



# Building scalable IPSec infrastructure with MikroTik

IPSec, L2TP/IPSec, OSPF

# Presenter information

Tomas Kirnak

Network design

Security, wireless

Servers

Virtualization

MikroTik Certified Trainer

Atris, Slovakia

Established 1991



Complete IT solutions

Networking, servers

Virtualization

IP security systems

# Agenda

- IPsec basics
  - Configure the L2TP/IPsec AC
  - Configure Mikrotik Client
  - Configure Windows client for Raod Warriors
- + Security and firewalling
- + IPsec Mythbusting
- + Live demo

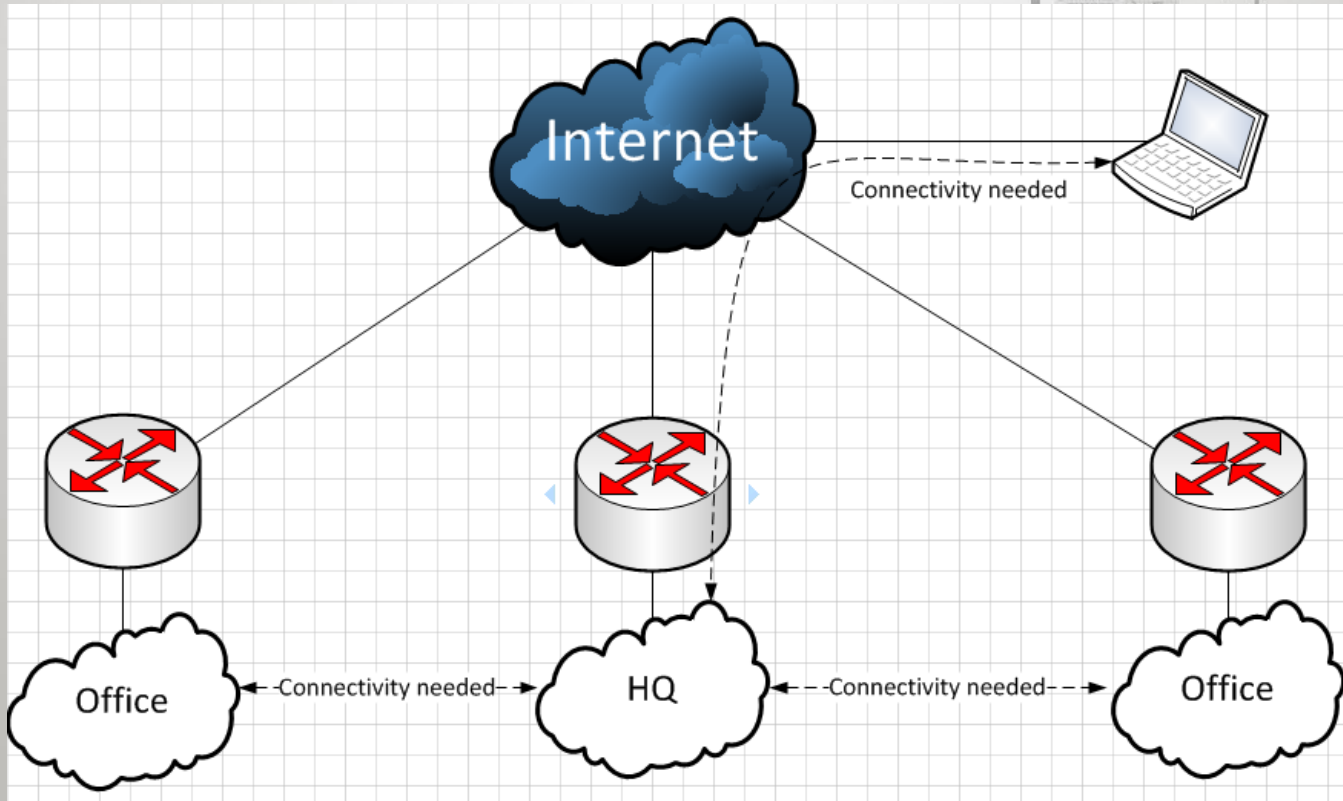
# Everyone needs to be connected

- The basic business need: connectivity
- Branch offices, retail outlets, etc.
- Employees on the road need access.

# Answer: V irtual P ivate N etworks

- In the past: WAN links or private circuits
- Today VPN is a better answer, mostly because internet connection is fast and cheap.

# Objective:



# Problems:

- How do I VPN?
- What about security?
- How to deal with connections from unknown networks for road warriors?

# Solution:

- IPsec
- L2TP over IPsec with OSPF
- L2TP over IPsec for Road Warriors



# IPSec basics

- IPSec is a standard for secure communication over public networks.
- To establish an IPSec connection – 2 phases
- Phase 1 – IKE – Internet Key exchange
- Phase 2 – IPSec

# Phase 1 – IKE

- Generates keys and Security Associations (SAs) used for further IPSec encryption
- These keys are used to secure the traffic.
- IKE is configured in IPSec -> Peers

\*not how IKE actually works, simplified version

# Phase 2 - IPSec

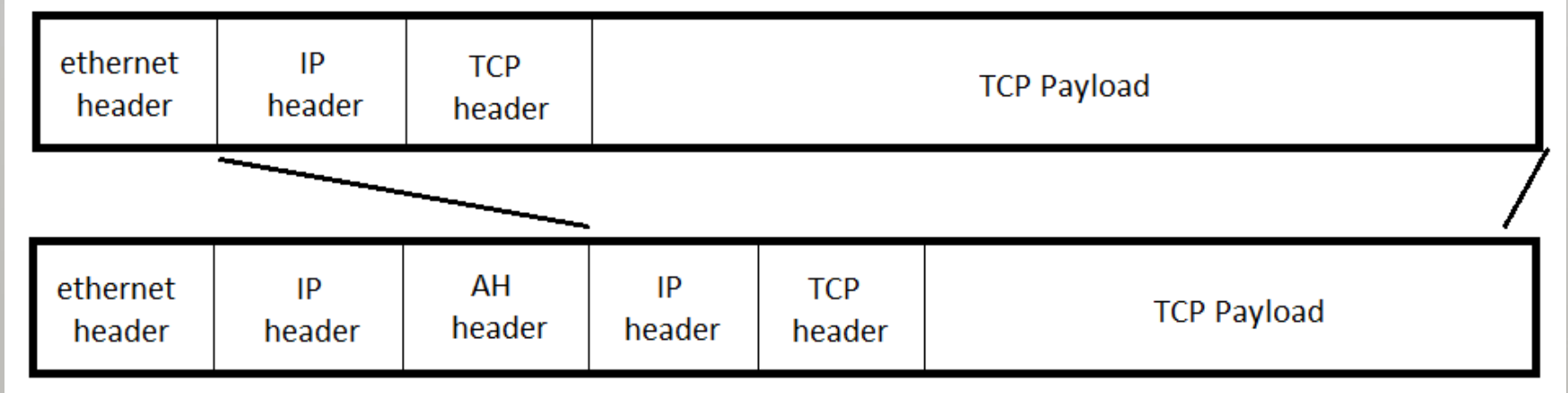
- Configured in IPSec -> Policy
- Protocols: AH - Authentication Header  
ESP - Encapsulating Security Payload
- Modes: Transport  
Tunnel

# AH vs. ESP

- AH is used for authenticating traffic only.
- ESP is used for encrypting traffic. ESP also can, but doesn't have to authenticate.

# Tunnel mode

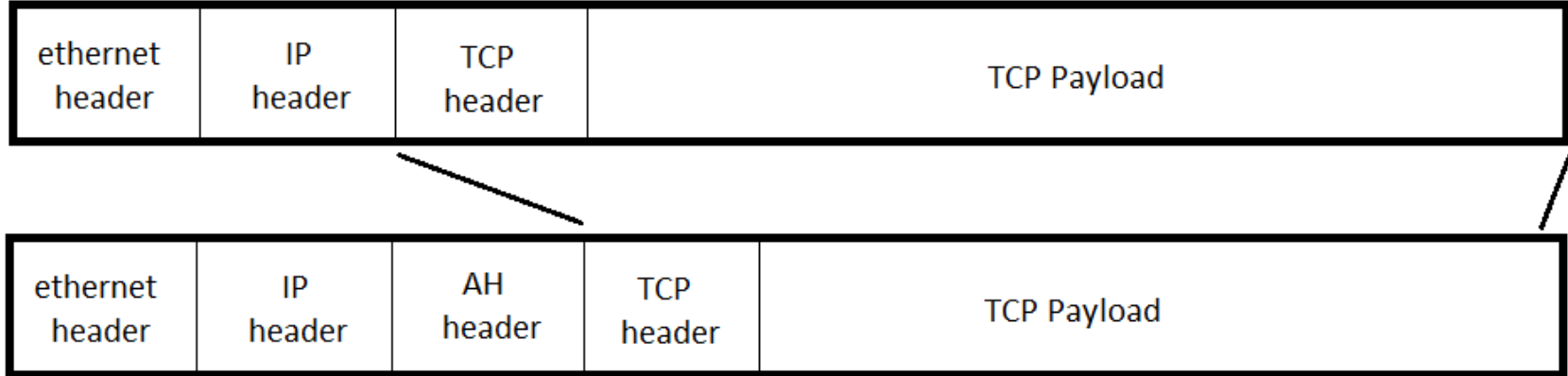
- The whole IP packet is encrypted.



- Therefore, tunnel mode can be used for VPN.

# Transport mode

- Only the payload of the packet is encapsulated and secured.



- Transport mode is used to secure host-to-host, or end-to-end traffic.

# Tunnel vs. Transport

Tunnel mode:

- + Simple and very fast to configure.
- + No routing needed.
- Policies need to be configured for all networks taking part in the VPN, on all devices taking part in the VPN.
- The tunnel is not an actual interface, no OSPF.

\*not covered in this presentation

# Tunnel vs. Transport

- Transport mode is only for securing traffic; we need something else to VPN.
- We will use L2TP to tunnel and do the VPN. We will then secure the L2TP tunnel with IPSec in transport mode.
- This provides benefits of an actual L2TP interface and, therefore, OSPF.
- You can do a full mesh between all IPSec peers, or just one connection to the AC, OSPF will take care of routing.



# What needs to be configured

- Since IPSec works in 2 phases, we need to configure each phase separately.
- Both Phases need to be configured, and need to match on both endpoints of the IPSec connection.

# Configuring IPsec Phase 1

- Configure phase 1:

This will generate the SAs which will later be used to encrypt the traffic.

The transaction that generates the SAs can be encrypted by the IKE process differently than the actual traffic encryption in Phase 2.

\*not how IKE actually works, simplified version

# IPSec Peer – part 1

New IPsec Peer

Address: 0.0.0.0/0

Port: 500

Auth. Method: pre shared key

Secret: ourlittlesecret

Exchange Mode: main

Send Initial Contact

NAT Traversal

My ID User FQDN:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

- Address – which IPsec partner addresses is this configuration for
- Secret – used to start the key exchange and generation. It can also be a certificate
- NAT Traversal – encapsulates IPsec packets in UDP, making IPsec NAT compatible.

# IPSec Peer – part 2

Proposal Check: obey

Hash Algorithm: md5

Encryption Algorithm: 3des

DH Group: modp1024

Generate Policy

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: 15 s

DPD Maximum Failures: 5

enabled

- Hash and encryption algorithms used for securing our traffic.
- md5 and sha are supported for hashing.
- Many encryption algorithms are supported (des, 3des, aes128-256)
- DPD – very useful when the other side of IPSec connection dies.

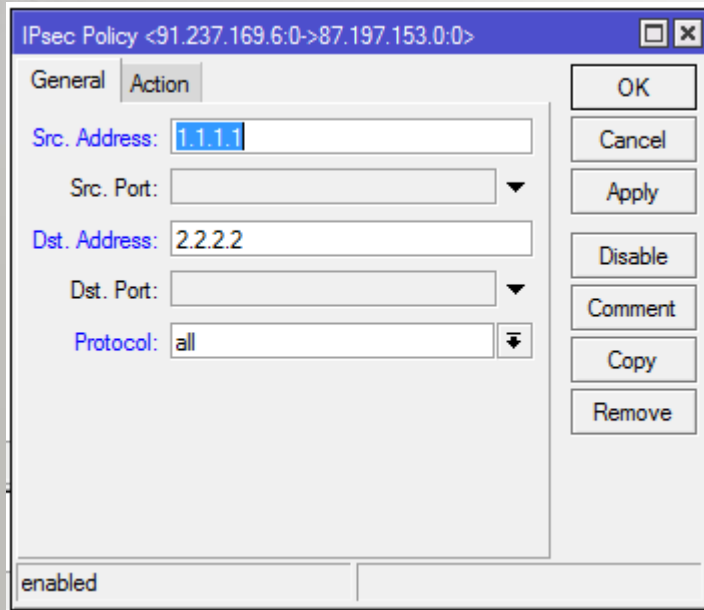
# Configuring IPsec Phase 2

- Continue with phase 2:  
This will tell the router what to actually encrypt and which SAs to use

These SAs were generated in Phase 1

# IPSec policy – part 1

- This tells the router what traffic should IPSec be applied to.
- For traffic from src address to the dst address, apply IPSec.

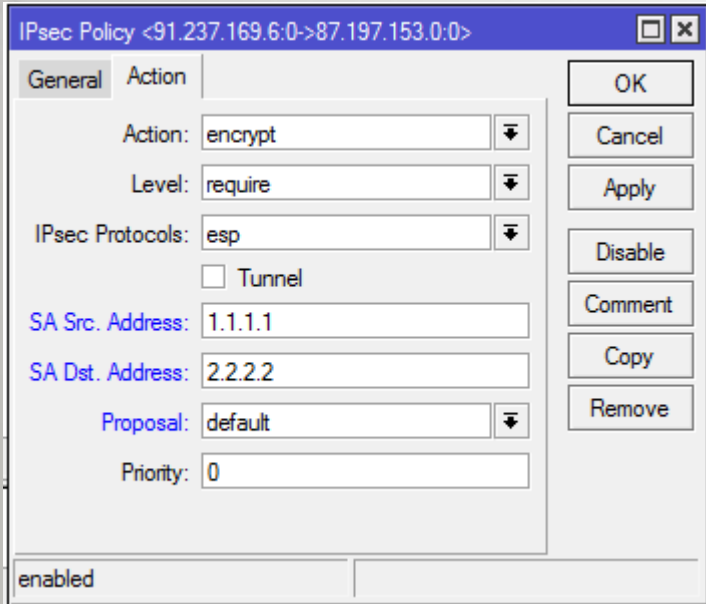


The screenshot shows a configuration window titled "IPsec Policy <91.237.169.6:0->87.197.153.0:0>". It has two tabs: "General" and "Action". The "General" tab is active and contains the following fields:

- Src. Address: 1.1.1.1
- Src. Port: (empty dropdown)
- Dst. Address: 2.2.2.2
- Dst. Port: (empty dropdown)
- Protocol: all

At the bottom left, there is a checkbox labeled "enabled" which is checked. On the right side of the window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

# IPSec policy – part 2



- Configure what to do with the traffic  
(encrypt using ESP Transport mode)
- Which SAs to use, and which proposal

# IPSec proposal

IPsec Proposal <default>

Name:

Auth. Algorithms

md5  sha1  null

Encr. Algorithms

null  3des  aes-192  blowfish  camellia-128  camellia-256  des  aes-128  aes-256  twofish  camellia-192

Lifetime:

PFS Group:

enabled default

OK  
Cancel  
Apply  
Disable  
Copy  
Remove

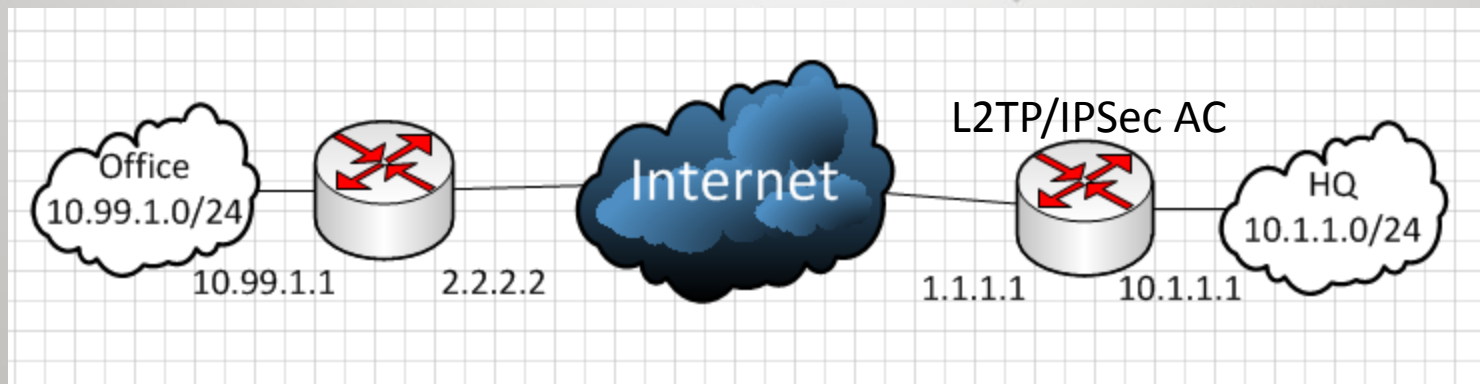
- Tells our router what encryption and hashing algorithms to use in Phase 2



# Configuring IPsec

Configuration tip: enable IPsec logging  
`/system logging add topics=ipsec`

# Actual example topology



\*simplified network  
for use in all next examples

# L2TP server config

```
/ip pool
add name=L2TP_Clients ranges=10.255.255.101-10.255.255.255

/ppp profile
add address-list=L2TP_Clients local-address=10.255.255.1 name=L2TP remote-address=L2TP_Clients

/ppp secret
add name=tomas password=pass profile=L2TP service=l2tp

/interface l2tp-server server
set authentication=mschap2 default-profile=L2TP enabled=yes keepalive-timeout=10
```

# IPSec config on the AC

```
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-128
/ip ipsec peer
add comment=L2TP/IPsec dpd-interval=5s dpd-maximum-failures=3 exchange-mode=main-l2tp generate-policy=yes \
hash-algorithm=sha lifetime=1h nat-traversal=yes secret=publicVPNaccess send-initial-contact=no
```

IPsec Peer <0.0.0.0/0>

Address:	0.0.0.0/0	OK
Port:	500	Cancel
Auth. Method:	pre shared key	Apply
Secret:	publicVPNaccess	Disable
		Comment
		Copy
		Remove
Exchange Mode:	main l2tp	
	<input type="checkbox"/> Send Initial Contact	
	<input checked="" type="checkbox"/> NAT Traversal	
My ID User FQDN:		
Proposal Check:	obey	
Hash Algorithm:	sha	
Encryption Algorithm:	3des	
DH Group:	modp1024	
	<input checked="" type="checkbox"/> Generate Policy	
Lifetime:	01:00:00	
Lifeytes:		

IPsec Proposal <default>

Name:	default	OK
		Cancel
		Apply
		Disable
		Copy
		Remove
- Auth. Algorithms -		
<input type="checkbox"/> md5	<input checked="" type="checkbox"/> sha1	
<input type="checkbox"/> null		
- Encr. Algorithms -		
<input type="checkbox"/> null	<input type="checkbox"/> des	
<input type="checkbox"/> 3des	<input checked="" type="checkbox"/> aes-128	
<input type="checkbox"/> aes-192	<input type="checkbox"/> aes-256	
<input type="checkbox"/> blowfish	<input type="checkbox"/> twofish	
<input type="checkbox"/> camellia-128	<input type="checkbox"/> camellia-192	
<input type="checkbox"/> camellia-256		
Lifetime:	00:30:00	
PFS Group:	modp 1024	
enabled	default	

# Config on the remote router

```
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-128
/ip ipsec peer
add address=AC_Public_IP dpd-interval=5s dpd-maximum-failures=3 hash-algorithm=\
  sha1 secret=publicVPNaccess
/ip ipsec policy
add dst-address=AC_Public_IP sa-dst-address=AC_Public_IP sa-src-address=\
  my_WAN_IP src-address=my_WAN_IP
/interface l2tp-client
add connect-to=AC_Public_IP disabled=no name=L2TP/IPSec password=pass profile=default user=tomas
```

New IPsec Policy

General Action

Src. Address: 2.2.2.2

Src. Port: [ ]

Dst. Address: 1.1.1.1

Dst. Port: [ ]

Protocol: 255 (all)

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled

New IPsec Policy

General Action

Action: encrypt

Level: require

IPsec Protocols: esp

Tunnel

SA Src. Address: 2.2.2.2

SA Dst. Address: 1.1.1.1

Proposal: default

Priority: 0

OK

Cancel

Apply

Disable

Comment

Copy

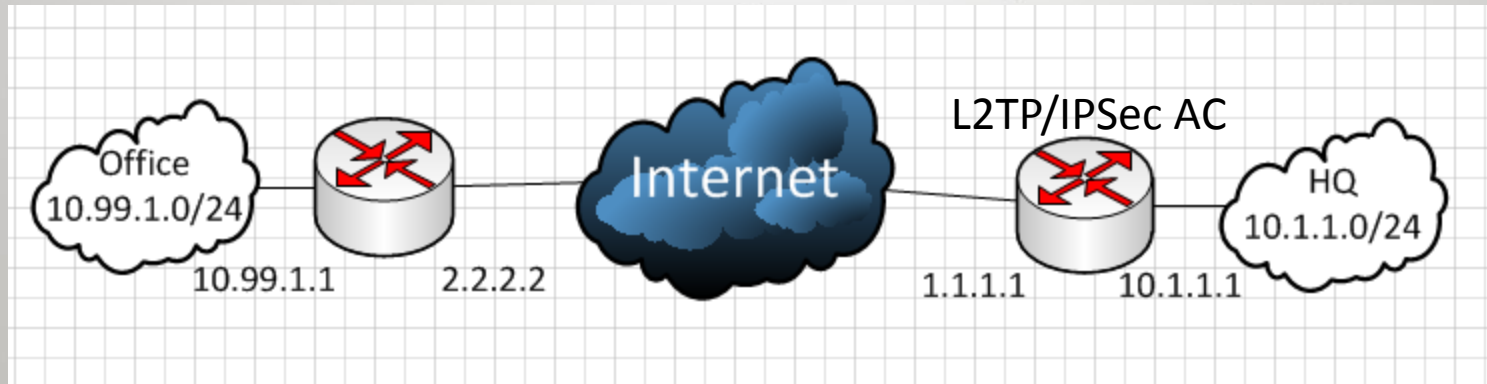
Remove

enabled

# Fast OSPF solution

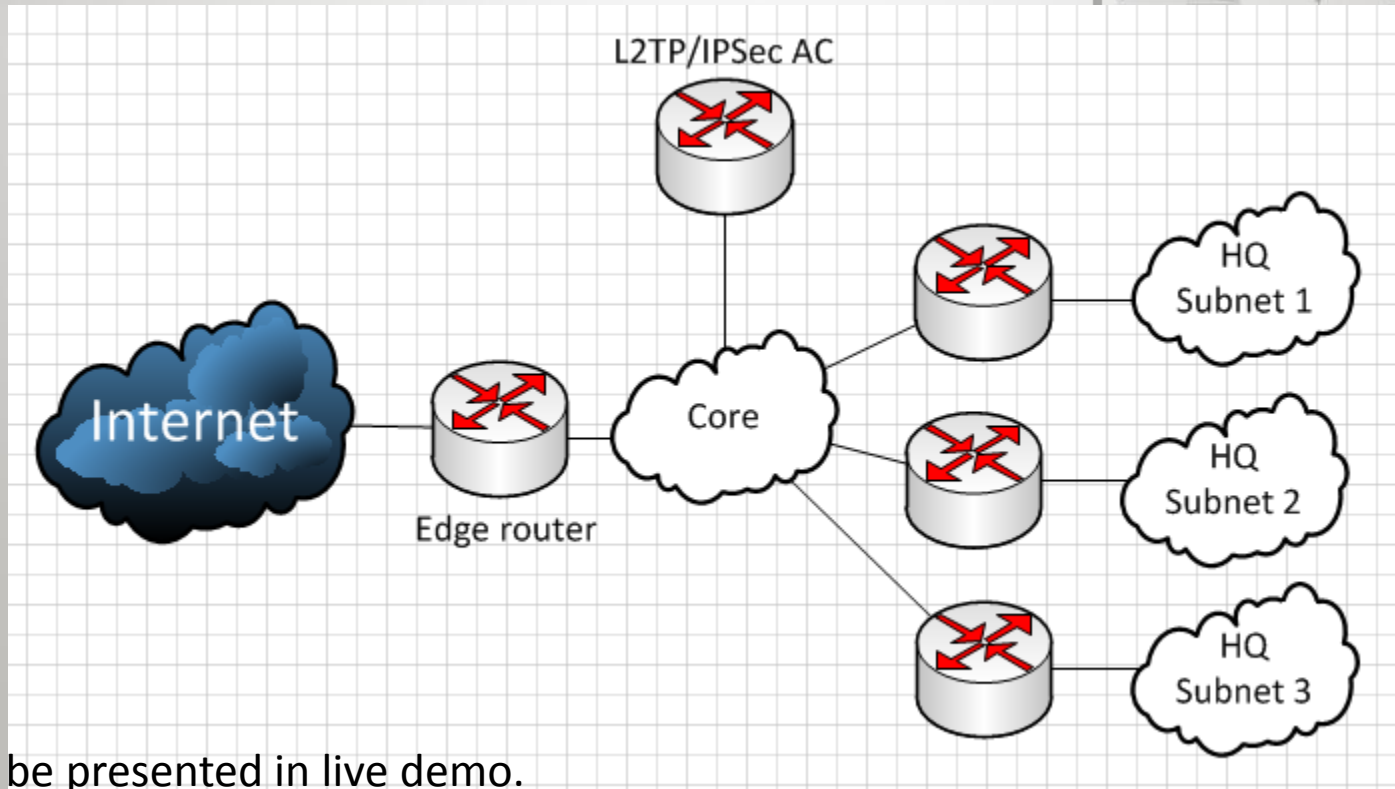
- Since L2TP is an interface, we need to do routing to be able to reach the HQ through that interface. We will use OSPF for our routing needs.
- Set a unique Instance Router ID for each router.
- Configure OSPF network of 0.0.0.0/0
- Note: NOT proper implementation of OSPF

# Actual example topology



Communication between the HQ and Office subnets will be possible. The packets will go over the L2TP interface, secured with IPsec in Transport mode.

# In bigger networks



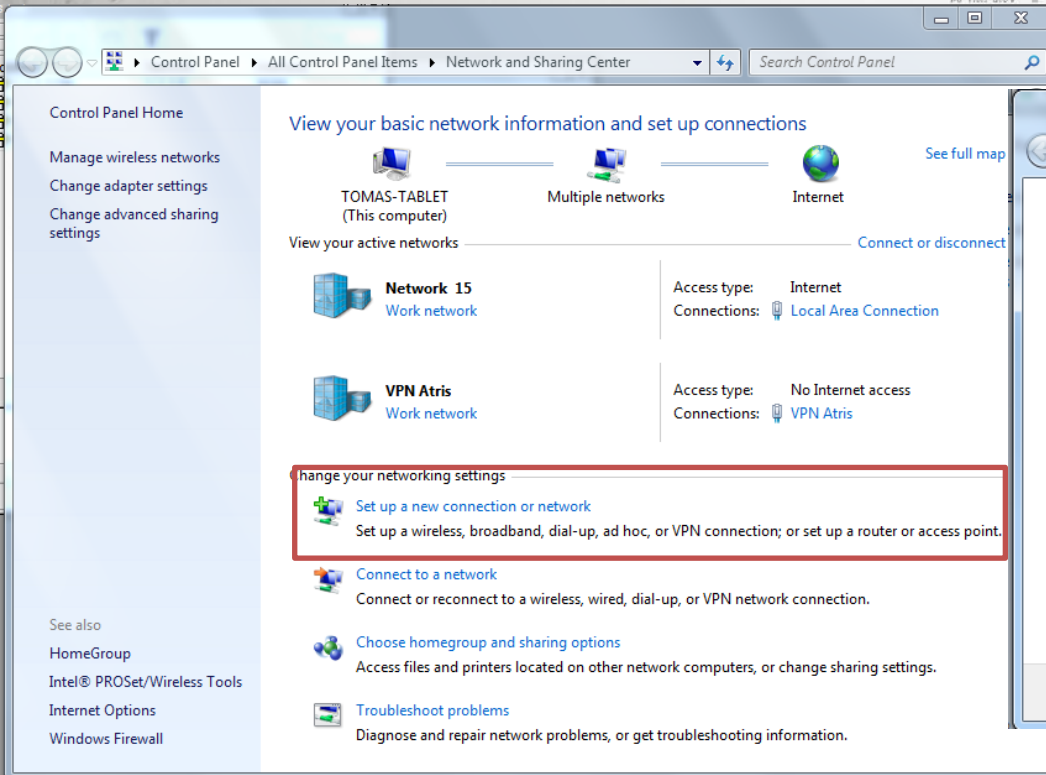
\* This will be presented in live demo.  
The basic configuration of the AC is the same.



# Road Warriors

- Roaming clients don't want to carry a router around just to connect to their company infrastructure.
- We will configure Windows to connect directly to our L2TP/IPSec AC and gain secure access to our inner infrastructure.
- L2TP/IPSec clients exist in Linux, Mac, Android, iToys...

# L2TP/IPSec on Windows



Control Panel Home

Manage wireless networks  
Change adapter settings  
Change advanced sharing settings

View your basic network information and set up connections [See full map](#)

TOMAS-TABLET (This computer) Multiple networks Internet

View your active networks [Connect or disconnect](#)

**Network 15**  
Work network  
Access type: Internet  
Connections: Local Area Connection

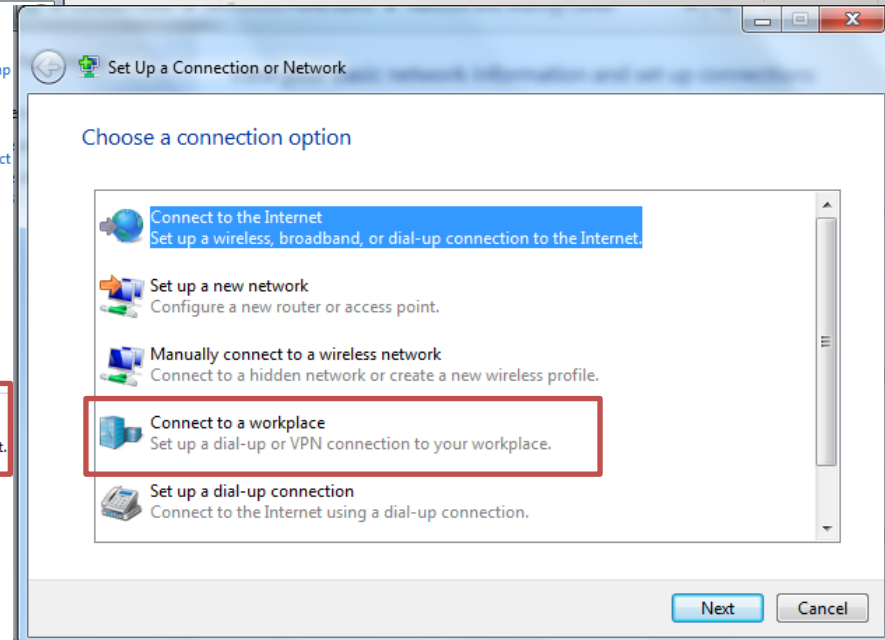
**VPN Atris**  
Work network  
Access type: No Internet access  
Connections: VPN Atris

**Change your networking settings**

- [Set up a new connection or network](#)  
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
- [Connect to a network](#)  
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
- [Choose homegroup and sharing options](#)  
Access files and printers located on other network computers, or change sharing settings.
- [Troubleshoot problems](#)  
Diagnose and repair network problems, or get troubleshooting information.

See also

- HomeGroup
- Intel® PROSet/Wireless Tools
- Internet Options
- Windows Firewall



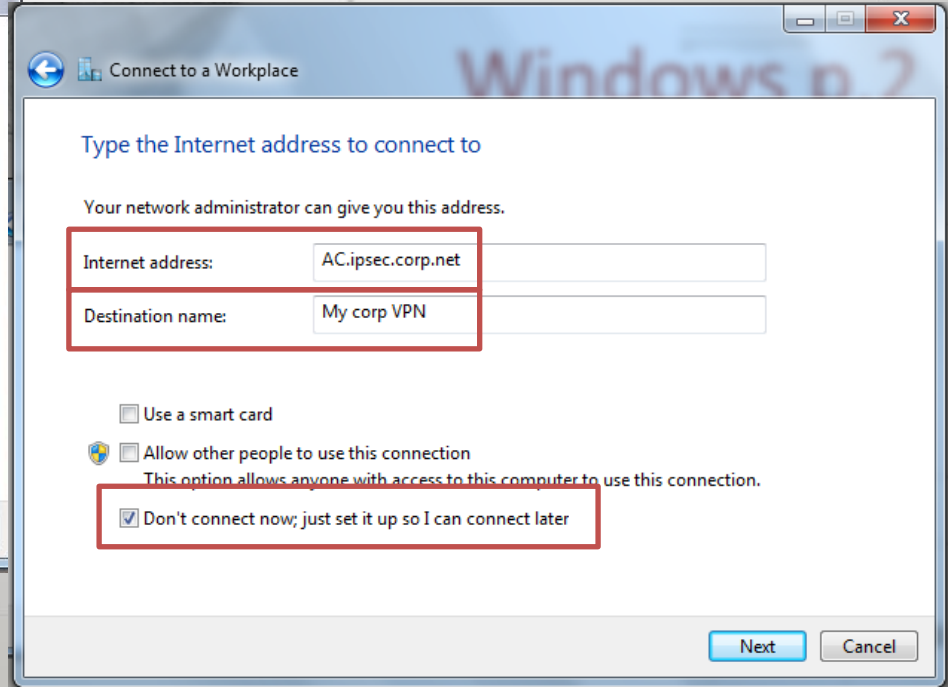
Set Up a Connection or Network

Choose a connection option

- Connect to the Internet**  
Set up a wireless, broadband, or dial-up connection to the Internet.
- Set up a new network**  
Configure a new router or access point.
- Manually connect to a wireless network**  
Connect to a hidden network or create a new wireless profile.
- Connect to a workplace**  
Set up a dial-up or VPN connection to your workplace.
- Set up a dial-up connection**  
Connect to the Internet using a dial-up connection.

Next Cancel

# Windows p.2



# Windows p.3

Connect to a Workplace

Type your user name and password **L2TP credentials**

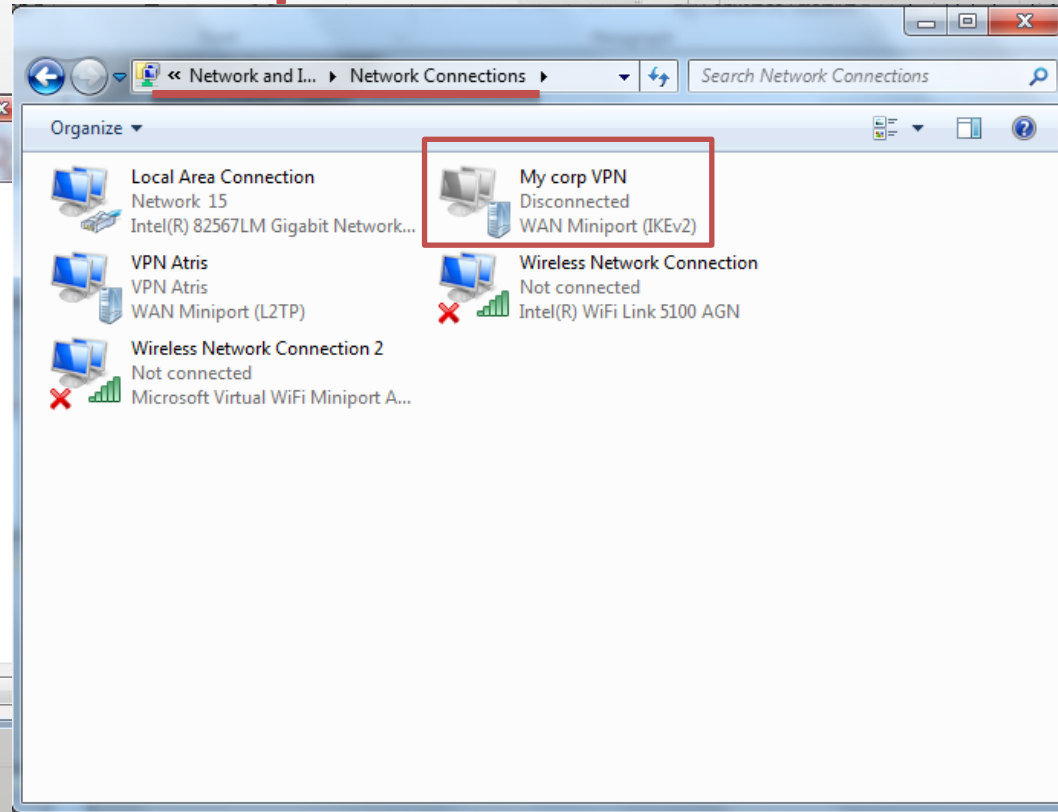
User name:

Password:

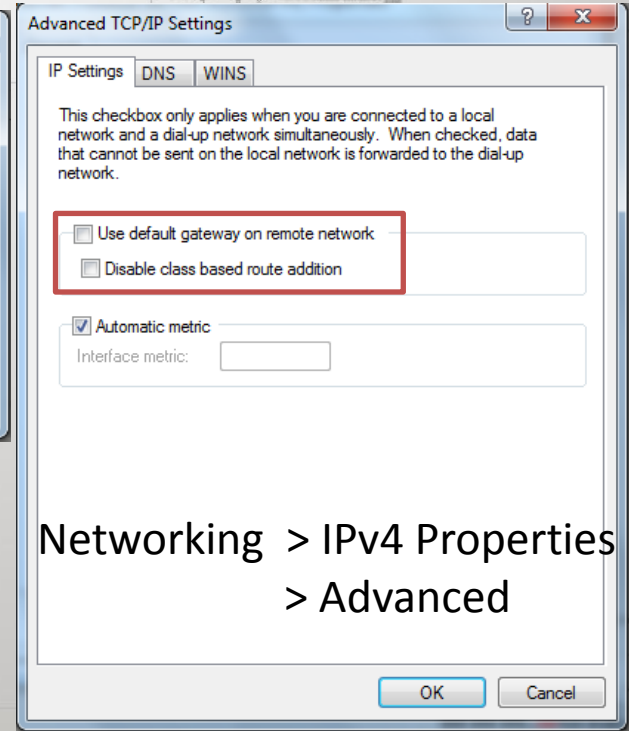
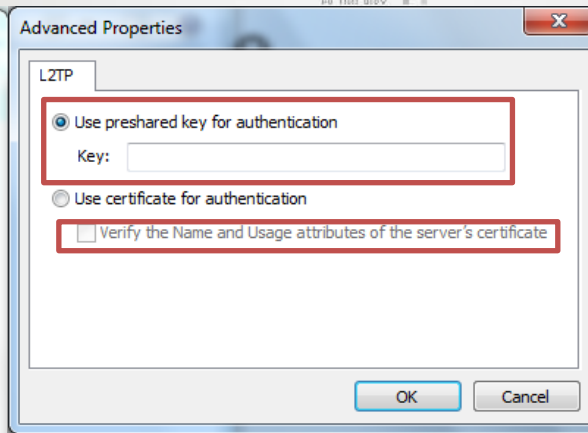
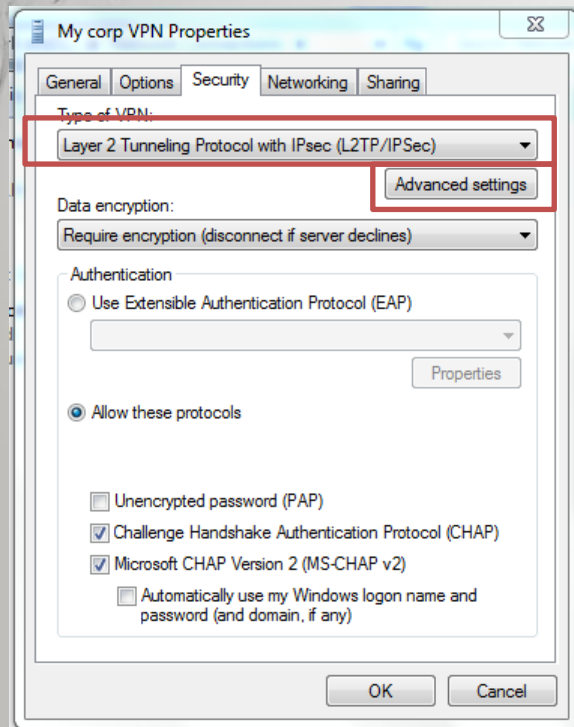
Show characters

Remember this password

Domain (optional):

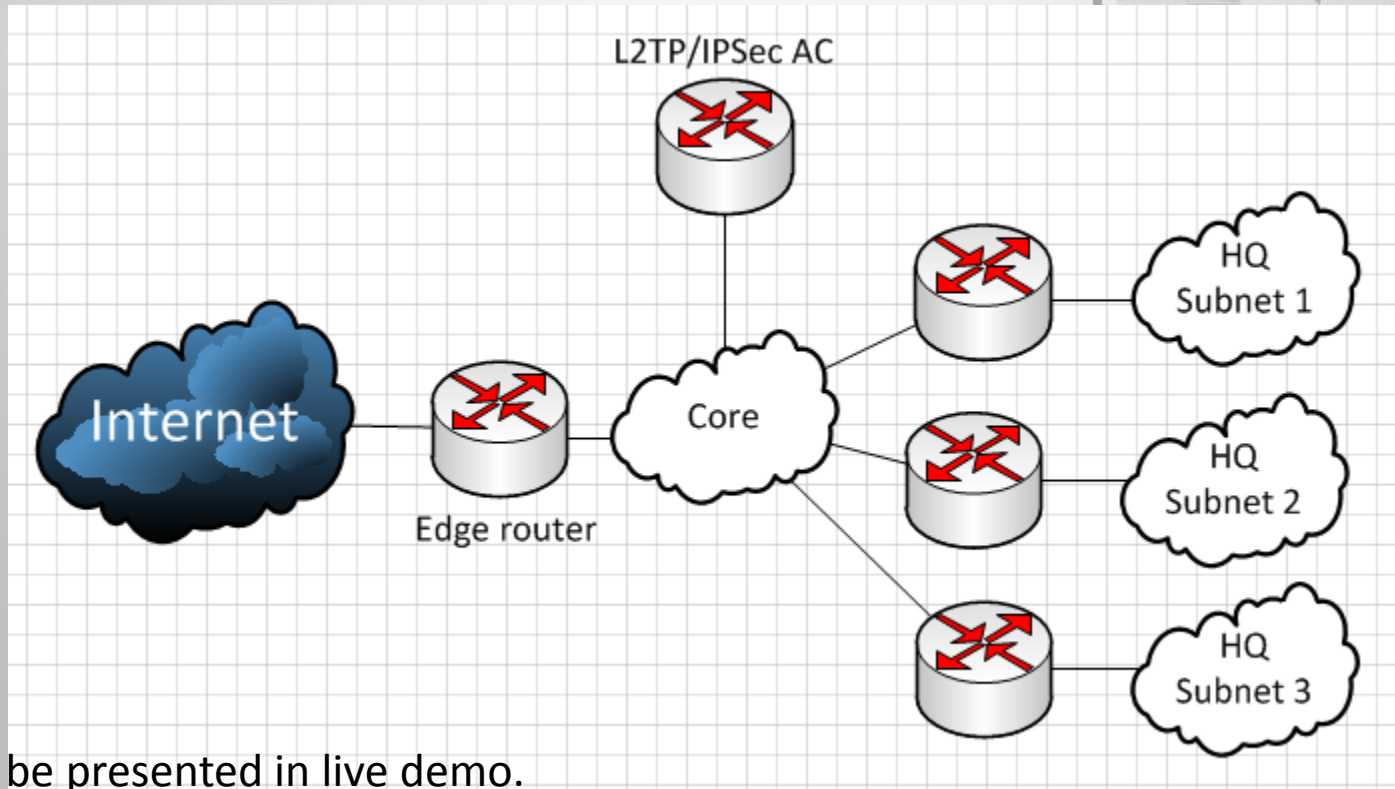


# Windows p.4



Networking > IPv4 Properties  
> Advanced

# In bigger networks



\* This will be presented in live demo.  
The basic configuration of the AC is the same.

# Live Demo

- Get to a server on corp LAN – 10.3.1.99

# Mythbusters, IPSec edition

IPSec does not work through NAT.

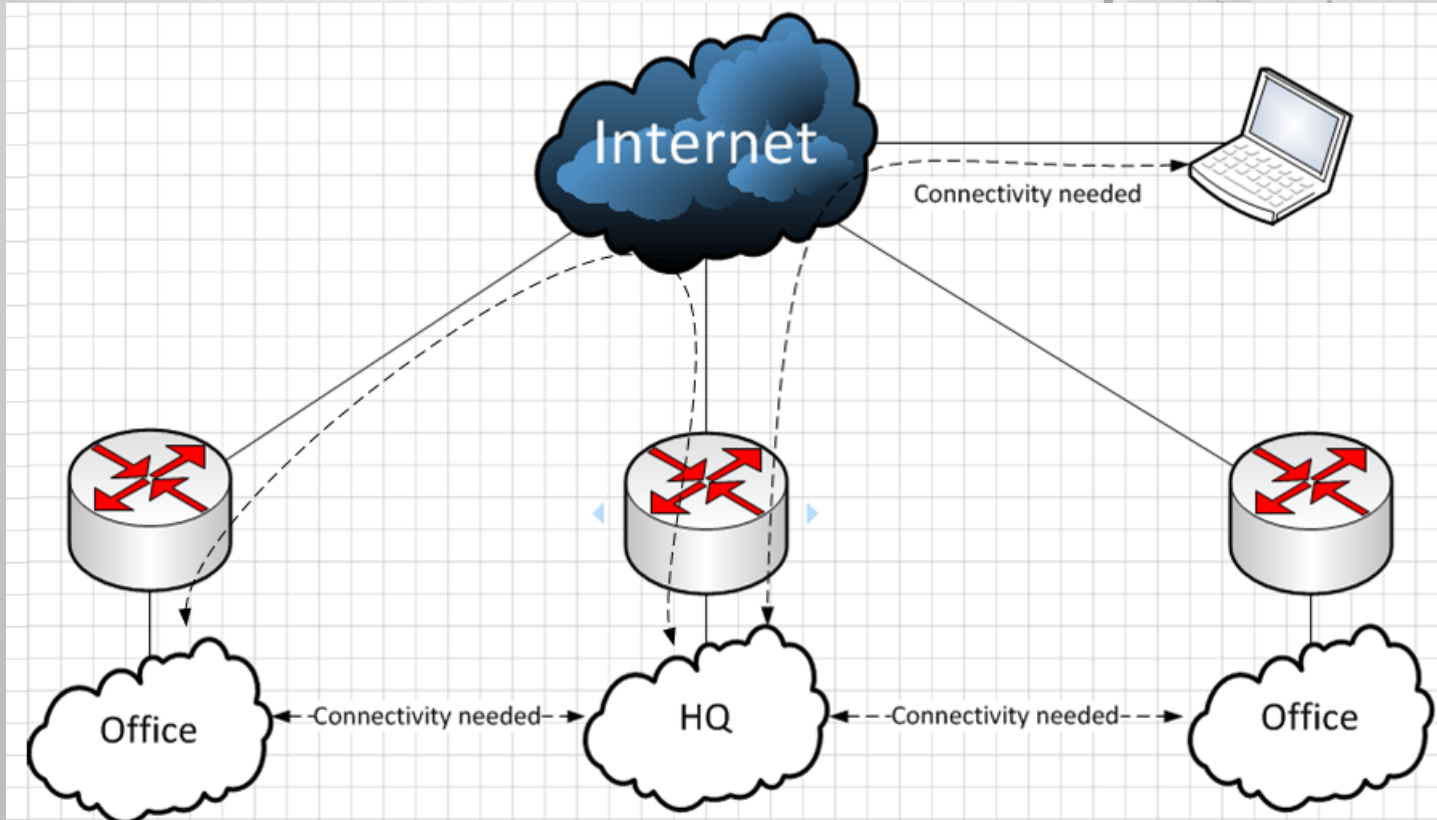
Not true.



# Live Demo

- Get from my Road Warrior, through the corp infrastructure to a PC in an Office which is also connected by L2TP/IPSec – 192.168.2.2

# Exact data flow:



# Explaining the routes

Administrator: C:\Windows\system32\cmd.exe

Trace complete.

```
C:\Users\tomas>tracert -d 10.3.1.99
```

Tracing route to 10.3.1.99 over a maximum of 30 hops

1	44 ms	46 ms	49 ms	10.255.255.1
2	55 ms	46 ms	45 ms	10.1.0.2
3	49 ms	49 ms	53 ms	10.3.1.99

Trace complete.

```
C:\Users\tomas>tracert -d 192.168.2.2
```

Tracing route to 192.168.2.2 over a maximum of 30 hops

1	46 ms	55 ms	45 ms	10.255.255.1
2	47 ms	48 ms	49 ms	10.1.0.1
3	75 ms	74 ms	71 ms	10.255.2.2
4	76 ms	83 ms	74 ms	192.168.2.2

Trace complete.

```
C:\Users\tomas>
```

L2TP/IPSec AC

Router of a subnet on core

Destination

Our L2TP/IPSec AC

Other Office L2TP/IPSec AC

Router at the Other Office

Destination

# Security:

- IPSec requires the following rules in firewall to be unblocked on input:
  - UDP 500 – IKE
  - UDP 4500 – NAT Traversal
  - L4 Proto 50 – IPSec ESP
- L2TP needs to also be accessible, but only to IPSec enabled peers.

# Mythbusters, IPSec edition

There is no way to allow L2TP server to IPSec enabled peers only in MikroTik firewall. It doesn't have an IPSec policy matcher.

Not true.

# Secure services for IPSec peers only

- MikroTik firewall doesn't have an IPSec policy matcher. But we can easily script this functionality.

[http://wiki.mikrotik.com/wiki/Securing\\_L2TP\\_Server\\_for\\_IPSec](http://wiki.mikrotik.com/wiki/Securing_L2TP_Server_for_IPSec)

# Mythbusters, IPSec edition

There is no way to use IPSec on MikroTik with a dynamic WAN IP, because the policy will not catch the traffic

Not true.

# Resolution

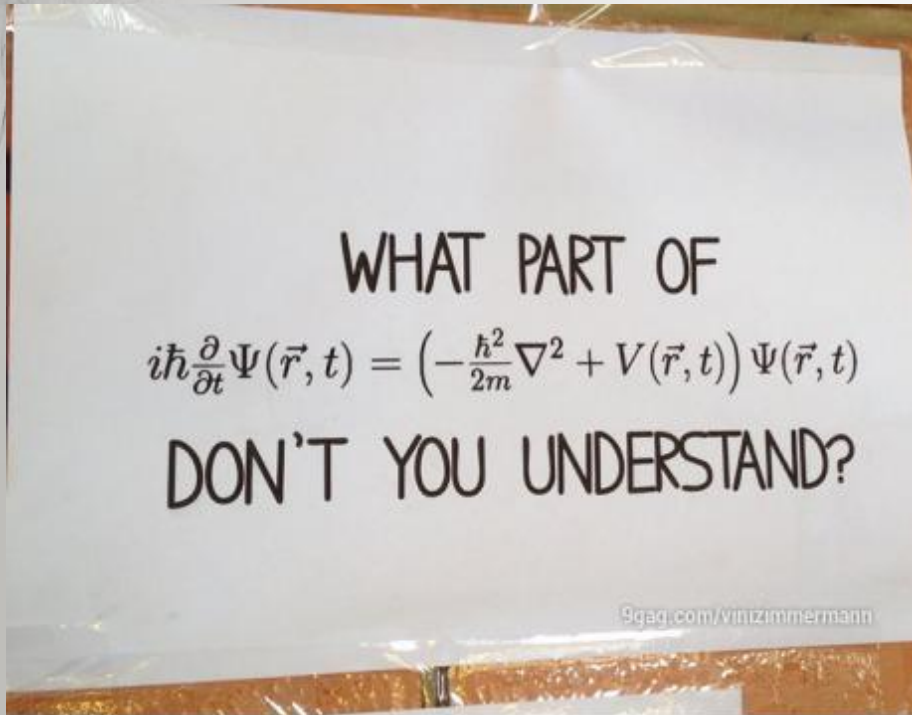
- Use a script to change the policy when the WAN IP changes.

[http://wiki.mikrotik.com/wiki/IPSec\\_Policy\\_Dynamic](http://wiki.mikrotik.com/wiki/IPSec_Policy_Dynamic)



# Known issues:

- If you have multiple IP addresses on the interface which you use to connect the L2TP client, the L2TP server will only respond on the lowest IP.
- Dynamically created IPsec policies will never be deleted by the IPsec daemon.
- You can not have more than one 0.0.0.0/0 peer. If you configure multiple, only one will work.
  - Use certificates to solve problems with one PSK for all peers.



If you have any questions, please ask now, or find me after the presentation.



Thanks for listening

Tomas Kirnak

t.kirnak@atris.sk