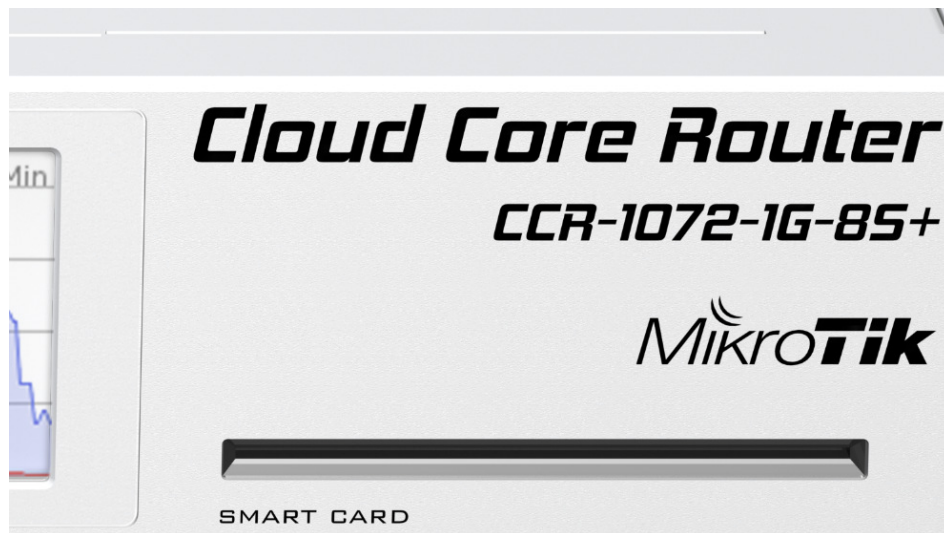


Cloud Core Router (tile CPU family)

Smart Card slots



21



CCR 1072 – full size



CCR 1009 – sim factor



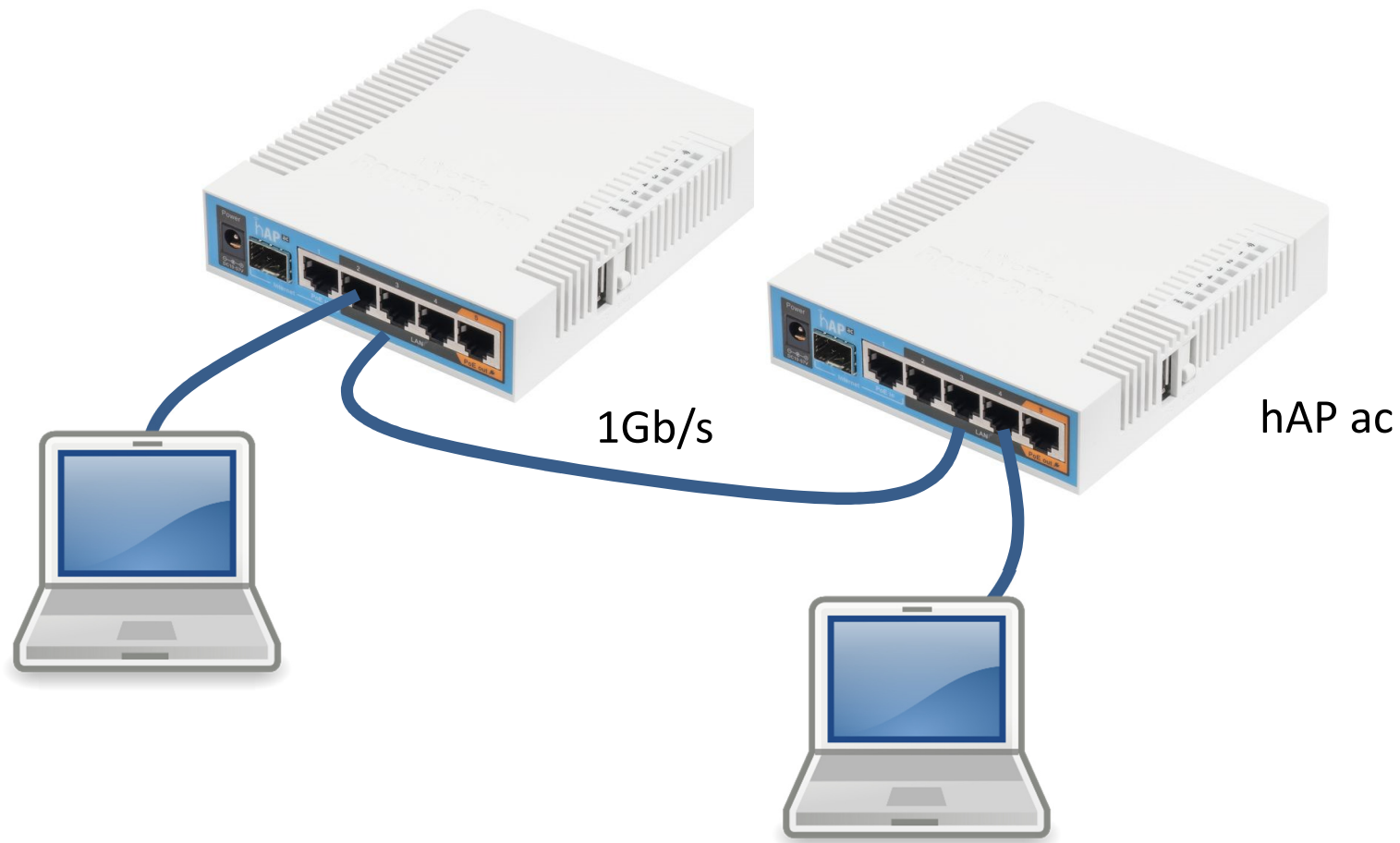
Tunnel characteristics

VPN type	Logical interface	Encryption	Authentication	Can be bridged
EoIP	+	-	-	+
IPIP	+	-	-	-
PPTP	+	+ MPPE128	-	with BCP
L2TP	+	+ MPPE128	-	with BCP
PPPoE	+	+ MPPE128	-	with BCP
SSTP	+	TLS (AES/RC4)	+ TLS	with BCP
OpenVPN	+	TLS (AES/BF)	+ TLS	with BCP
GRE	+	-	-	-
IPSec	-	+	+	-

Performance testbed



23





Testbed calibration

simple routing, no encryption, no fastpath

Transfer size: 1GB

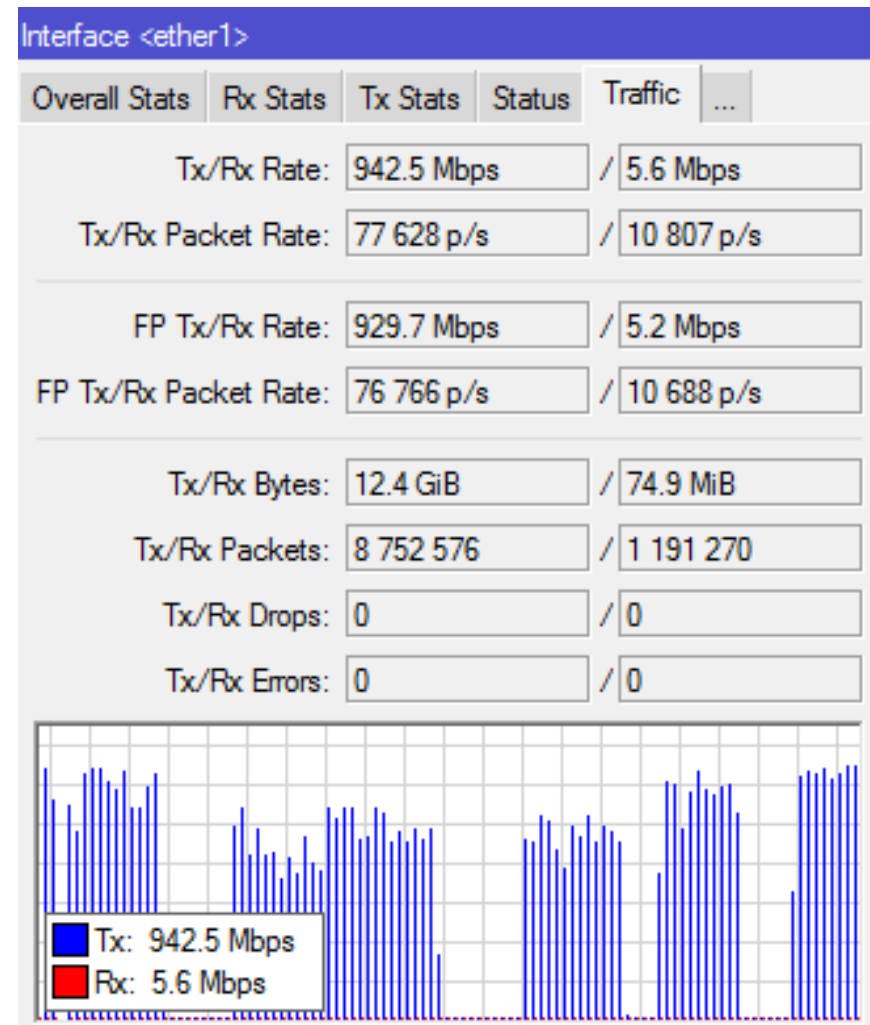
Protocol: SMB3 over TCP

time: 9.938s

cpu ~ 35%

average bandwidth: 805 Mb/s

overhead: 4.3%



PPTP benchmark



25

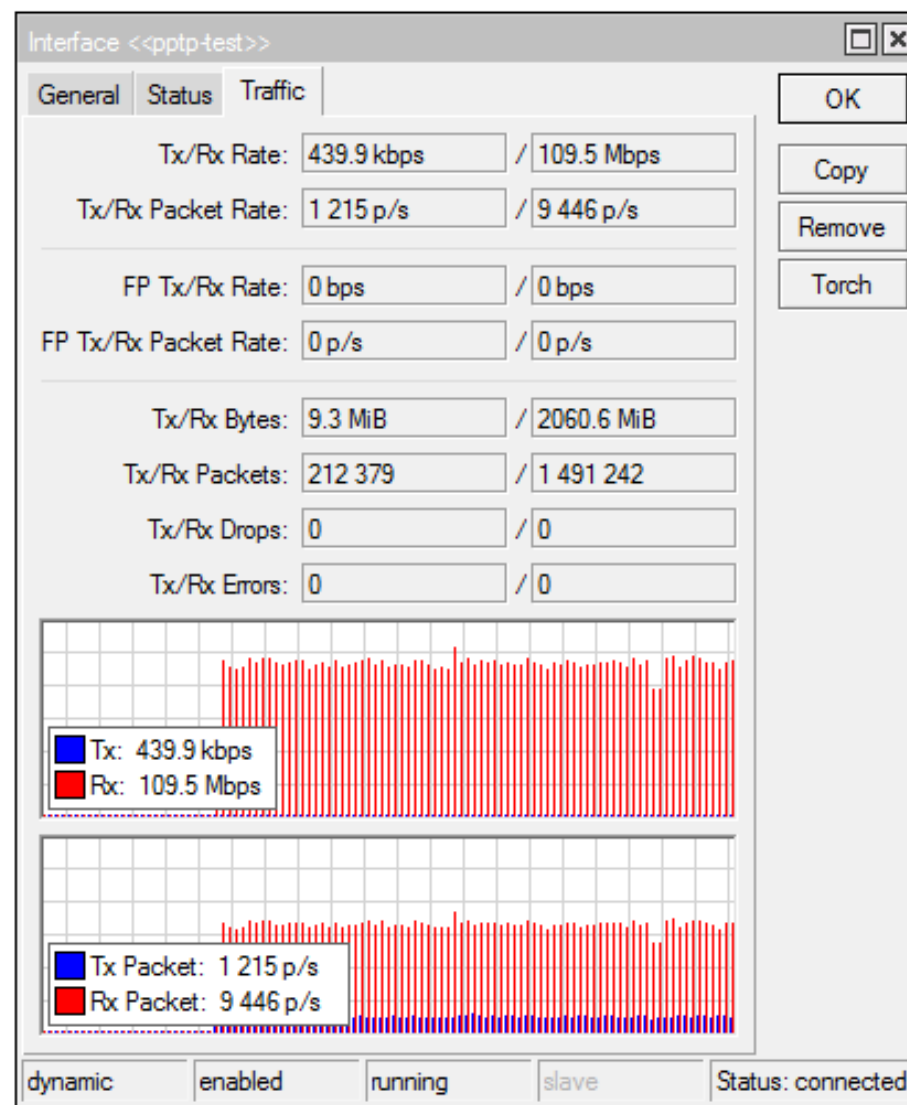
PPTP, MPPE128 stateless

time: 9.938s

cpu ~ 99%

average bandwidth: 97.44 Mb/s

overhead: 7.2%



IPSec benchmark



26

Et...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack	
800 (ip)	50 (ipsec)	3.3.3.2	3.3.3.1			435.8 k...	48.4 Mbps	457	40	▼
800 (ip)	6 (tcp)	2.2.2.9:445 (smb)	1.1.1.4:40457			0 bps	46.5 Mbps	0	40	▲

IPSec, AES128 / SHA1 / pfs

time: 169.525s

cpu ~ 99%

average bandwidth: 47.19 Mb/s

overhead: 8.3%

IPSec, AES256 / SHA1 / pfs

time: 203.436s

cpu ~ 99%

average bandwidth: 39.32 Mb/s

overhead: 8.3%

OVPN benchmark



27

Interface List

Interface

Ethernet

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VRRP

Bonding

LTE

	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
DR	<ovpn-test>	OVPN Server Binding		522.5 kbps	31.1 Mbps	1 382	2 601
R	ether1	Ethernet	1598	32.0 Mbps	752.8 kbps	2 649	1 438
	ether2	Ethernet	1598	0 bps	0 bps	0	0
R	ether3	Ethernet	1598	2.6 Mbps	35.4 Mbps	2 569	4 702
	ether4	Ethernet	1598	0 bps	0 bps	0	0
	ether5	Ethernet	1598	0 bps	0 bps	0	0

OVPN, AES-128-CBC/SHA1/ 2048 certificate
time: 325.66s
cpu ~ 65%
average bandwidth : 24.56 Mb/s

OVPN, AES-256-CBC/SHA1/ 2048 certificate
time: 357.94s
cpu ~ 70%
average bandwidth : 22.35 Mb/s
~15% overhead

Interface <ether3>					
Ethernet	Overall Stats	Rx Stats	Tx Stats	Status	Traffic
Tx/Rx Bytes: 90529427 / 1237277873					
Tx/Rx 64: 0 / 0					
Tx/Rx 65-127: 590235 / 4397					
Tx/Rx 128-255: 70953 / 517692					
Tx/Rx 256-511: 4140 / 11660					
Tx/Rx 512-1023: 19782 / 7529					
Tx/Rx 1024-1518: 15180 / 747912					
Tx/Rx 1519-max: 0 / 0					
Tx/Rx Too Long: 0 / 0					

SSTP benchmark



28

Interface List

Interface

Ethernet

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VRRP

Bonding

LTE

Find

	Name	Type	L2 MTU	Tx	Rx	Tx Pac
DR	<sstp-test>	SSTP Server Binding		231.2 kbps	16.0 Mbps	
R	ether1	Ethernet	1598	17.2 Mbps	341.4 kbps	
	ether2	Ethernet	1598	0 bps	0 bps	
R	ether3	Ethernet	1598	1048.4 kbps	18.7 Mbps	
	ether4	Ethernet	1598	0 bps	0 bps	

SSTP, AES256-CBC (certificate/fps impact minimal)

time: 533.887s

cpu ~ 50%

av.bandwidth : 15.00 Mb/s

overhead: 13%

Experimentation summary



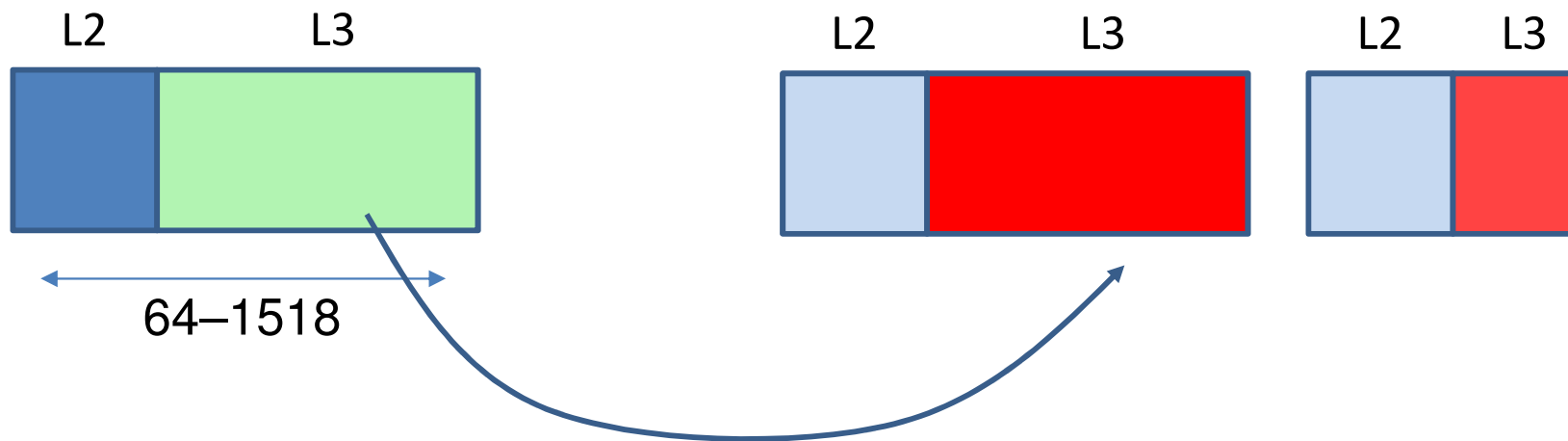
29

VPN	Measured Mb/s	Overhead	CPU
-	805	4.3%	35%
PPTP	97.5	7.2%	99%
IPSec	47	8.3%	99%
OVPN	25	15%	65%
SSTP	15	13%	50%

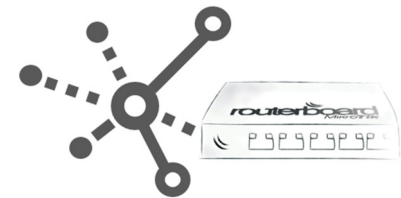
What happens to data packet



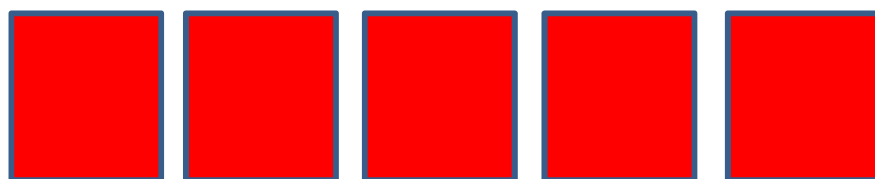
30



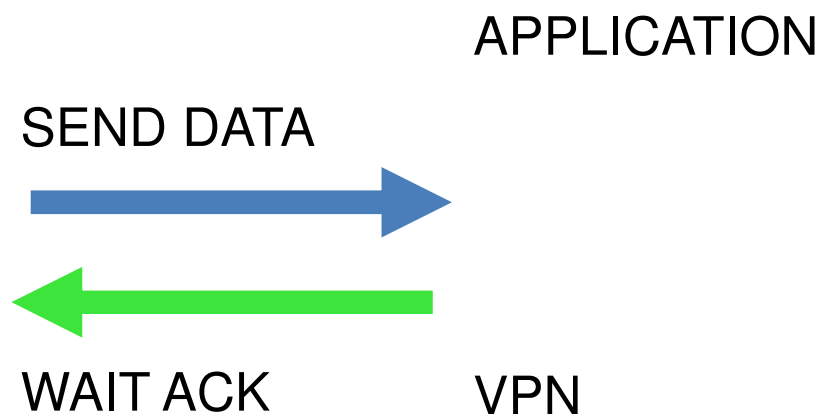
TCP over TCP problem



31



TCP-WINDOW 64kb



Conclusion – encryption works



32

- IPSEC – on CCR routers with routable IPs
- OVPN – primary choice for road warriors (its now time to switch from PPTP)
- SSTP – primary choice for MS Windows
- GRE-IPSEC to connect to Cisco
- Waiting for IKEv2



all IPv6 devices must
support IPSec

SXT-LTE now can get IPv6 address.
This is a great potential for IPv6 VPNs in mobile world.

Thank You!

