

Deep-dive: IPSec & Xauth mode-config

Your guide to IPSec and VPNs

Presenter information

Tomas Kirnak

System Architect
Automation & Monitoring

MikroTik Certified Trainer
MikroTik Certified Consultant



Unimus

About Unimus

Disaster recovery
(configuration backup)

Configuration management
(change diffs, network-wide auditing, etc.)

Automation
(mass reconfiguration, config-push, etc.)



Unimus

Why are we talking about
IPSec Xauth mode-config?

Note for posterity

- If you find this presentation online in a .pdf, please watch the video
- Proper explanations to every slide and much more information available

<https://www.youtube.com/c/TomasKirnak/videos>

Presentation agenda

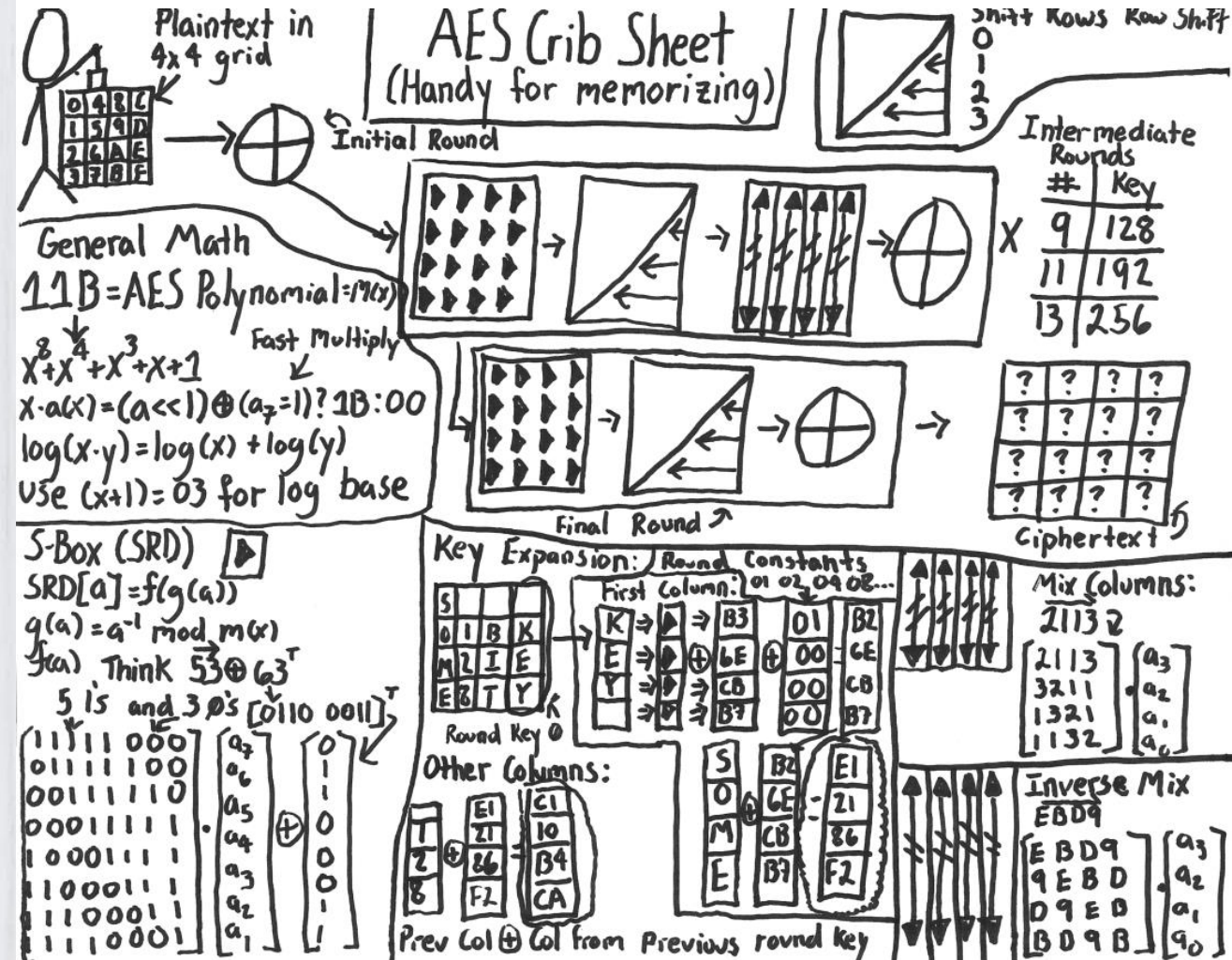
- How does IPSec work?
- Configuration examples
- Xauth mode-config vs. other options
- Configuring MikroTik AC
- Configuring client
- Security and other misc. bits

Before we start

- This presentation deals specifically with Road-Warriors (remote, roaming clients)
- Site-to-site tunneling should NOT use Xauth mode-config
- But what you learn about IPSec here will be useful for any (and all) IPSec- related things

How does IPsec work?

Part 1:



What is IPSec?

- IPSec is a standard for secure communication over public networks
- Specifically, IPSec allows us to ensure payload integrity, and / or encrypt the payload.

IPSec functions

- Integrity validation
IPSec AH (Authentication Header)
- Payload encryption (can also validate)
IPSec ESP (Encapsulating Security Payload)

IPSec session

- To provide these functions, and IPSec session needs to be established.
- To establish an IPSec session – 2 phases
 - Phase 1 – IKE – Internet Key exchange
 - Phase 2 – IPSec

IKE

- Phase 1 (IKE) is responsible for the initial IPSec session establishment
- After Phase 1 is successfully negotiated, the 2 peers can start sending IPSec traffic to each other
- To establish an IKE session, a shared secret is required (PSK, cert, key, etc.)

IPSec traffic

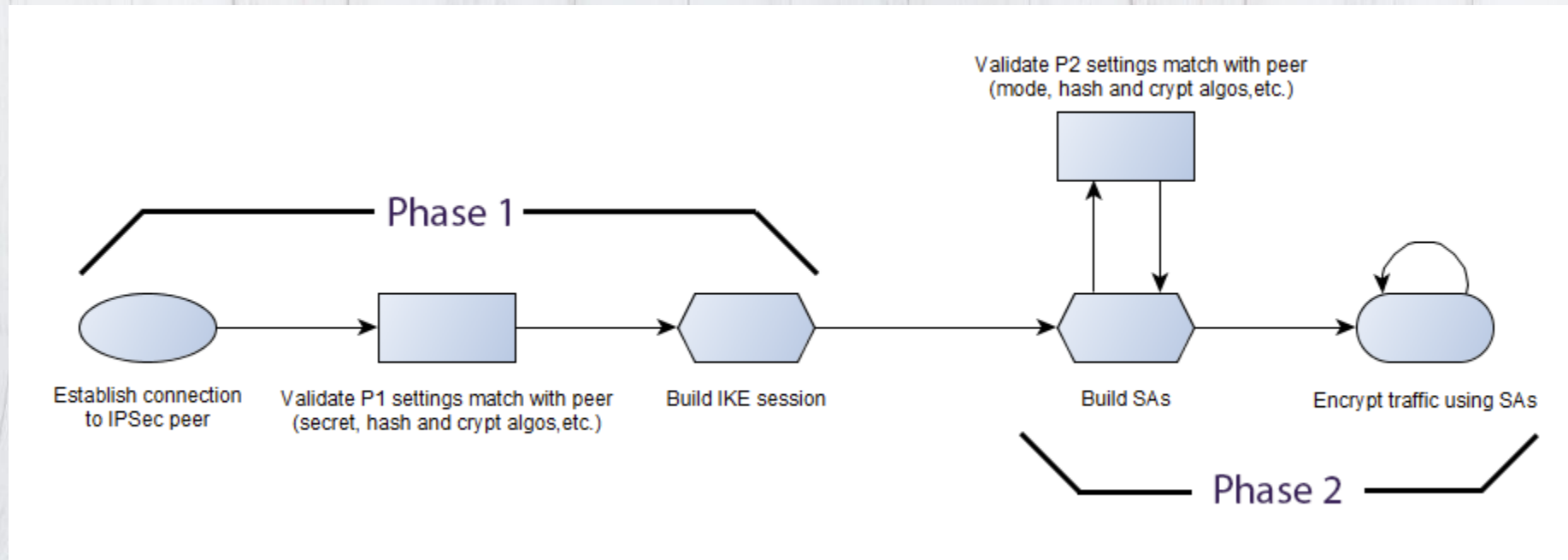
- IPSec policies are responsible for telling the IPSec service which traffic should be encrypted – and how.
- IPSec policies are like an IPSec routing table – they decide which traffic should go to what peer, and how it should be encrypted.

How is traffic encrypted?

- SAs (security associations) are responsible for encrypting traffic.
- After IKE is negotiated, SAs are built, and then traffic is encrypted.
- IPSec = not that hard right?

Visualizing IPSec

- Visualizing the IPSec process



- Note: this is vastly simplified

In RouterOS

- Please note, that in RouterOS, having some matching traffic is required for the IPSec process to kick in.
- In other words, there needs to be some traffic matching an IPSec policy, before anything is done.

Closer look at Phase 2

- Lets take a closer look at Phase 2, and the IPSec policies.
- IPSec policies dictate:
 - What traffic is to be processed by IPSec
 - To which peer should the traffic go
 - What to do with the traffic (auth vs. crypt)
 - How to process the traffic (transport vs. tunnel mode)

IPSec modes

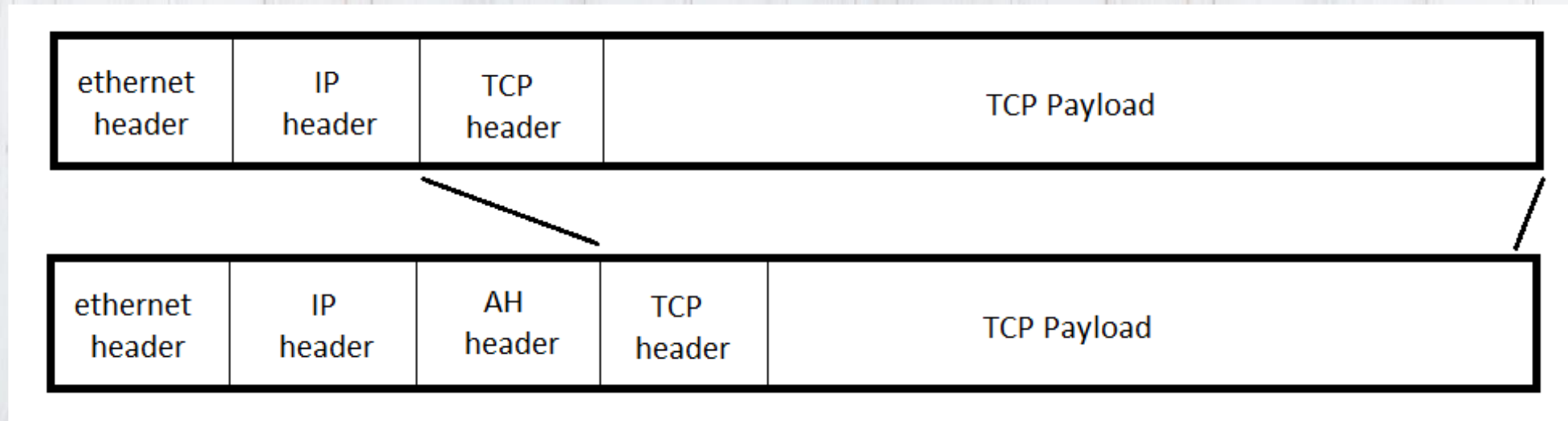
- We mentioned modes (transport vs. tunnel), lets talk about this
- IPSec Phase 2 supports 2 modes:
 - Transport mode
 - Tunnel mode

Transport vs. Tunnel

- Transport mode
 - Secures a data stream
 - Encapsulates L4 datagram
- Tunnel mode
 - Tunnels traffic
 - Encapsulates entire L3 packet

Transport mode

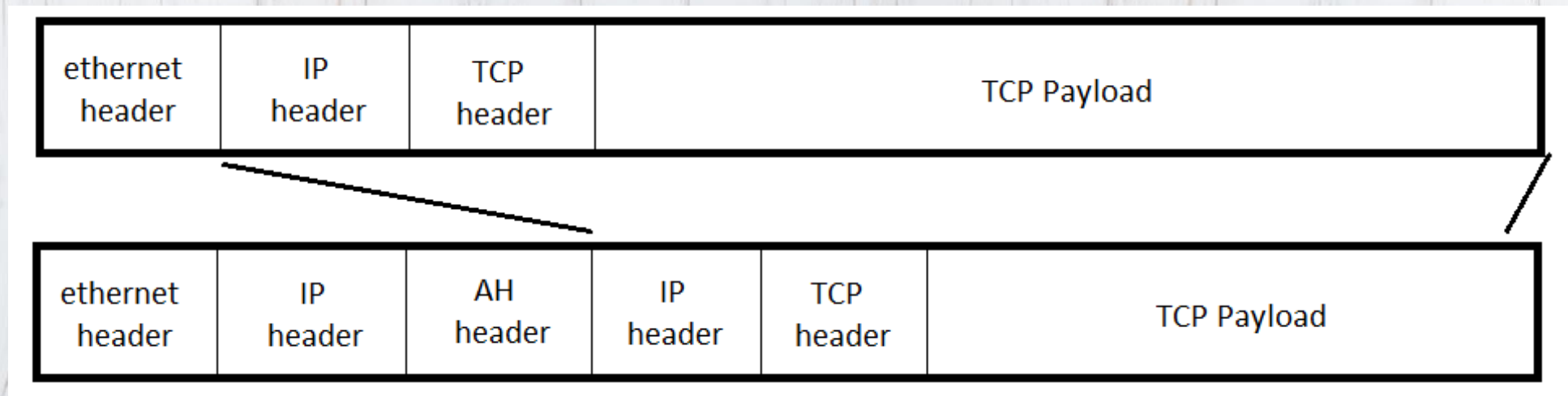
- Only the payload of the packet is encapsulated and secured



- Transport mode is used to secure host-to-host / end-to-end traffic

Tunnel mode

- The whole IP packet is encrypted



- Therefore, tunnel mode can be used for VPN by itself

Last part

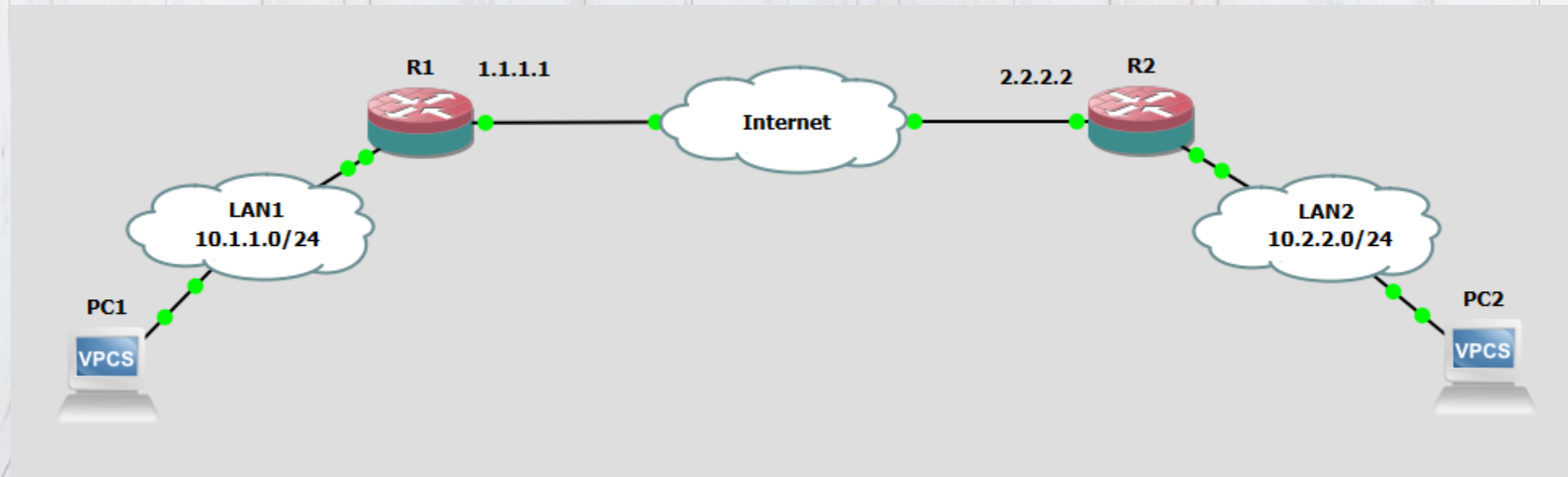
- IPSec proposal – crypt configuration
- This tells RouterOS which crypto / hashing algorithms to use on our traffic
- Basically – how secure do we want this VPN to be

RouterOS sum-up

- `/ip ipsec peer`
Defines Phase 1 settings for our our IPSec peers
- `/ip ipsec policy`
Defines what traffic to process, and how to process it
- `/ip ipsec proposal`
Defines what crypto / hashing algos to use

Let's see an example

- To understand this, let's visualize it:



- Basic site-to-site VPN

In tunnel mode

R1

```
# create peer (Phase 1)
/ip ipsec peer
add address=2.2.2.2/32 dh-group=modp2048
dpd-interval=10s dpd-maximum-failures=3 enc-
algorithm=aes-256 hash-algorithm=sha512
secret=superSecret

# create policy (Phase 2)
/ip ipsec policy
add dst-address=10.2.2.0/24 sa-dst-address=2.2.2.2
sa-src-address=1.1.1.1 src-address=10.1.1.0/24
tunnel=yes

# traffic in IPSec tunnel must not be NATed
/ip firewall nat
add action=accept chain=srcnat dst-
address=10.2.2.0/24
```

R2

```
# create peer (Phase 1)
/ip ipsec peer
add address=1.1.1.1/32 dh-group=modp2048 dpd-
interval=10s dpd-maximum-failures=3 enc-
algorithm=aes-256 hash-algorithm=sha512
secret=superSecret

# create policy (Phase 2)
/ip ipsec policy
add dst-address=10.1.1.0/24 sa-dst-address=1.1.1.1
sa-src-address=2.2.2.2 src-address=10.2.2.0/24
tunnel=yes

# traffic in IPSec tunnel must not be NATed
/ip firewall nat
add action=accept chain=srcnat dst-
address=10.1.1.0/24
```

In transport mode

R1

```
# IPsec setup
/ip ipsec peer
add address=2.2.2.2/32 dh-group=modp2048 dpd-
interval=10s dpd-maximum-failures=3 enc-algorithm=aes-
256 hash-algorithm=sha512 secret=superSecret
/ip ipsec policy
add dst-address=2.2.2.2/32 protocol=gre src-
address=1.1.1.1/32

# GRE to tunnel the traffic
/interface gre
add clamp-tcp-mss=no dont-fragment=inherit
keepalive=10s,3 mtu=1400 name=gre-tunnel1 remote-
address=2.2.2.2

# routing
/ip address
add address=10.255.0.1/24 interface=gre-tunnel1
/ip route
add distance=1 dst-address=10.2.2.0/24 gateway=10.255.0.2
```

R2

```
# IPsec setup
/ip ipsec peer
add address=1.1.1.1/32 dh-group=modp2048 dpd-
interval=10s dpd-maximum-failures=3 enc-algorithm=aes-
256 hash-algorithm=sha512 secret=superSecret
/ip ipsec policy
add dst-address=1.1.1.1/32 protocol=gre src-
address=2.2.2.2/32

# GRE to tunnel the traffic
/interface gre
add clamp-tcp-mss=no dont-fragment=inherit
keepalive=10s,3 mtu=1400 name=gre-tunnel1 remote-
address=1.1.1.1

# routing
/ip address
add address=10.255.0.2/24 interface=gre-tunnel1
/ip route
add distance=1 dst-address=10.1.1.0/24 gateway=10.255.0.1
```

Note on the setups

- In previous setups, we used the default proposal
- Please note the default should be adjusted for better security

adjust how traffic is encrypted

/ip ipsec proposal

set [find default=yes] auth-algorithms=sha256 enc-algorithms=aes-128-cbc
pfs-group=modp2048

Tunnel vs. Transport 2

- So what should you use for site-to-site VPNs?
- If possible, always use IPSec transport mode, with an underlying tunnel
- Why – because you get an interface
(IPSec policies to drive traffic in Tunnel mode aren't an interface)
- Having an interface allows you to do OSPF, torch, easier firewalling, etc.

Part 2:

What about
road warriors?



Oh what a day...

- Previous cases dealt with a site-to-site VPN
- However, just as often we need to support Road-Warriors - remote, roaming clients
- This means we now want a client-to-site setup
- This is not a network anymore, just a single client – often behind NAT

Our options

- We have multiple options here:
 - PPTP (please don't)
 - SSTP
 - OVPN
 - L2TP / IPSec
 - IPSec Xauth mode-config
 - IKEv2

Why Xauth mode-config?

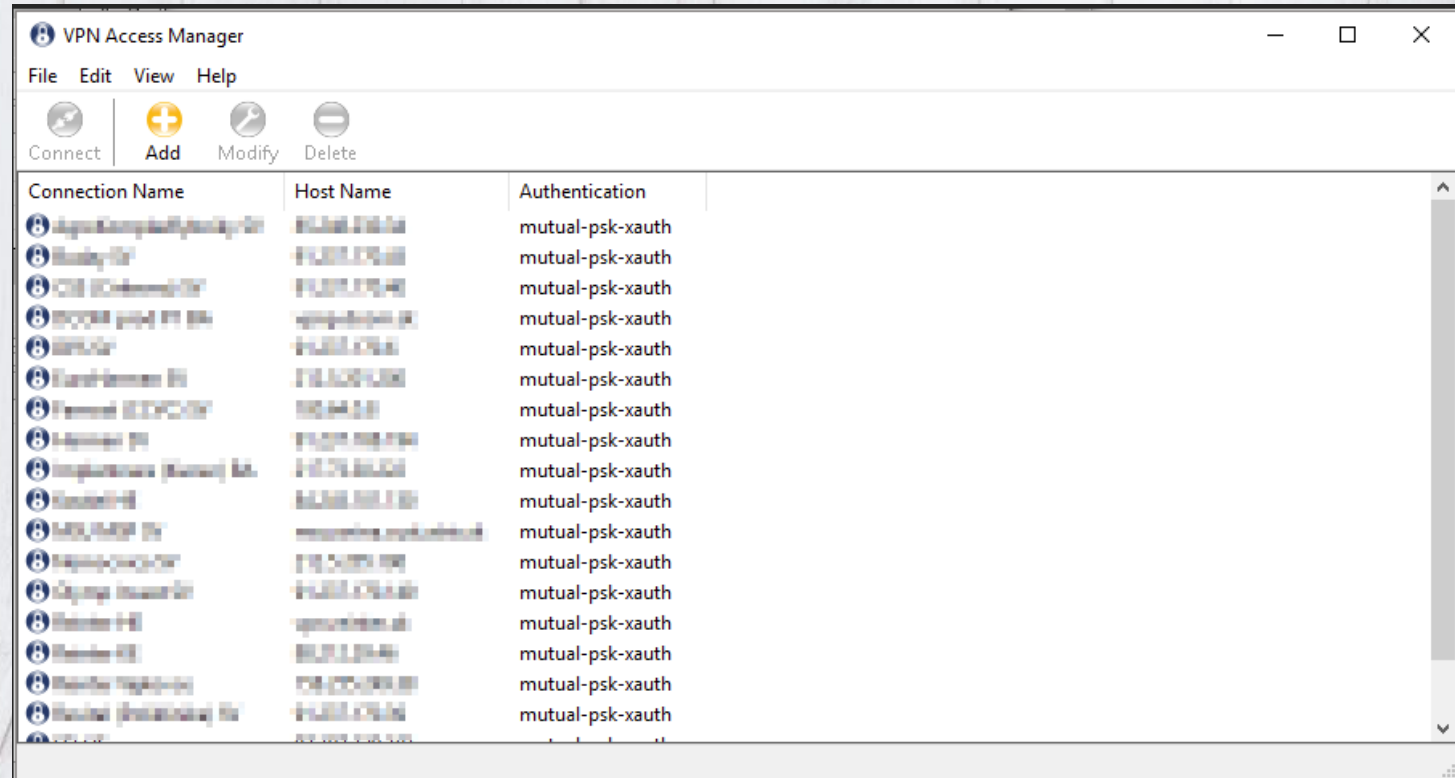
- Support in ALL major OS (including mobile)
- Not TCP-based
- Support for keys, certs or a PSK
- Configuration push
Routes, DNS, etc.
- GREAT free client software
Shrew VPN client

What do road-warriors need?

- We really really want to push settings to road-warriors
- Specifically:
 - Routes (which traffic should go to VPN)
 - DNS (so they can resolve local hostnames)
- Let's discuss why...

Managing VPNs...

- Having the ability to export / import VPN profiles is a great time-saving feature
- Imagine having to configure this manually
- Sending a profile file to import for a non-IT user is MUCH easier than configuring the OS-included VPN



Which client to use?

- We will be using Shrew VPN client for the rest of this presentation
- Great, free, available for all major OS
TONS of features, support for all we need here
- On mobile, use the OS built-in client

How to configure this?

- Let's see how to configure an Xauth mode-config AC on RouterOS

The image displays three sequential screenshots of the 'New IPsec Peer' configuration window in RouterOS, illustrating the steps to configure an Xauth mode-config AC.

General Tab:

- Address: 0.0.0.0/0
- Port: (empty)
- Local Address: (empty)
- Auth. Method: pre shared key xauth
- Exchange Mode: main
- ☒ Passive
- Secret: thisIsSuperSecret
- XAuth Login: (empty)
- XAuth Password: (empty)
- enabled responder

Advanced Tab:

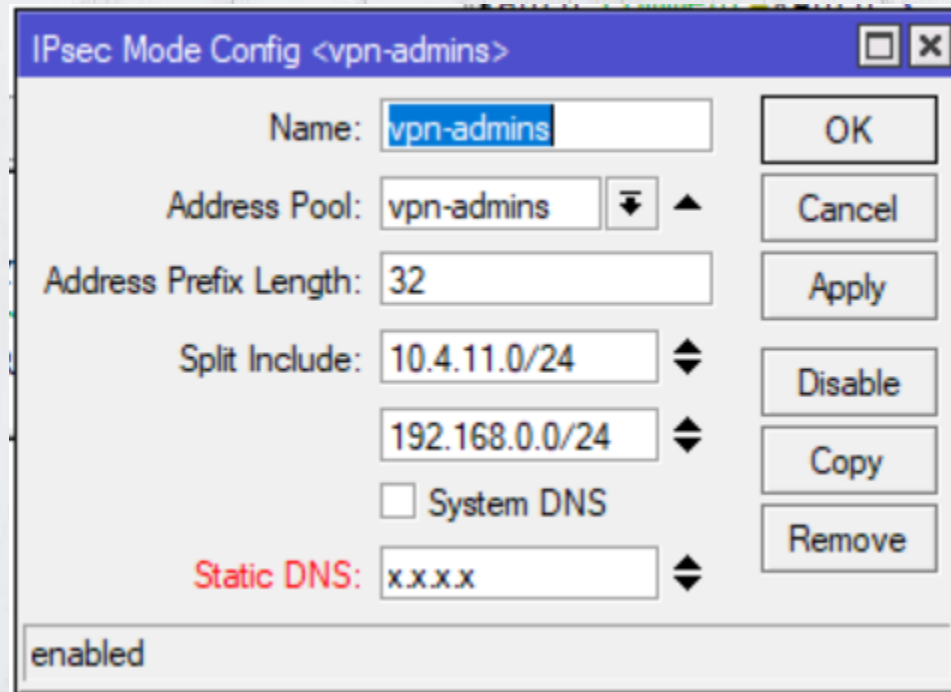
- Policy Template Group: default
- ☐ Send Initial Contact
- ☒ NAT Traversal
- My ID Type: auto
- Mode Configuration: vpn-admins
- Generate Policy: port strict
- Lifetime: 1d 00:00:00
- Lifeytes: (empty)
- DPD Interval: 10 s
- DPD Maximum Failures: 3
- Proposal Check: obey
- Compatibility Options: ☐ skip peer id validation
- enabled responder

Encryption Tab:

- Hash Algorithm: sha512
- Encryption Algorithm:
 - ☐ des
 - ☐ 3des
 - ☐ aes-128
 - ☐ aes-192
 - ☒ aes-256
 - ☐ blowfish
 - ☐ camellia-128
 - ☐ camellia-192
 - ☐ camellia-256
- DH Group:
 - ☐ modp768
 - ☐ modp1024
 - ☐ ec2n155
 - ☐ ec2n185
 - ☐ modp1536
 - ☒ modp2048
 - ☐ modp3072
 - ☐ modp4096
 - ☐ modp6144
 - ☐ modp8192
- OK, Cancel, Apply, Disable, Comment, Copy, Remove buttons
- enabled responder

How to push config to clients

- To push config to clients, we just need to specify a mode-config config



The screenshot shows a Windows-style dialog box titled "IPsec Mode Config <vpn-admins>". It contains several input fields and a list of buttons. The "Name" field is set to "vpn-admins". The "Address Pool" is a dropdown menu showing "vpn-admins". The "Address Prefix Length" is set to "32". The "Split Include" section has two entries: "10.4.11.0/24" and "192.168.0.0/24", each with a double-headed arrow icon. There is an unchecked checkbox for "System DNS". The "Static DNS" field is set to "x.x.x.x" and has a red label. On the right side, there are buttons for "OK", "Cancel", "Apply", "Disable", "Copy", and "Remove". At the bottom left, the status "enabled" is displayed.

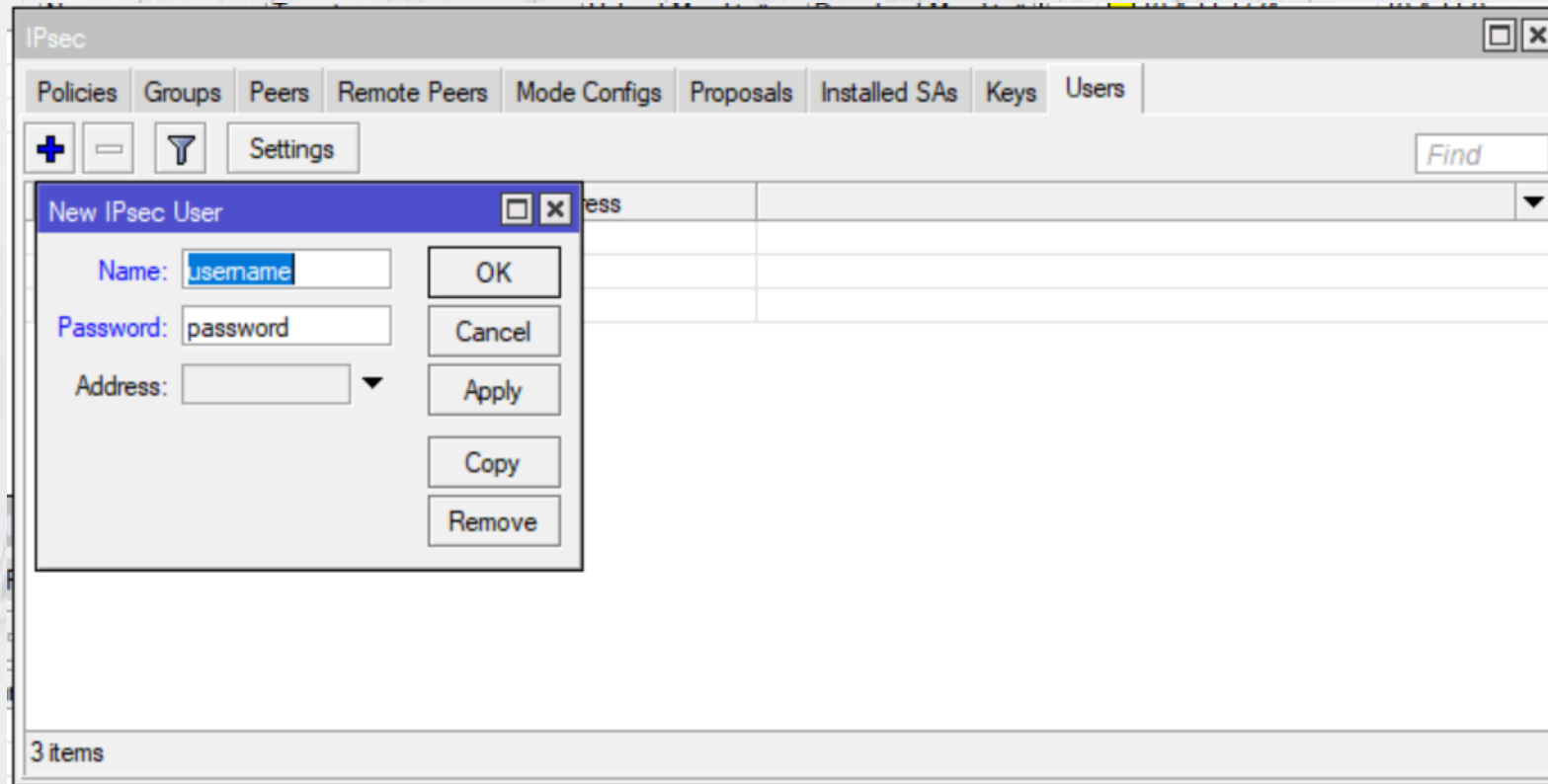
Name:	vpn-admins	OK
Address Pool:	vpn-admins	Cancel
Address Prefix Length:	32	Apply
Split Include:	10.4.11.0/24	Disable
	192.168.0.0/24	Copy
	☐ System DNS	Remove
Static DNS:	x.x.x.x	
enabled		

What about IPSec policy?

- Policy will be generated automatically
- `generate-policy=port-strict` in the Peer configuration will take care of this

Last step – our warriors

Now we can generate our Xauth users:



You can also do Radius auth!

Full AC config

```
# Peer
/ip ipsec peer
add address=0.0.0.0/0 auth-method=pre-shared-key-xauth dpd-interval=10s dh-group=modp2048
dpd-maximum-failures=3 enc-algorithm=aes-256 generate-policy=port-strict hash-algorithm=sha512
mode-config=vpn-admins passive=yes secret=ipsec-secret send-initial-contact=no
```

```
# mode-config
/ip pool
add name=vpn-admins ranges=10.255.254.0/24

/ip ipsec mode-config
add address-pool=vpn-admins name=vpn-admins split-include=10.4.11.0/24,192.168.0.0/24 system-
dns=no dns=x.x.x.x
```

```
# user
/ip ipsec user
add name=username password=password
```

```
# adjust how traffic is encrypted
/ip ipsec proposal
set [ find default=yes ] auth-algorithms=sha256 enc-algorithms=aes-128-cbc pfs-group=modp2048
```

How to configure client 1

The image displays three sequential screenshots of the 'VPN Site Configuration' window, illustrating the configuration steps for 'client 1'.

First Screenshot (General Tab):

- Remote Host:** Host Name or IP Address is 'ac.ip.address', Port is '500', and Auto Configuration is set to 'ike config pull'.
- Local Host:** Adapter Mode is 'Use a virtual adapter and assigned address', MTU is '1300', and 'Obtain Automatically' is checked for the Address field.

Second Screenshot (Firewall Options Tab):

- Firewall Options:** NAT Traversal is 'enable', NAT Traversal Port is '4500', Keep-alive packet rate is '10' Secs, IKE Fragmentation is 'disable', and Maximum packet size is '1000' Bytes.
- Other Options:** 'Enable Dead Peer Detection' and 'Enable ISAKMP Failure Notifications' are checked, while 'Enable Client Login Banner' is unchecked.

Third Screenshot (DNS Tab):

- DNS:** 'Enable DNS' and 'Obtain Automatically' are checked. Server Address #1 through #4 are empty, and the DNS Suffix is empty.

How to configure client 2

The image displays three sequential screenshots of the 'VPN Site Configuration' dialog box, illustrating the steps to configure 'client 2'.

First Screenshot (Authentication Tab): The 'Authentication' tab is selected. The 'Authentication Method' is set to 'Mutual PSK + XAuth'. Under the 'Local Identity' sub-tab, the 'Identification Type' is set to 'IP Address'. The 'Address String' field is empty. The checkbox 'Use a discovered local host address' is checked. 'Save' and 'Cancel' buttons are at the bottom.

Second Screenshot (Name Resolution Tab): The 'Name Resolution' tab is selected. The 'Authentication Method' remains 'Mutual PSK + XAuth'. Under the 'Local Identity' sub-tab, the 'Identification Type' is set to 'Any'. The 'Address String' field is empty. 'Save' and 'Cancel' buttons are at the bottom.

Third Screenshot (Credentials Tab): The 'Credentials' tab is selected. The 'Authentication Method' remains 'Mutual PSK + XAuth'. Fields for 'Server Certificate Authority File', 'Client Certificate File', and 'Client Private Key File' are shown, each with a browse button (...). The 'Pre Shared Key' field contains a series of 12 black dots. 'Save' and 'Cancel' buttons are at the bottom.

How to configure client 3

The image displays three sequential screenshots of the 'VPN Site Configuration' window, illustrating the configuration steps for client 3. Each window has tabs for 'Authentication', 'Phase 1', 'Phase 2', and 'Policy'.

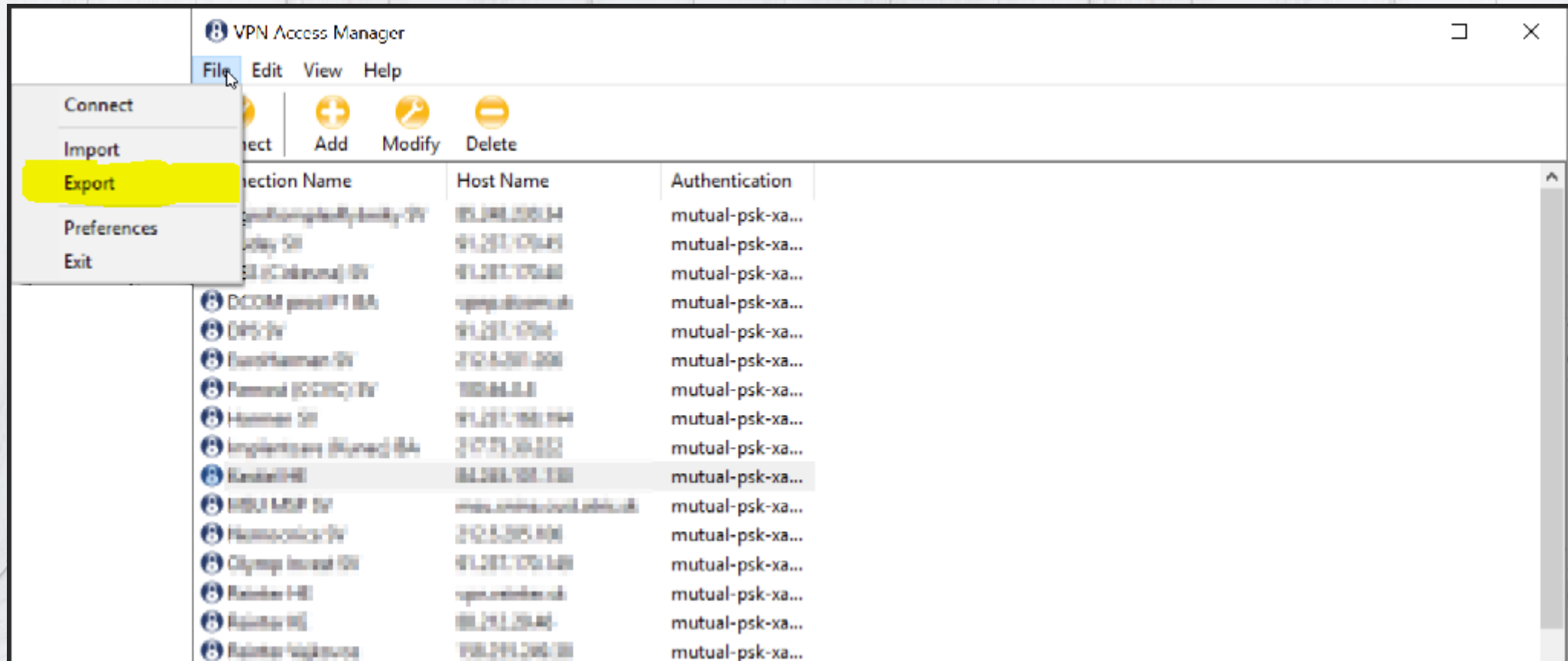
First Screenshot (Phase 1 tab): The 'Proposal Parameters' section is visible. The 'Exchange Type' is set to 'main'. The 'DH Exchange' is set to 'group 14'. The 'Cipher Algorithm' is set to 'aes'. The 'Cipher Key Length' is set to '256' Bits. The 'Hash Algorithm' is set to 'sha2-512'. The 'Key Life Time limit' is set to '86400' Secs. The 'Key Life Data limit' is set to '0' Kbytes. There is an unchecked checkbox for 'Enable Check Point Compatible Vendor ID'.

Second Screenshot (Phase 2 tab): The 'Proposal Parameters' section is visible. The 'Transform Algorithm' is set to 'esp-aes'. The 'Transform Key Length' is set to '128' Bits. The 'HMAC Algorithm' is set to 'sha2-256'. The 'PFS Exchange' is set to 'group 14'. The 'Compress Algorithm' is set to 'disabled'. The 'Key Life Time limit' is set to '3600' Secs. The 'Key Life Data limit' is set to '0' Kbytes.

Third Screenshot (Policy tab): The 'IPSEC Policy Configuration' section is visible. The 'Policy Generation Level' is set to 'unique'. There are two checkboxes: 'Maintain Persistent Security Associations' (unchecked) and 'Obtain Topology Automatically or Tunnel All' (checked). Below these is a 'Remote Network Resource' section with a large empty box and three buttons: 'Add', 'Modify', and 'Delete'.

Export config

- Export your config, send it to the Road Warrior



Part 3:

Security and other misc. bits

Error 404
Funny image not found...

Firewall rules

- Firewall input rules to allow IPSec traffic are simple

```
add action=accept chain=inut comment=IKE  
dst-port=500 protocol=udp
```

```
add action=accept chain=inut comment=NAT-T  
dst-port=4500 protocol=udp
```

```
add action=accept chain=input protocol=ipsec-esp
```

Routing note

- If you have a bigger routed network (OSPF, BGP, whatever) remember to add proper routes
- IPSec policies will route traffic on the AC, but the rest of the network has to know that traffic for IPSec road-warriors (the IP pool) needs to be routed to the AC

Where to learn more?

- Basics of encryption
<https://youtu.be/12Q3Mrh03Gk>
https://youtu.be/NOs34_-eREk
- How does Diffie-Hellman work?
https://youtu.be/ESPT_36pUFc
- How does AES work?
<http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html>

Additional resources

Things to watch/listen to

My other presentations and talks

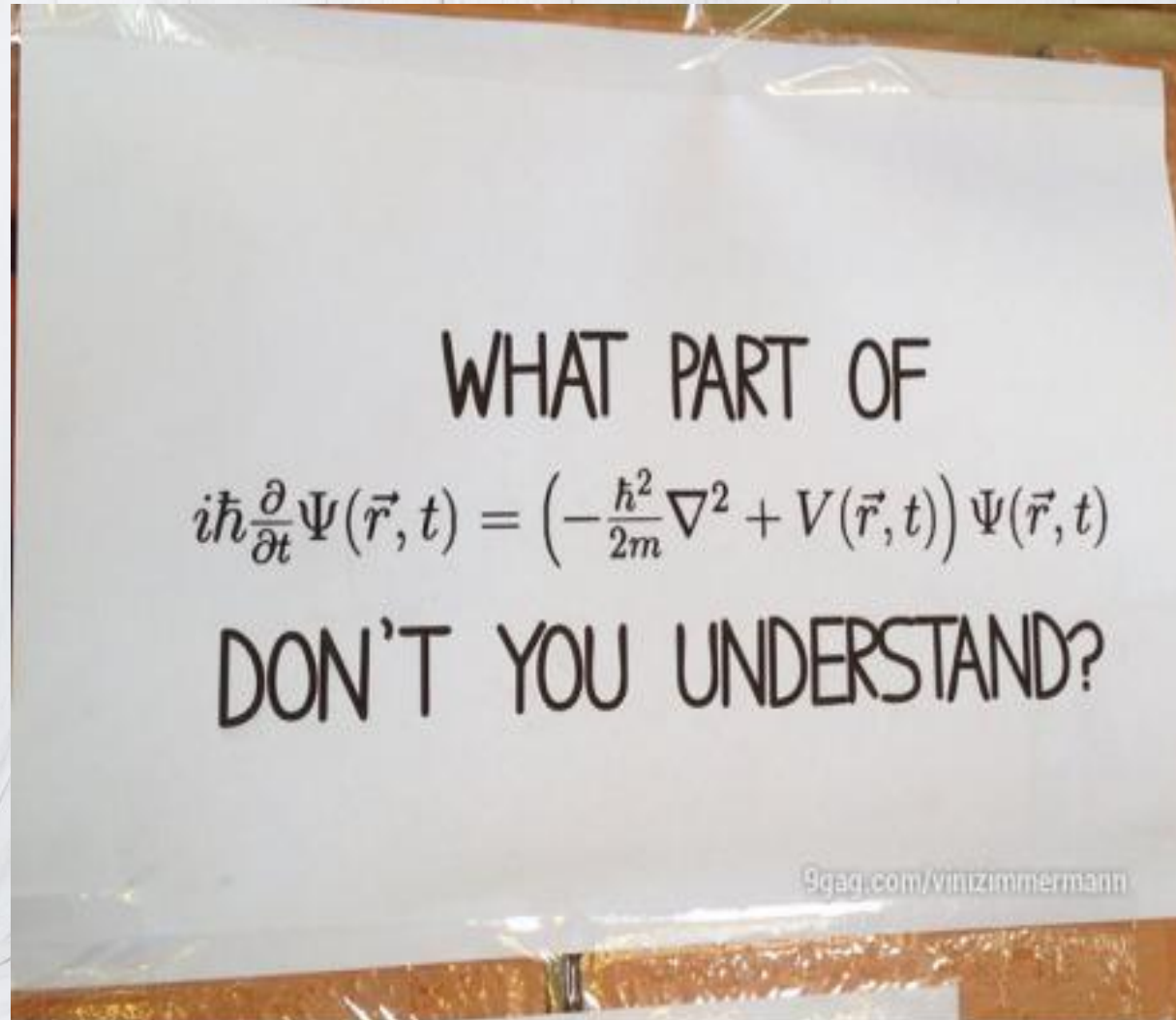
- Find all my other MUM presentations and more on:
<https://www.youtube.com/c/TomasKirnak/videos>

Load Balancing / Mangle deep dive
L2TP / IPSec deep dive
MLPS / VPLS / MTU deep dive
Monitoring / SNMP deep dive
Automation deep-dive
etc.

TheBrothersWISP

- I am a part of The Brothers WISP
- We do a bi-weekly networking podcast
<http://thebrotherswisp.com>
- Give us a listen if you feel like it!

Thank you very much for your attention!



Tomas Kirnak
tomas@unimus.net