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

www.atris.sk

Agenda

- IPSec basics
- Configure the L2TP/IPSec AC
- Configure Mikrotik Client
- Configure Windows client for Raod Warriors

+ Security and firewalling

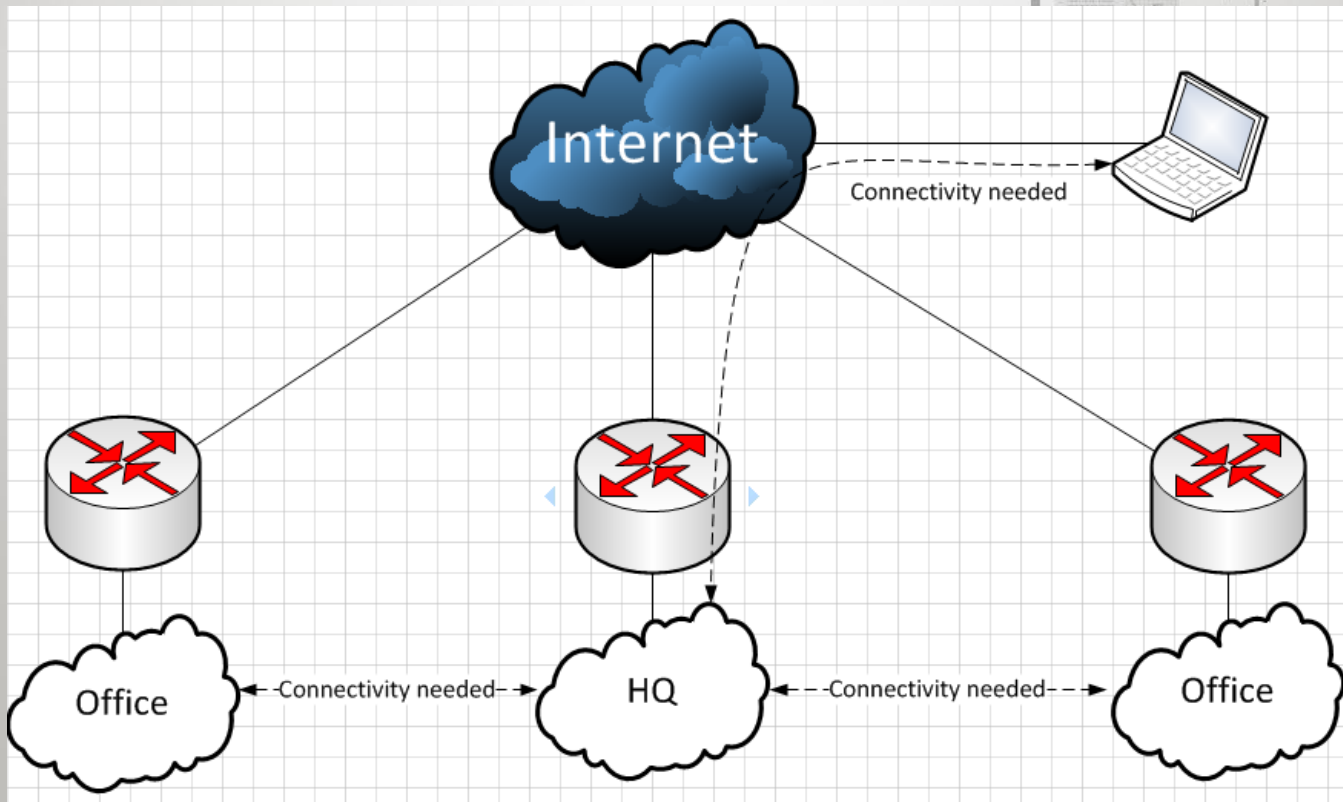+ IPSec Mythbusting

+ Live demo

www.atris.sk

Everyone needs to be connected

- The basic business need: connectivity

- Branch offices, retail outlets, etc.

- Employees on the road need access.

Answer: Virtual Private Networks

- In the past: WAN links or private circuits

- Today VPN is a better answer, mostly because internet connection is fast and cheap.

www.atris.sk

Objective:

Problems:

- How do I VPN?

- What about security?

- How to deal with connections from unknown networks for road warriors?

www.atris.sk

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
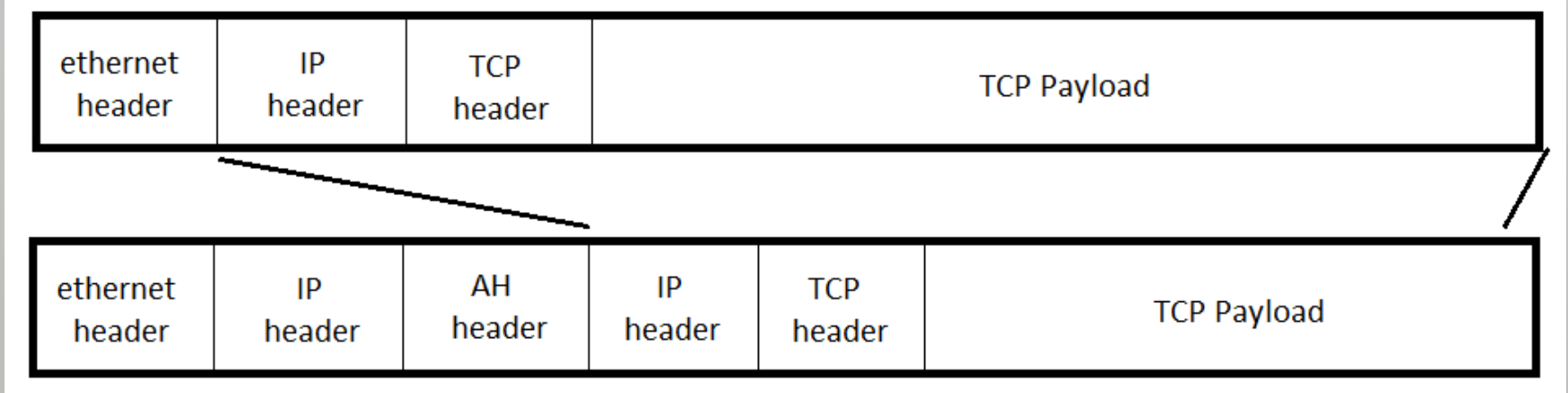
www.atris.sk

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 authentificating traffic only.

- ESP is used for encrypting traffic. ESP also can, but doesn't have to authentificate.
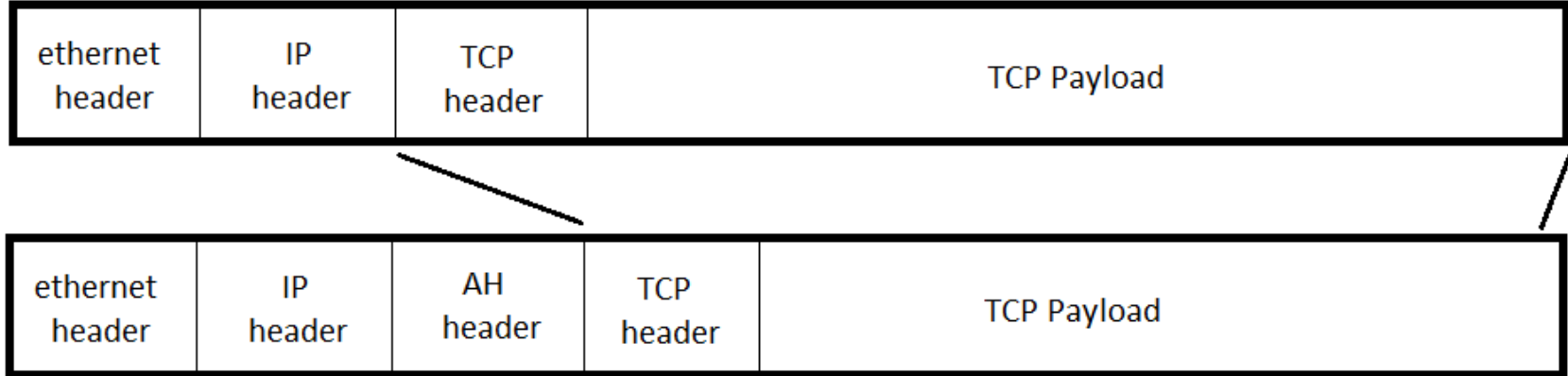
Tunnel mode

- The whole IP packet is encrypted.

ethernet header	IP header	TCP header	TCP Payload

ethernet header	IP header	AH header	IP header	TCP header	TCP Payload

- Therefore, tunnel mode can be used for VPN.

Transport mode

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

ethernet header	IP header	TCP header	TCP Payload

ethernet header	IP header	AH header	TCP header	TCP Payload

- 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 separatelly.

- 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 then the actual traffic encryption in Phase 2.

  *not how IKE actually works, simplified version

IPSec Peer – part 1

- 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
Lifebytes:

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.

www.atris.sk
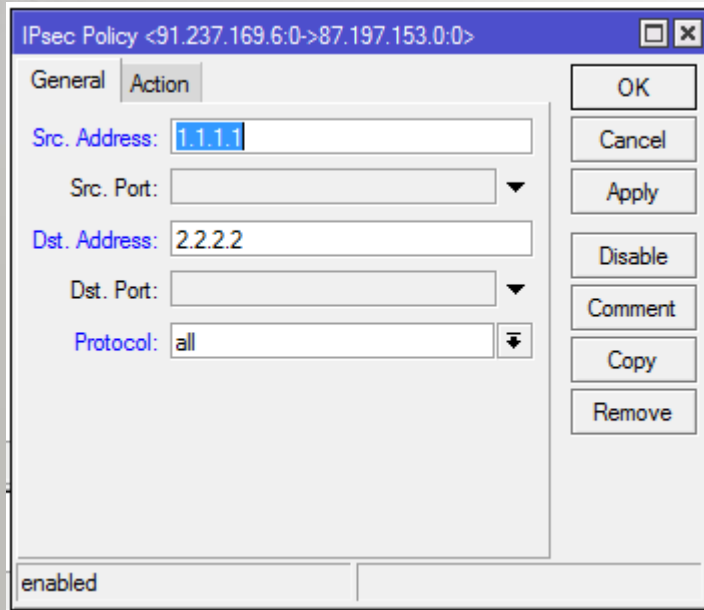
Configuring IPSec Phase 2

- 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.

www.atris.sk

IPSec policy – part 2
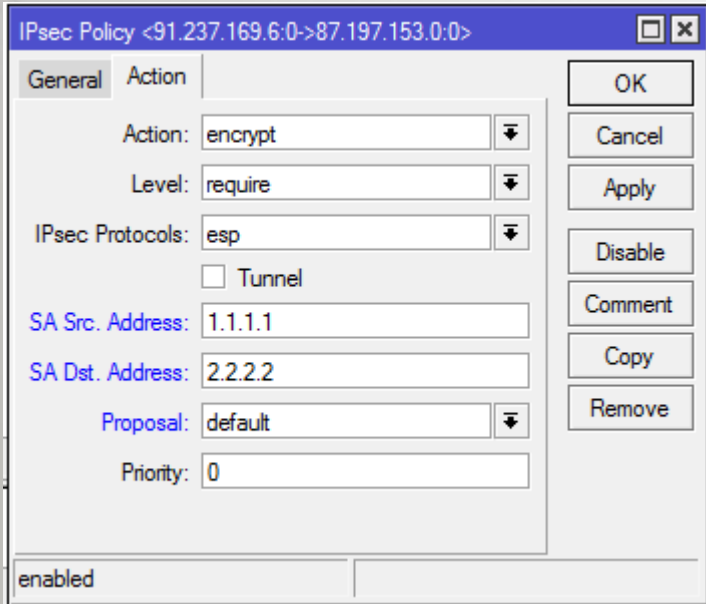
- Configure what to do with the traffic

    (encrypt using ESP Transport mode)
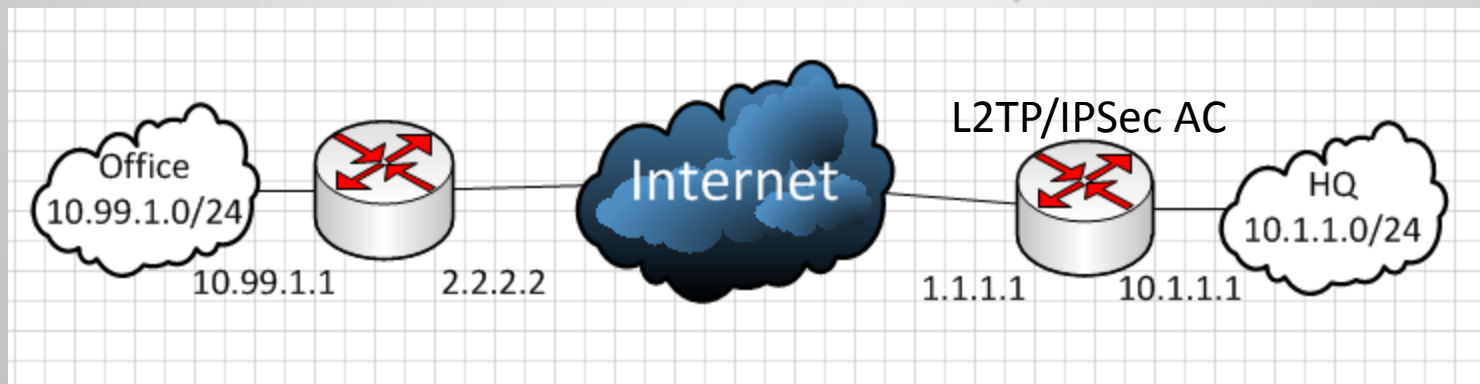

- Which SAs to use, and which proposal

www.atris.sk

IPSec proposal

- 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

www.atris.sk

Actual example topology

L2TP/IPSec AC

Office
10.99.1.0/24

Internet

HQ
10.1.1.0/24

10.99.1.1   2.2.2.2   1.1.1.1   10.1.1.1

*simplified network
for use in all next examples

www.atris.sk

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=sha1 lifetime=1h nat-traversal=yes secret=publicVPNaccess send-initial-contact=no
```


www.atris.sk

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
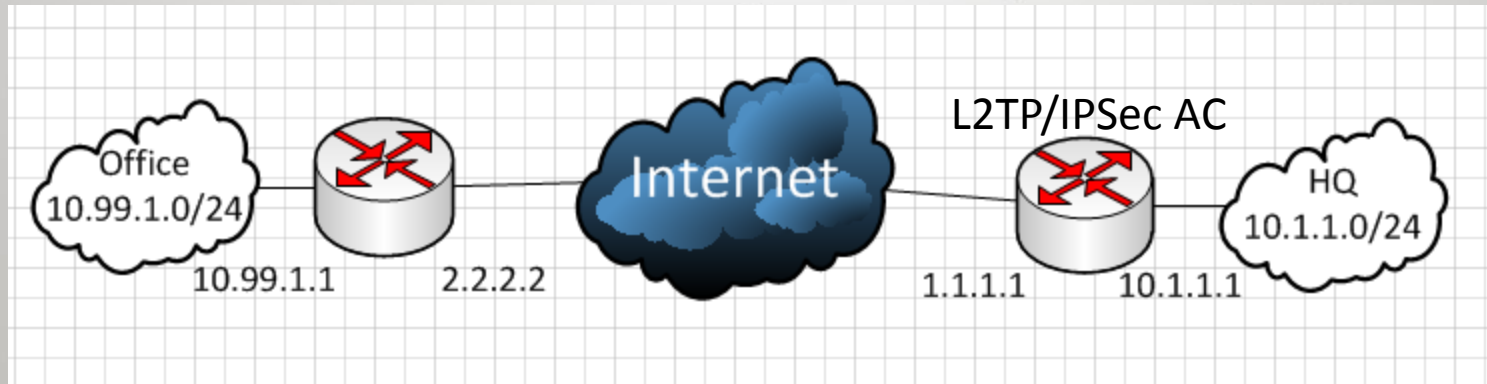Priority: 0

OK
Cancel
Apply
Disable
Comment
Copy
Remove

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.
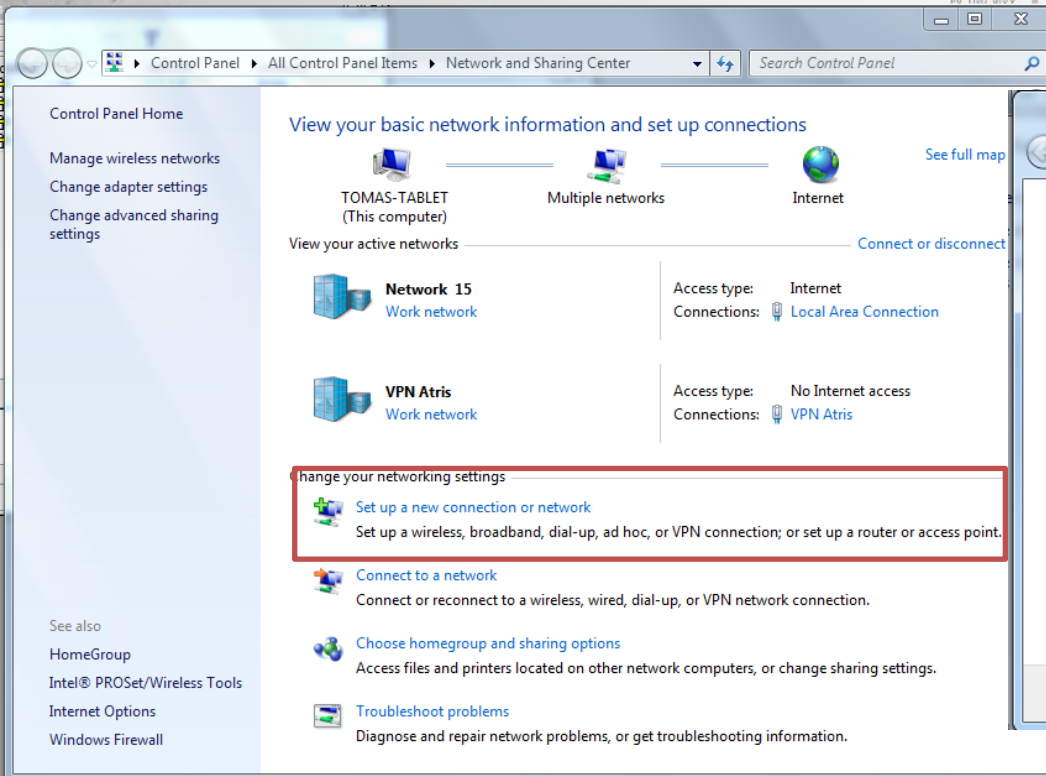
www.atris.sk

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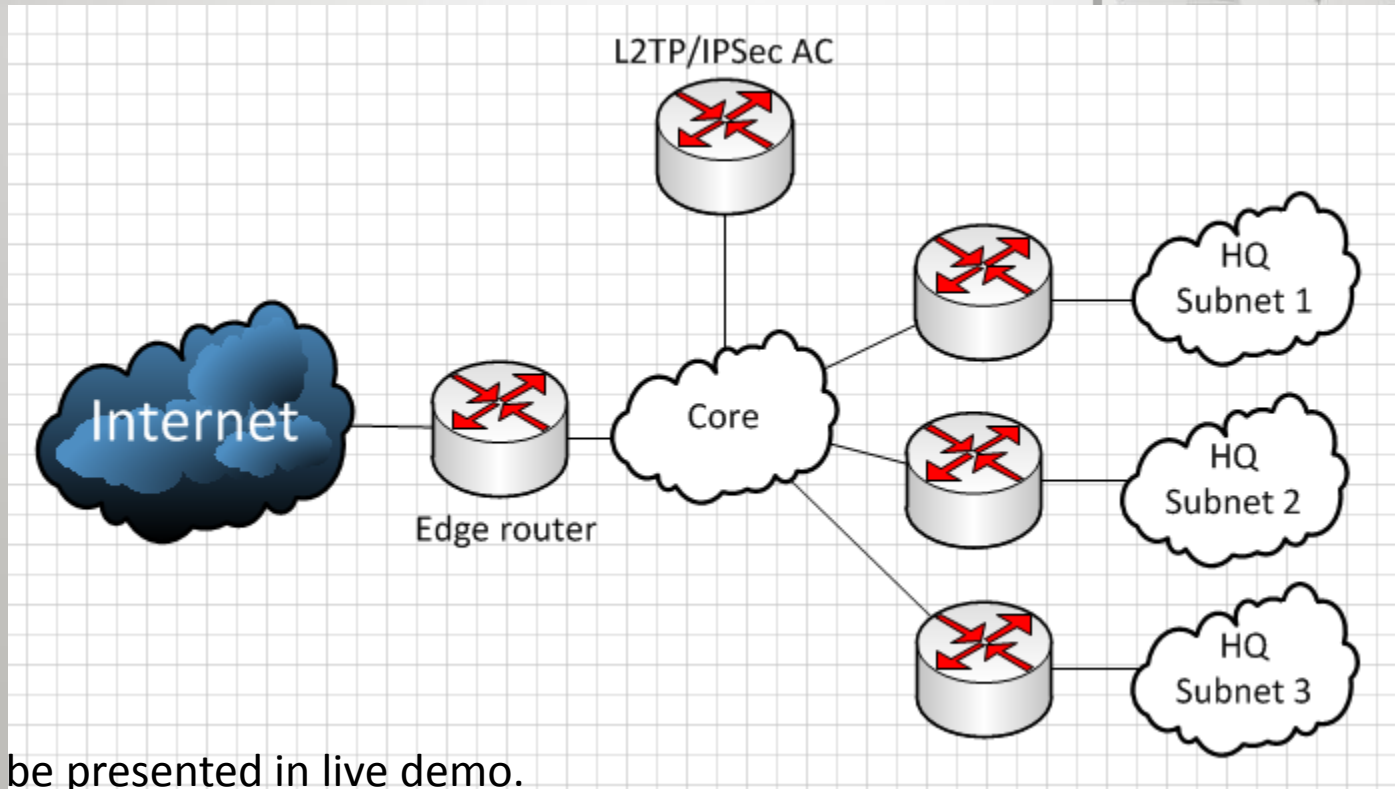
* This will be presented in live demo.
  The basic configuration of the AC is the same.

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…

www.atris.sk

L2TP/IPSec on Windows

www.atris.sk

Windows p.2

Windows p.3

L2TP credentials

www.atris.sk

Windows p.4

My corp VPN Properties

General | Options | Security | Networking | Sharing

Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec) ▼

[Advanced settings]

Data encryption:
Require encryption (disconnect if server declines) ▼

Authentication
○ Use Extensible Authentication Protocol (EAP)

[   ] ▼

[Properties]

● Allow these protocols

☐ Unencrypted password (PAP)
☑ Challenge Handshake Authentication Protocol (CHAP)
☑ Microsoft CHAP Version 2 (MS-CHAP v2)
☐ Automatically use my Windows logon name and password (and domain, if any)

[OK] [Cancel]

Advanced Properties

L2TP

● Use preshared key for authentication
    Key: [   ]

○ Use certificate for authentication
    ☐ Verify the Name and Usage attributes of the server's certificate

[OK] [Cancel]

Advanced TCP/IP Settings

IP Settings | DNS | WINS

This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

☐ Use default gateway on remote network
☐ Disable class based route addition

☑ Automatic metric
Interface metric: [   ]

Networking > IPv4 Properties > Advanced

[OK] [Cancel]

www.atris.sk

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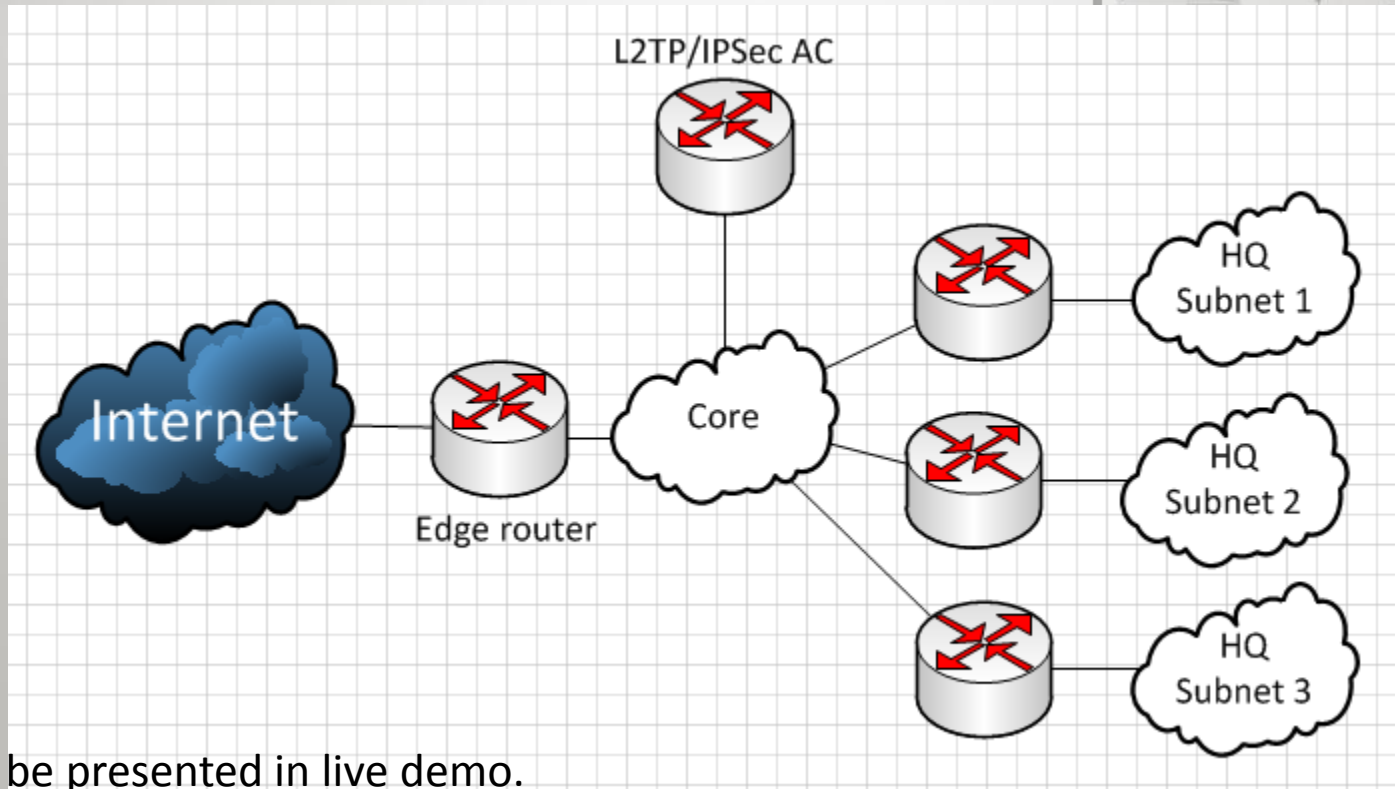
* This will be presented in live demo.
  The basic configuration of the AC is the same.

Live Demo

- Get to a server on corp LAN – 10.3.1.99

Mythbusters, IPSec edition

IPSec does not work through NAT.

Not true.
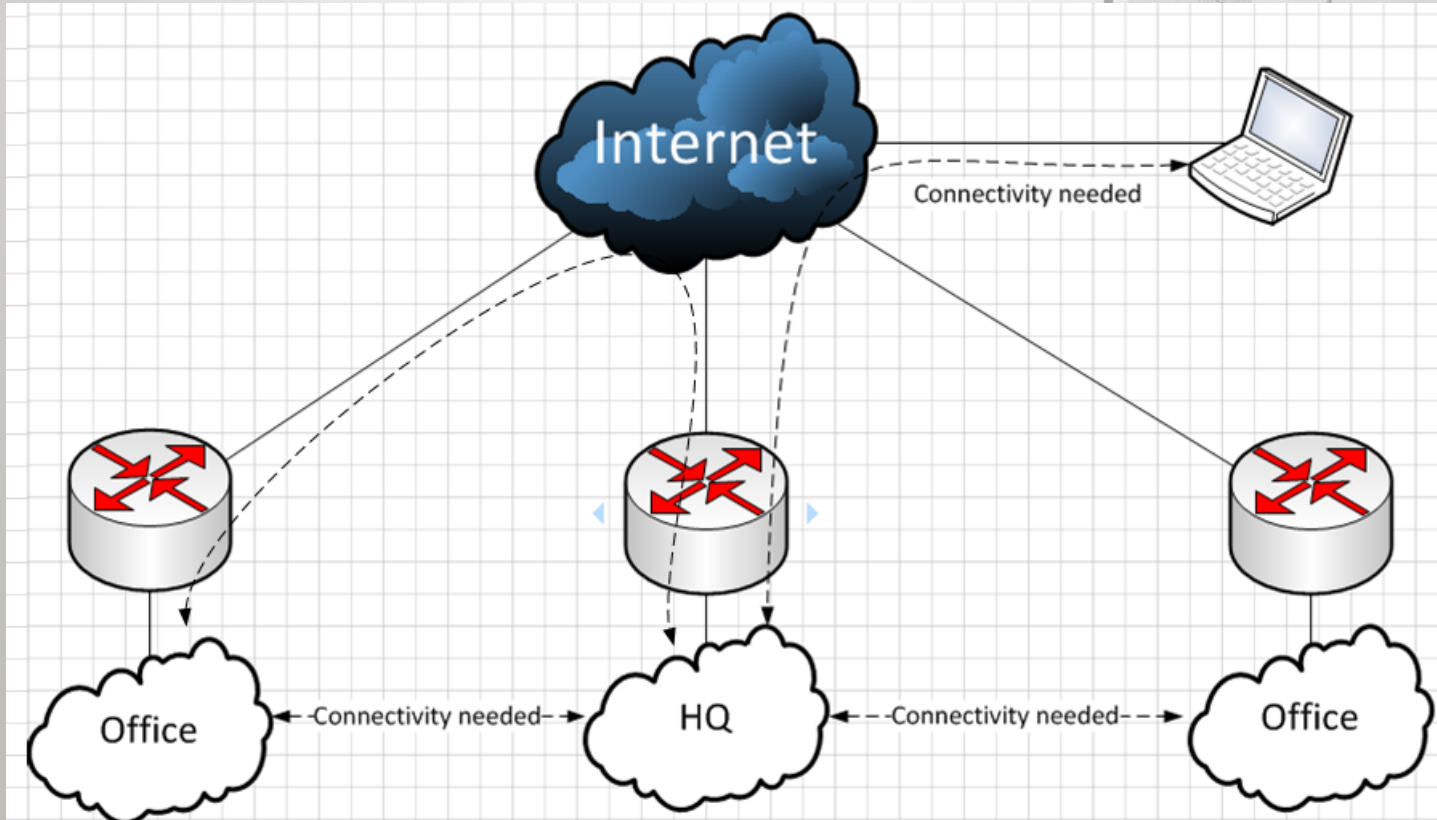
Live Demo

- 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.

www.atris.sk

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 <u>easily</u> script this functionality.

http://wiki.mikrotik.com/wiki/Securing_L2TP_Server_for_IPSec

www.atris.sk

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.

www.atris.sk

Resolution

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

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 deamon.

- You can not have more then 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.
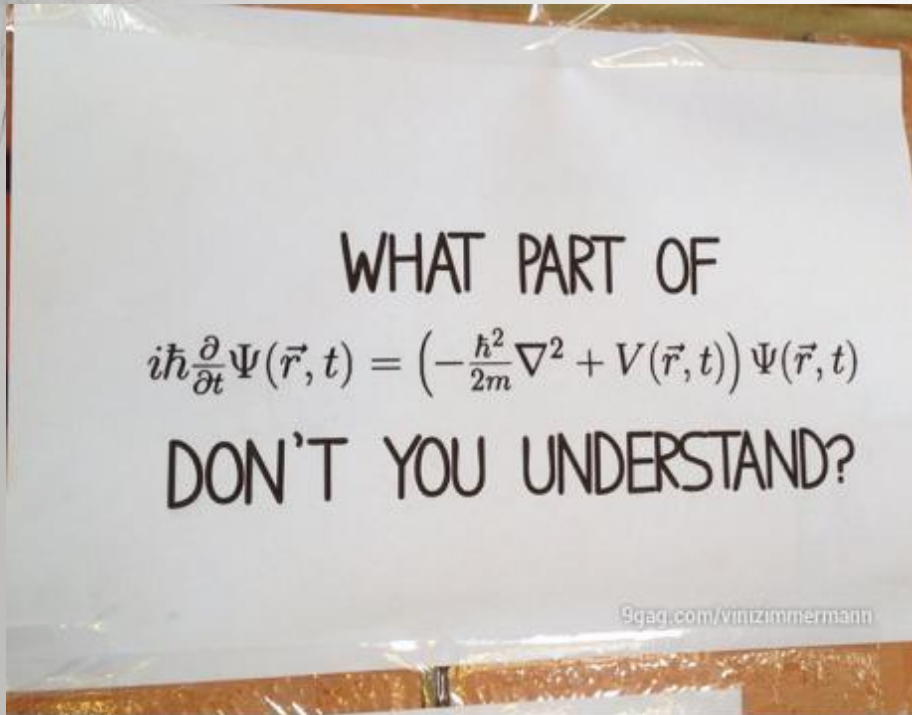
If you have any questions, please ask now, or find me after the presentation.

Thanks for listening

Tomas Kirnak

t.kirnak@atris.sk