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

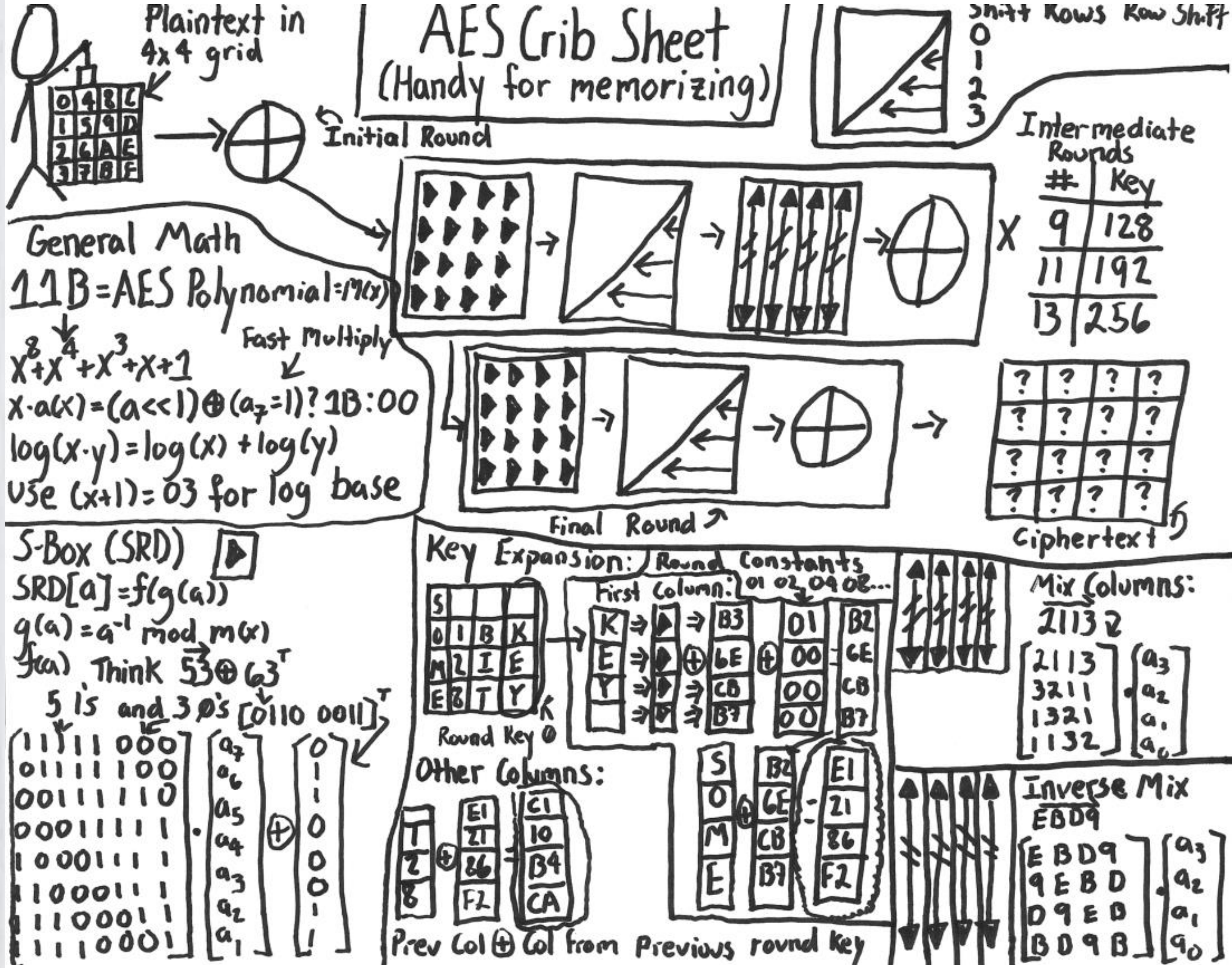
- This presentation deals specifically with Road-Warriors (remote, roaming clients)

- 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

Part 1:

How does IPSec work?



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.

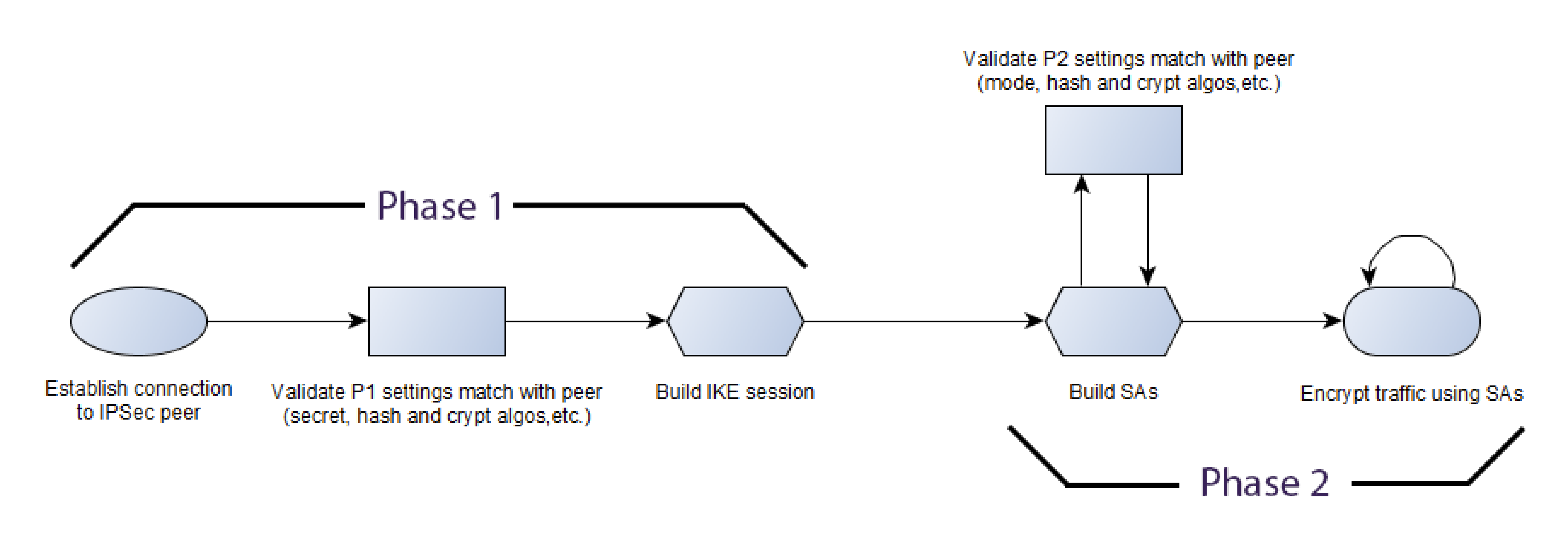
- IPSec policies are like an IPSec routing table – they decide which traffic should go to what peer, and how it should be encrypted.

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


Validate P2 settings match with peer
(mode, hash and crypt algos,etc.)
Phase 1
Establish connection
to IPSec peer
Validate P1 settings match with peer
(secret, hash and crypt algos,etc.)
Build IKE session
Build SAs
Encrypt traffic using SAs
Phase 2

- 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

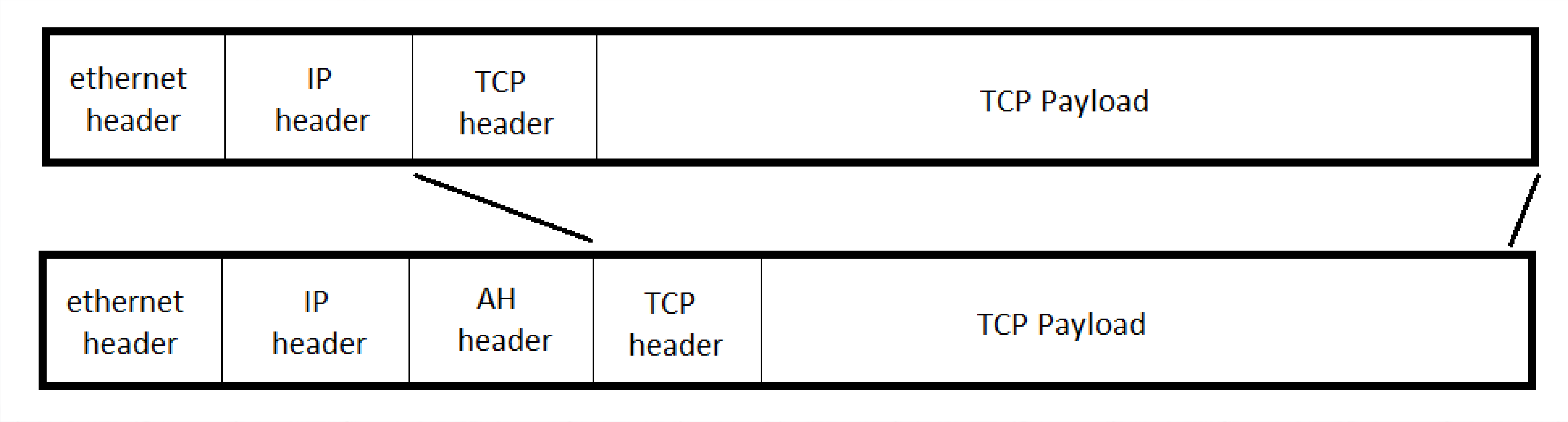
- IPSec Phase 2 supports 2 modes:
  Transport mode
  Tunnel mode

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 packed is encapsulated and secured



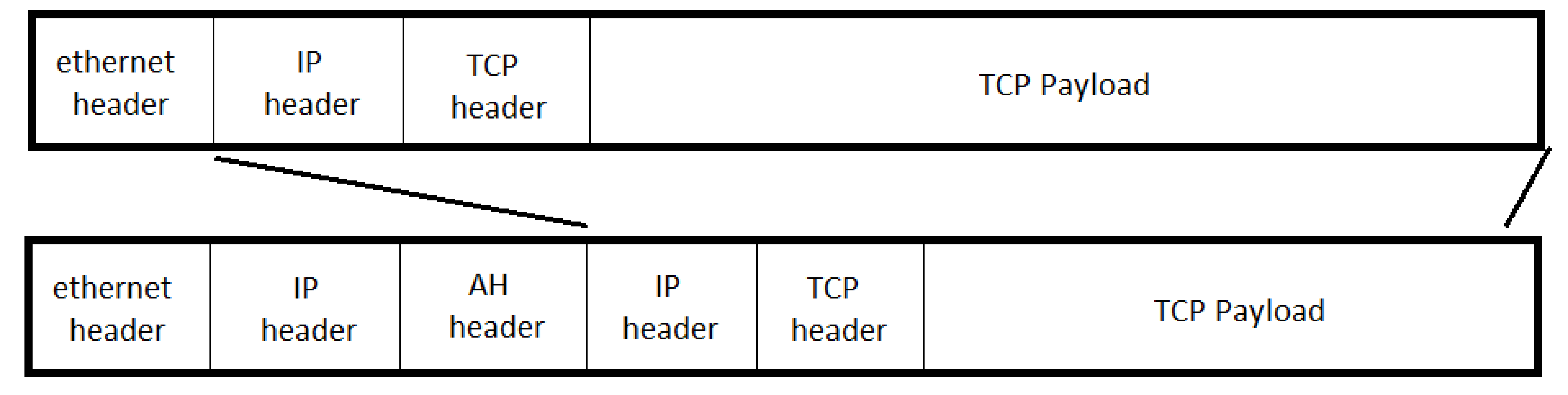
ethernet header | IP header | TCP header | TCP Payload

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

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

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 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

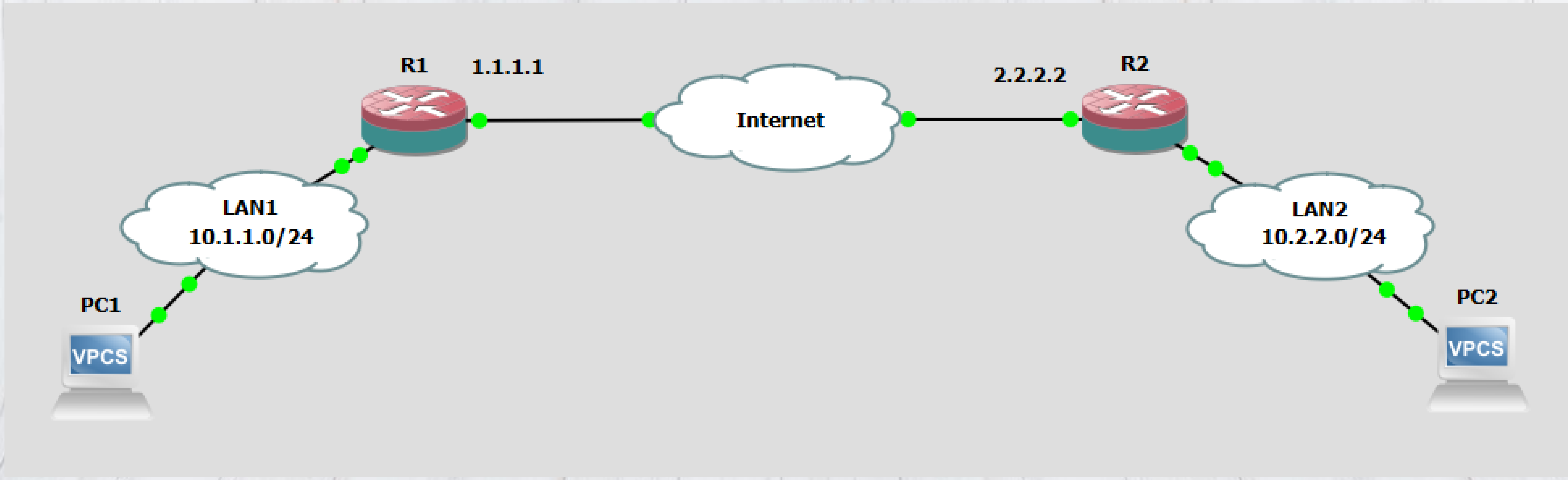
  Defines what traffic to process, and how to process it

- /ip ipsec proposal

  Defines what crypto / hashing algos to use

Let’s see an example

- To understand this, lets 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)

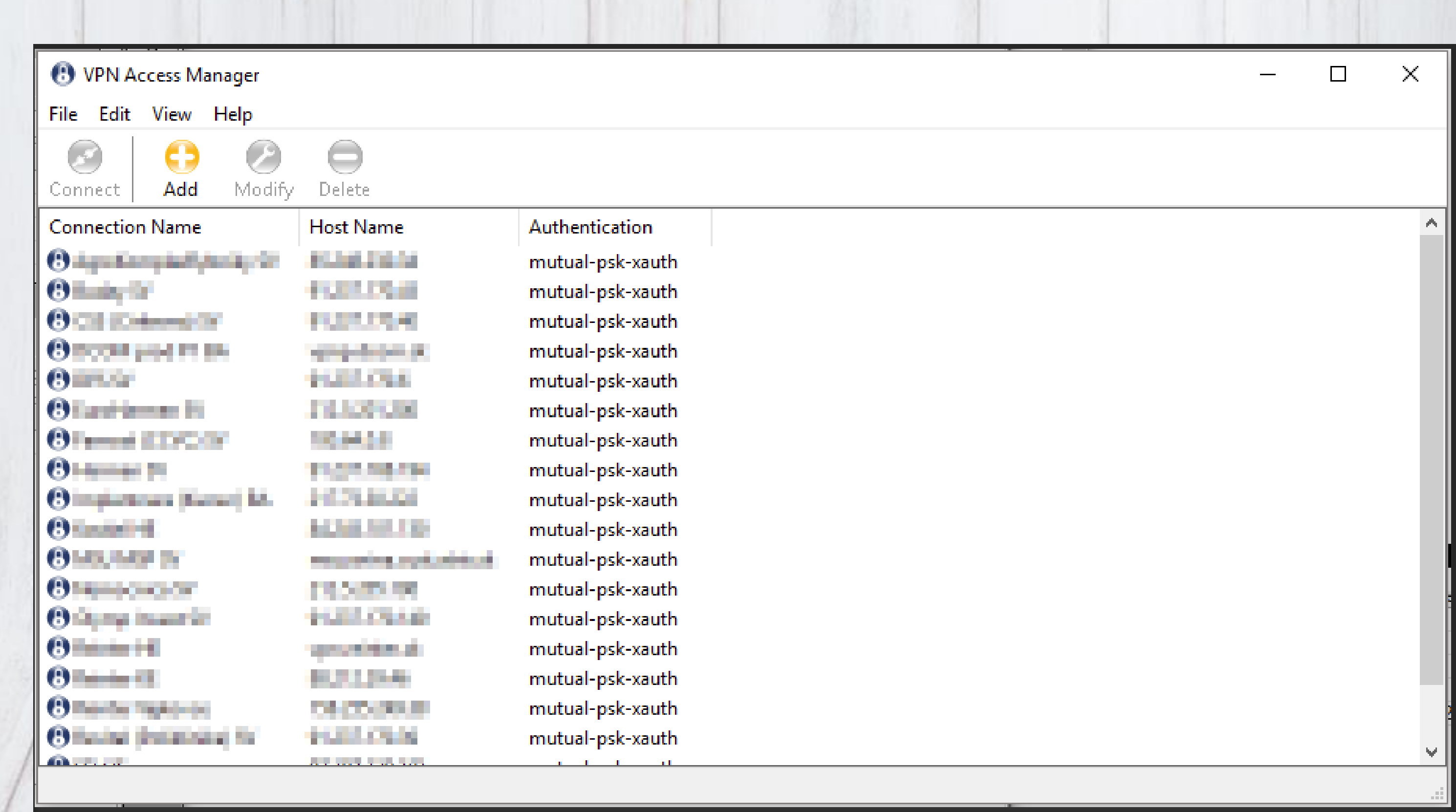
  DNS (so they can resolve local hostnames)
- Let’s discuss why…

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



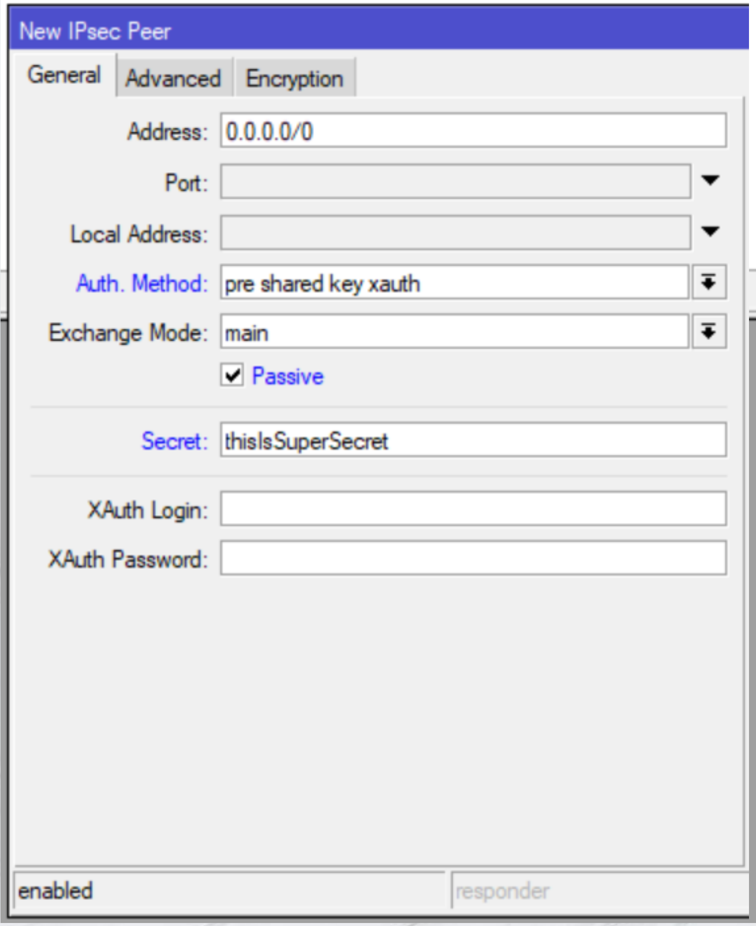
Connection Name	Host Name	Authentication
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth
[redacted]	[redacted]	mutual-psk-xauth

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

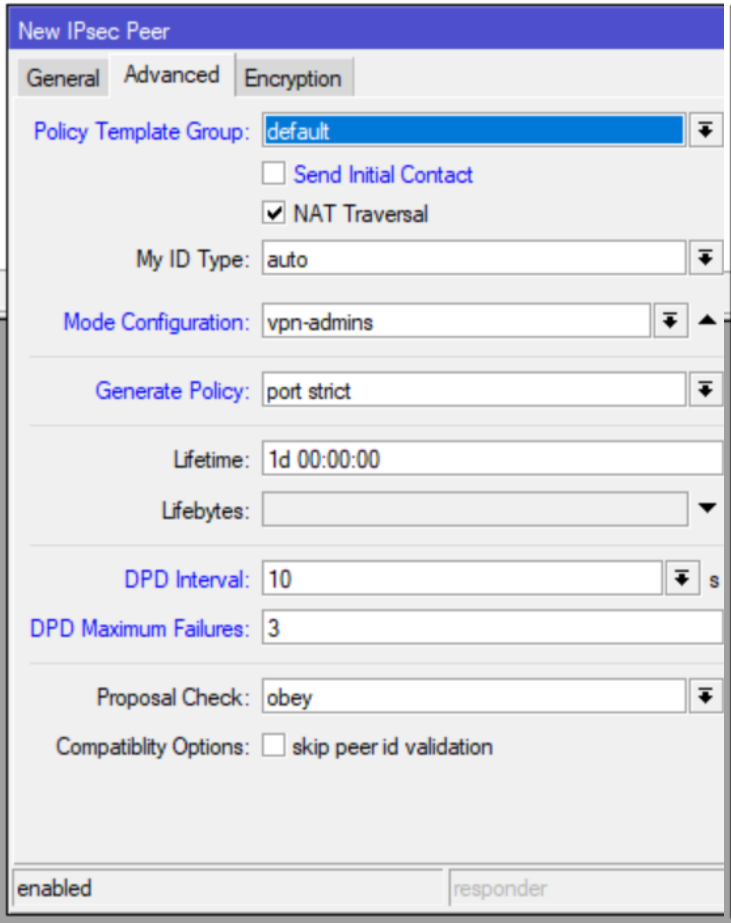


New IPsec Peer

General | Advanced | Encryption

Address: 0.0.0.0/0
Port:
Local Address:
Auth. Method: pre shared key xauth
Exchange Mode: main
☑ Passive
Secret: thisIsSuperSecret
XAuth Login:
XAuth Password:

enabled | responder

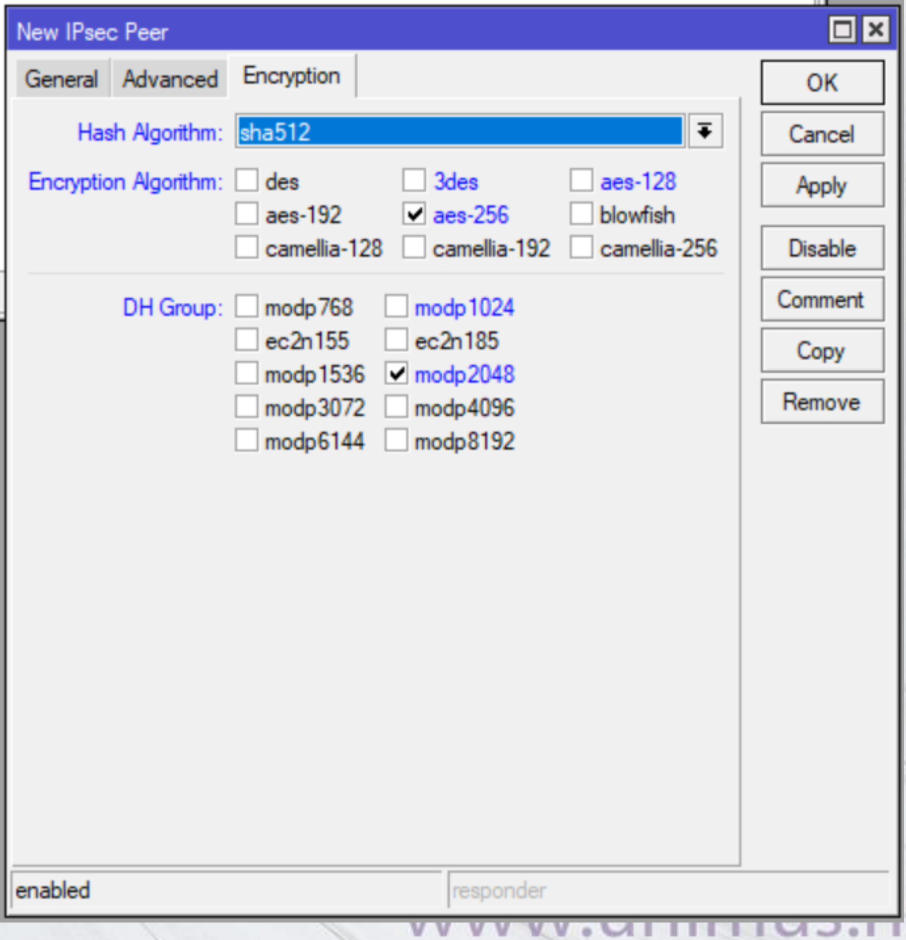


New IPsec Peer

General | Advanced | Encryption

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
Lifebytes:
DPD Interval: 10 s
DPD Maximum Failures: 3
Proposal Check: obey
Compatiblity Options: □ skip peer id validation

enabled | responder



New IPsec Peer

General | Advanced | Encryption

Hash Algorithm: sha512

Encryption Algorithm:

□ des	□ 3des	□ aes-128
□ aes-192	☑ aes-256	□ blowfish
□ camellia-128	□ camellia-192	□ camellia-256

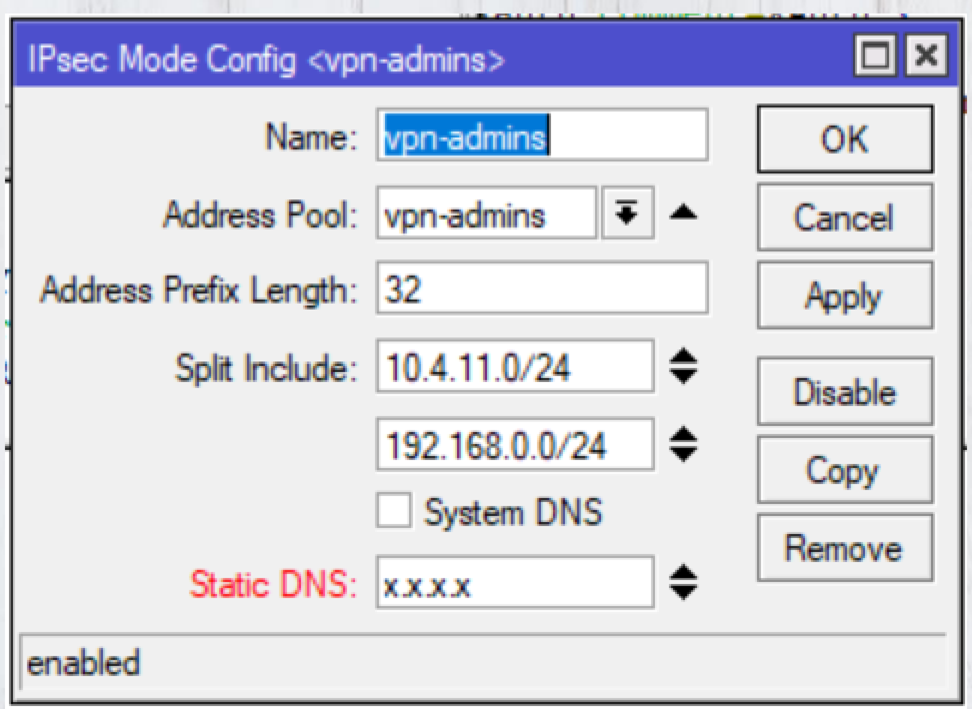
DH Group:

□ modp768	□ modp1024
□ ec2n155	□ ec2n185
□ modp1536	☑ modp2048
□ modp3072	□ modp4096
□ modp6144	□ modp8192

enabled | responder

How to push config to clients

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



IPsec Mode Config <vpn-admins>

Name: vpn-admins

Address Pool: vpn-admins

Address Prefix Length: 32

Split Include: 10.4.11.0/24

192.168.0.0/24

□ System DNS

Static DNS: x.x.x.x

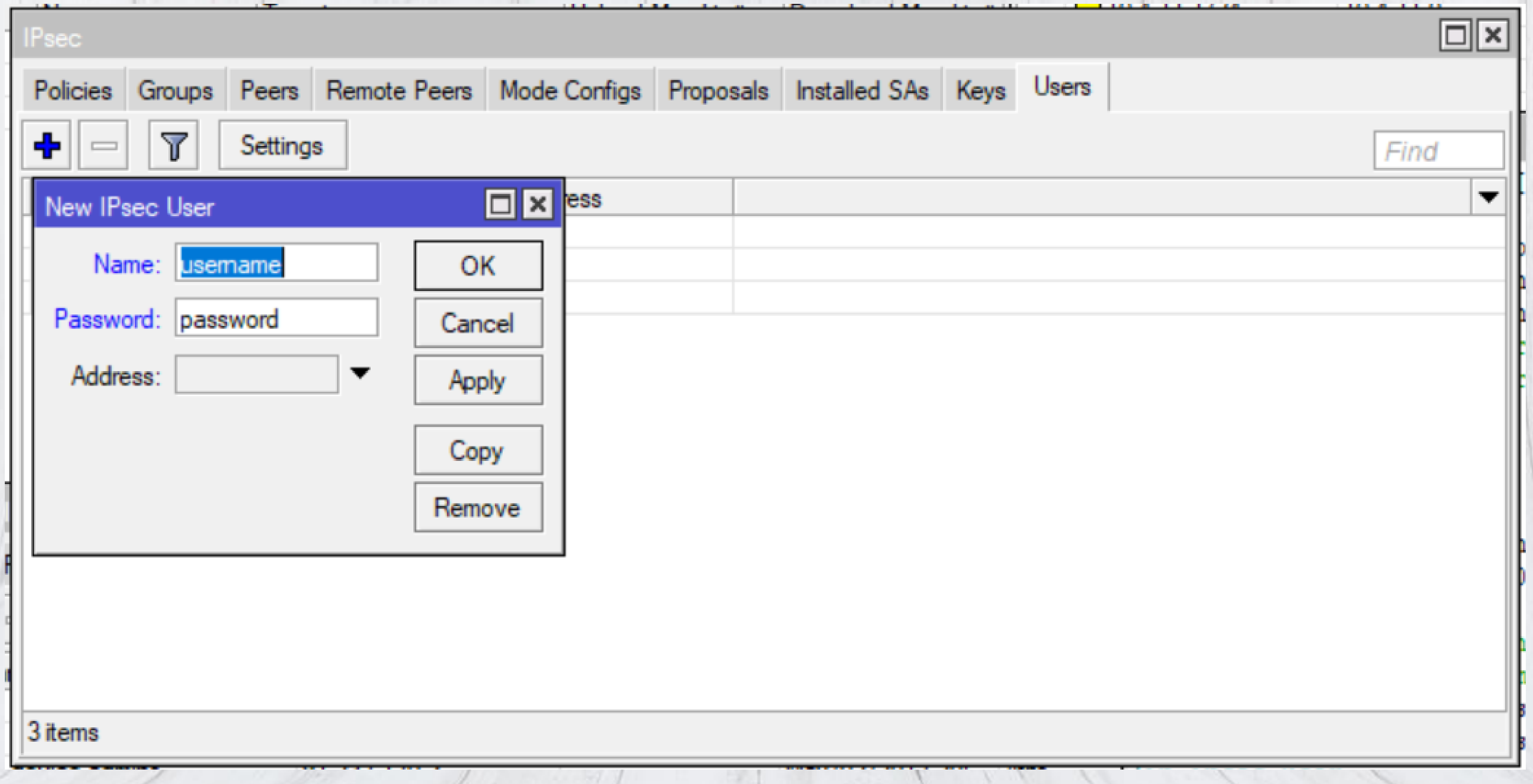
enabled

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:



Name: username

Password: password

Address:

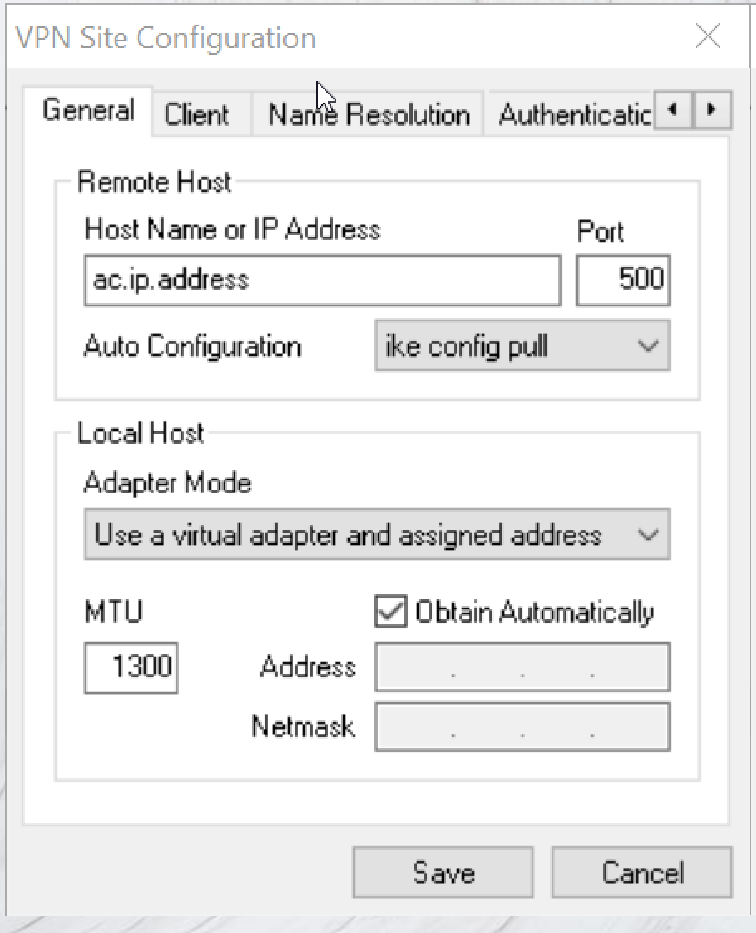
3 items

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



Remote Host

Host Name or IP Address: ac.ip.address

Port: 500

Auto Configuration: ike config pull

Local Host

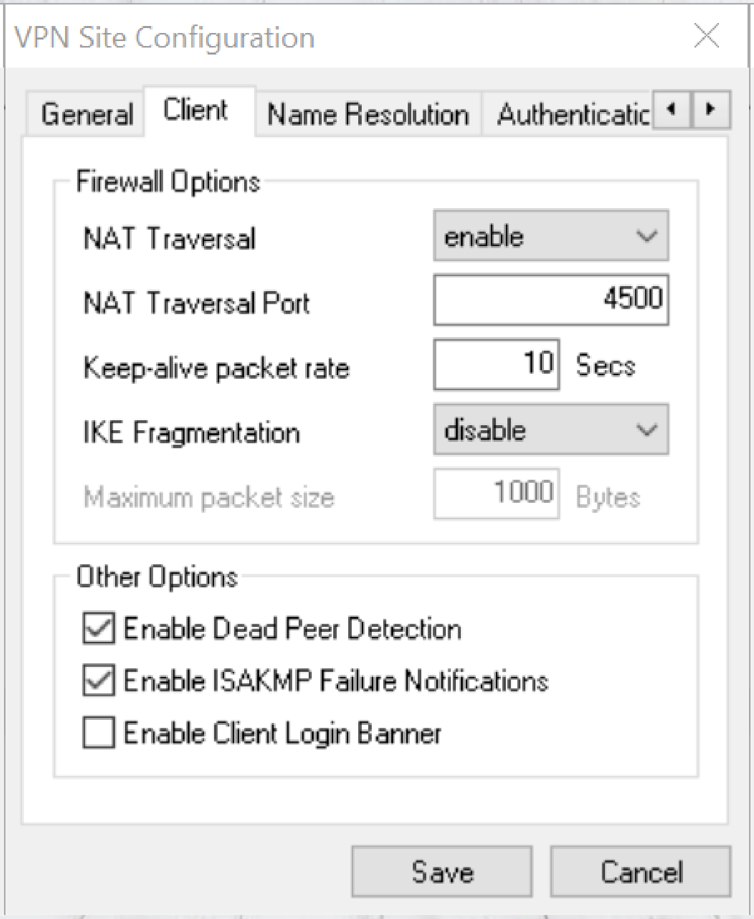
Adapter Mode: Use a virtual adapter and assigned address

MTU: 1300

☑ Obtain Automatically

Address: . . .

Netmask: . . .



Firewall Options

NAT Traversal: enable

NAT Traversal Port: 4500

Keep-alive packet rate: 10 Secs

IKE Fragmentation: disable

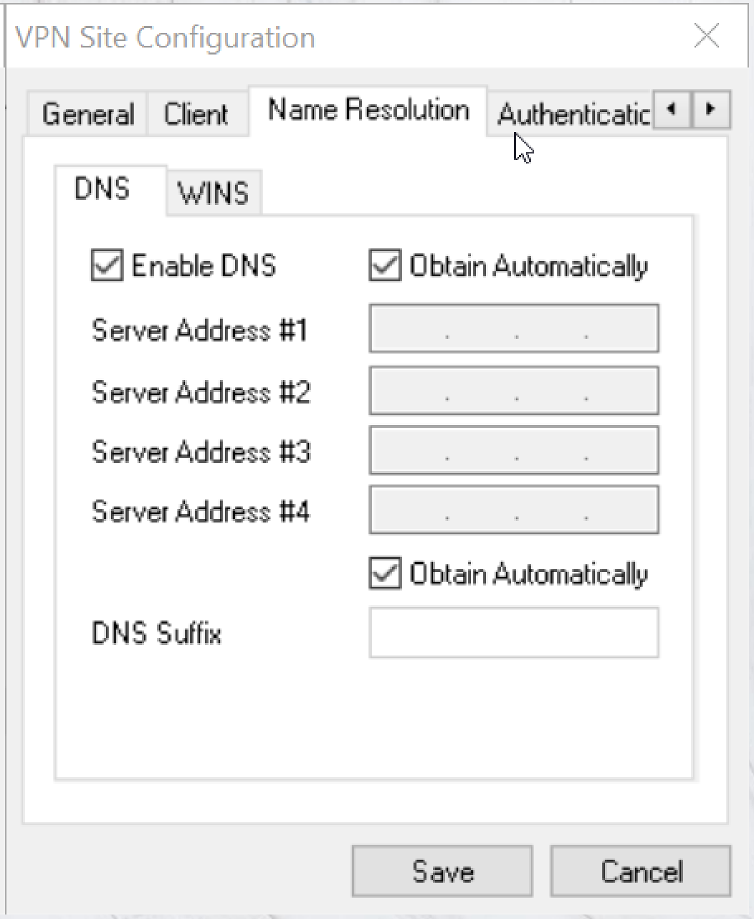
Maximum packet size: 1000 Bytes

Other Options

☑ Enable Dead Peer Detection

☑ Enable ISAKMP Failure Notifications

☐ Enable Client Login Banner



☑ Enable DNS

☑ Obtain Automatically

Server Address #1: . . .

Server Address #2: . . .

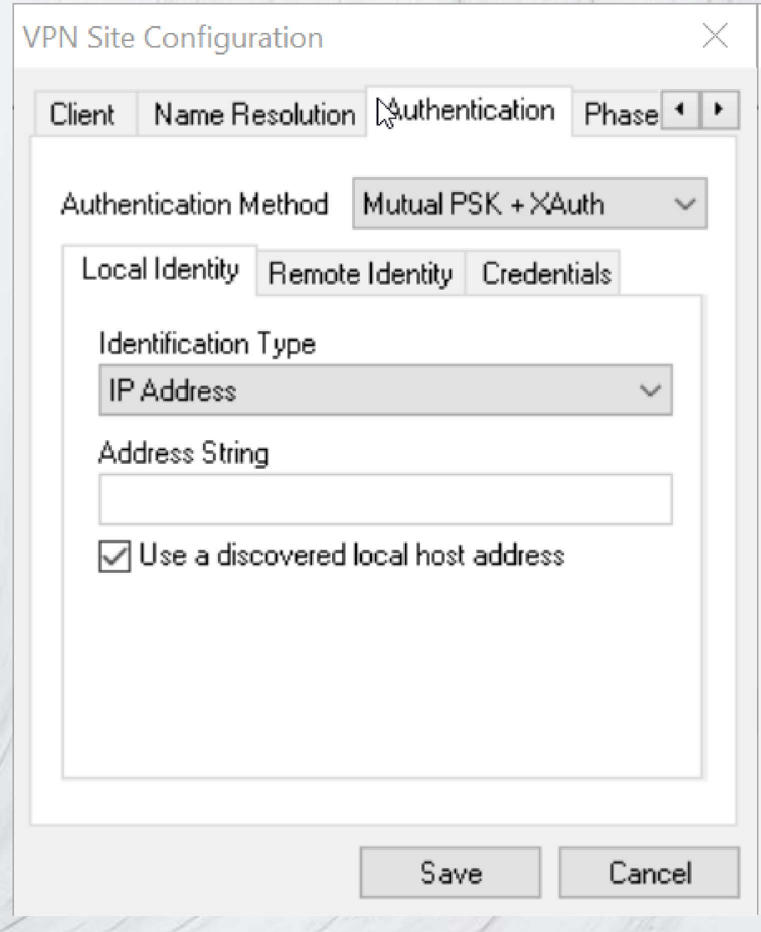
Server Address #3: . . .

Server Address #4: . . .

☑ Obtain Automatically

DNS Suffix:

How to configure client 2



VPN Site Configuration

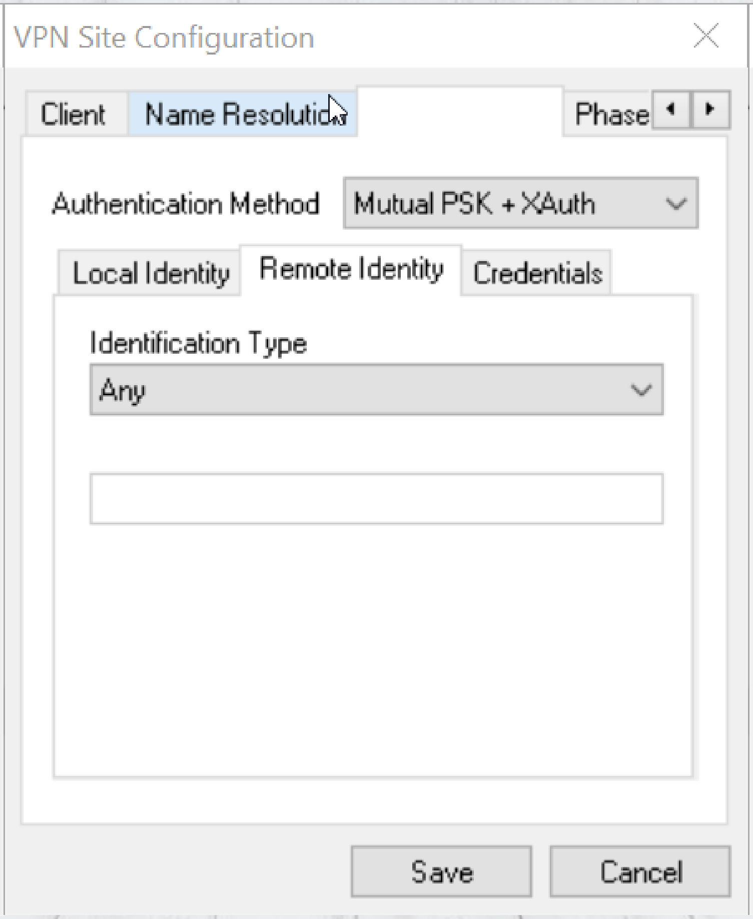
Authentication Method: Mutual PSK + XAuth

Local Identity

Identification Type: IP Address

Address String:

☑ Use a discovered local host address

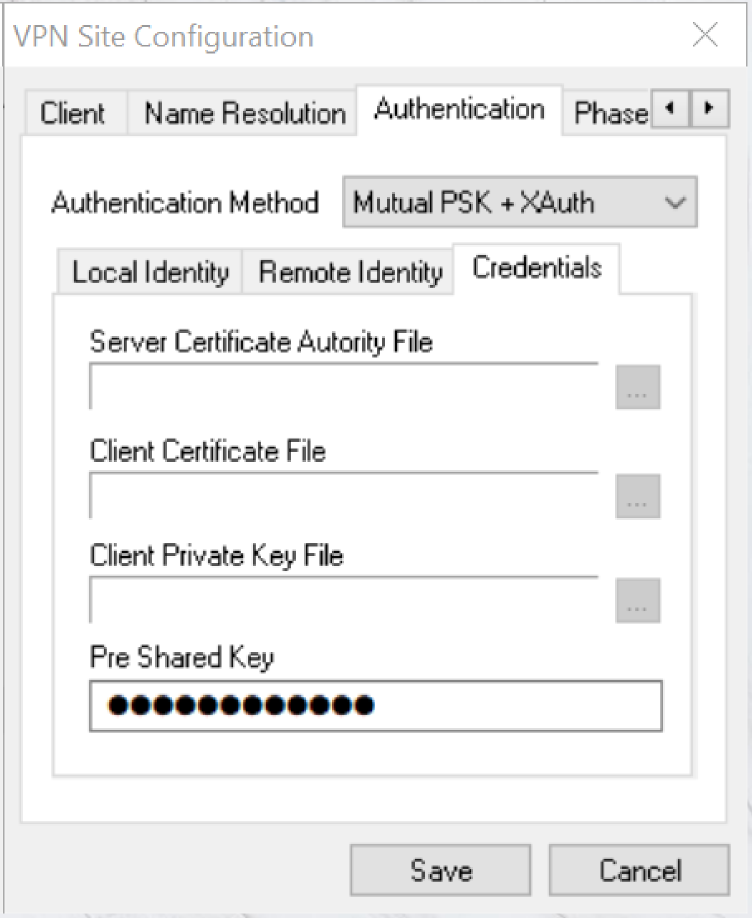


VPN Site Configuration

Authentication Method: Mutual PSK + XAuth

Remote Identity

Identification Type: Any



VPN Site Configuration

Authentication Method: Mutual PSK + XAuth

Credentials

Server Certificate Autority File

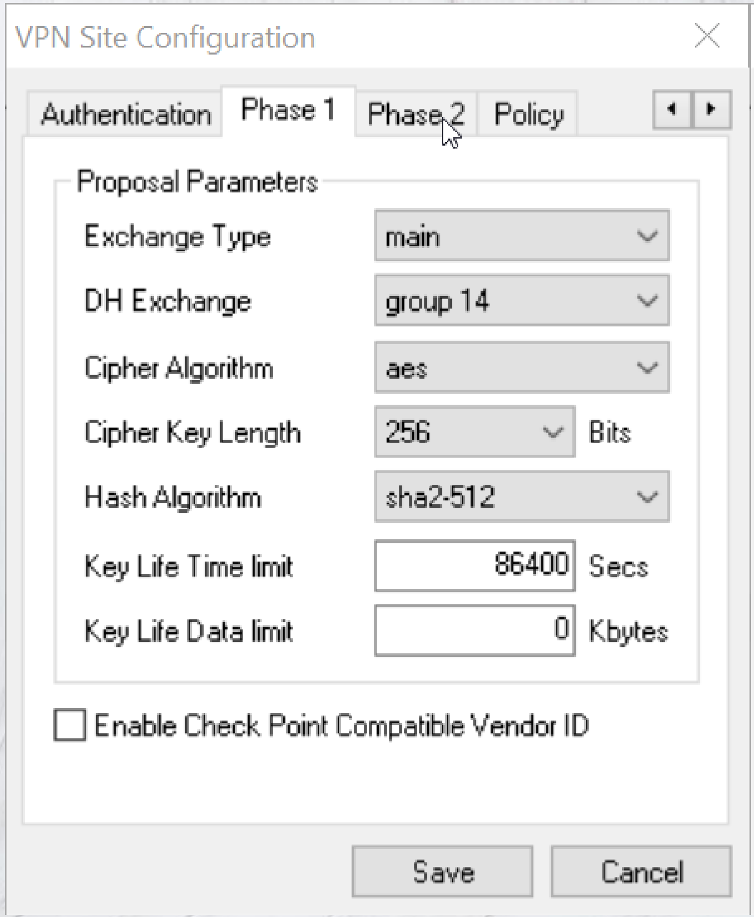
Client Certificate File

Client Private Key File

Pre Shared Key: ●●●●●●●●●●●●●

www.unimus.net

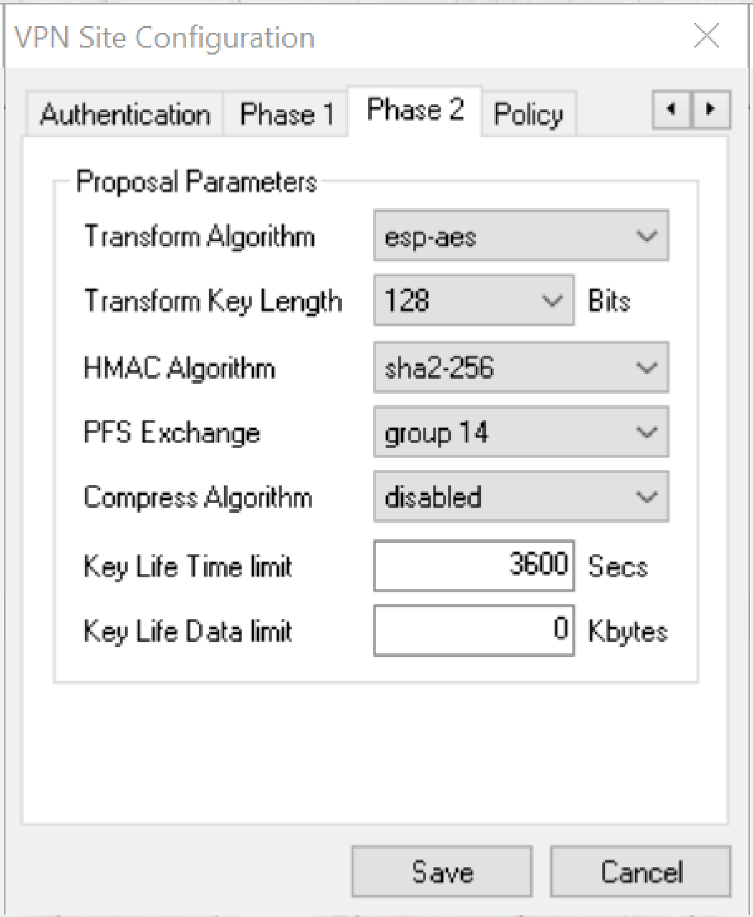
How to configure client 3



Proposal Parameters

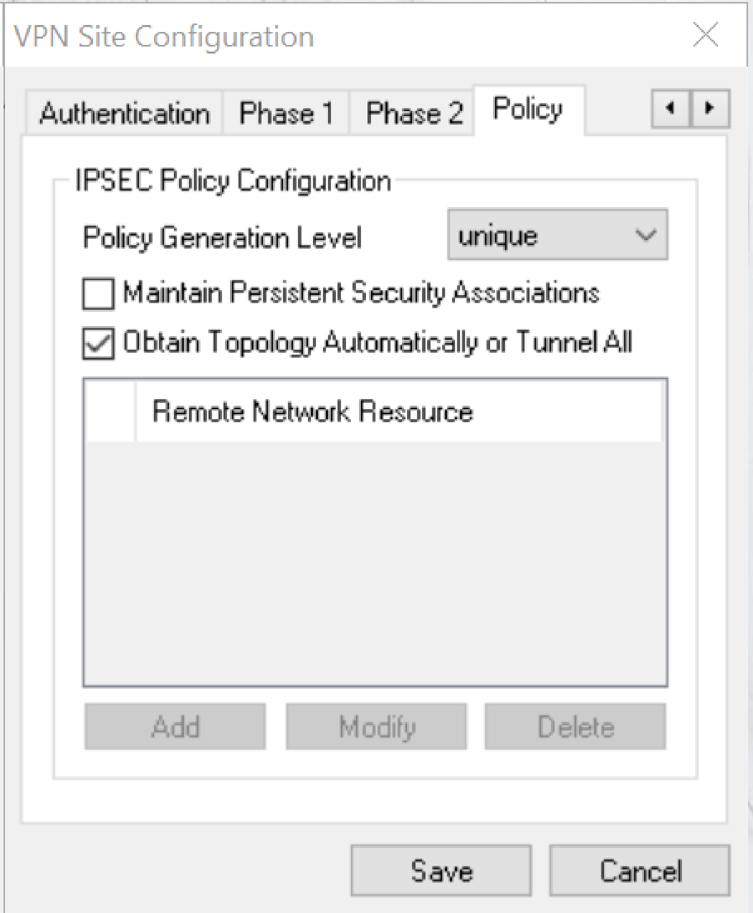
Exchange Type	main	
DH Exchange	group 14	
Cipher Algorithm	aes	
Cipher Key Length	256	Bits
Hash Algorithm	sha2-512	
Key Life Time limit	86400	Secs
Key Life Data limit	0	Kbytes

□ Enable Check Point Compatible Vendor ID



Proposal Parameters

Transform Algorithm	esp-aes	
Transform Key Length	128	Bits
HMAC Algorithm	sha2-256	
PFS Exchange	group 14	
Compress Algorithm	disabled	
Key Life Time limit	3600	Secs
Key Life Data limit	0	Kbytes



IPSEC Policy Configuration

Policy Generation Level: unique

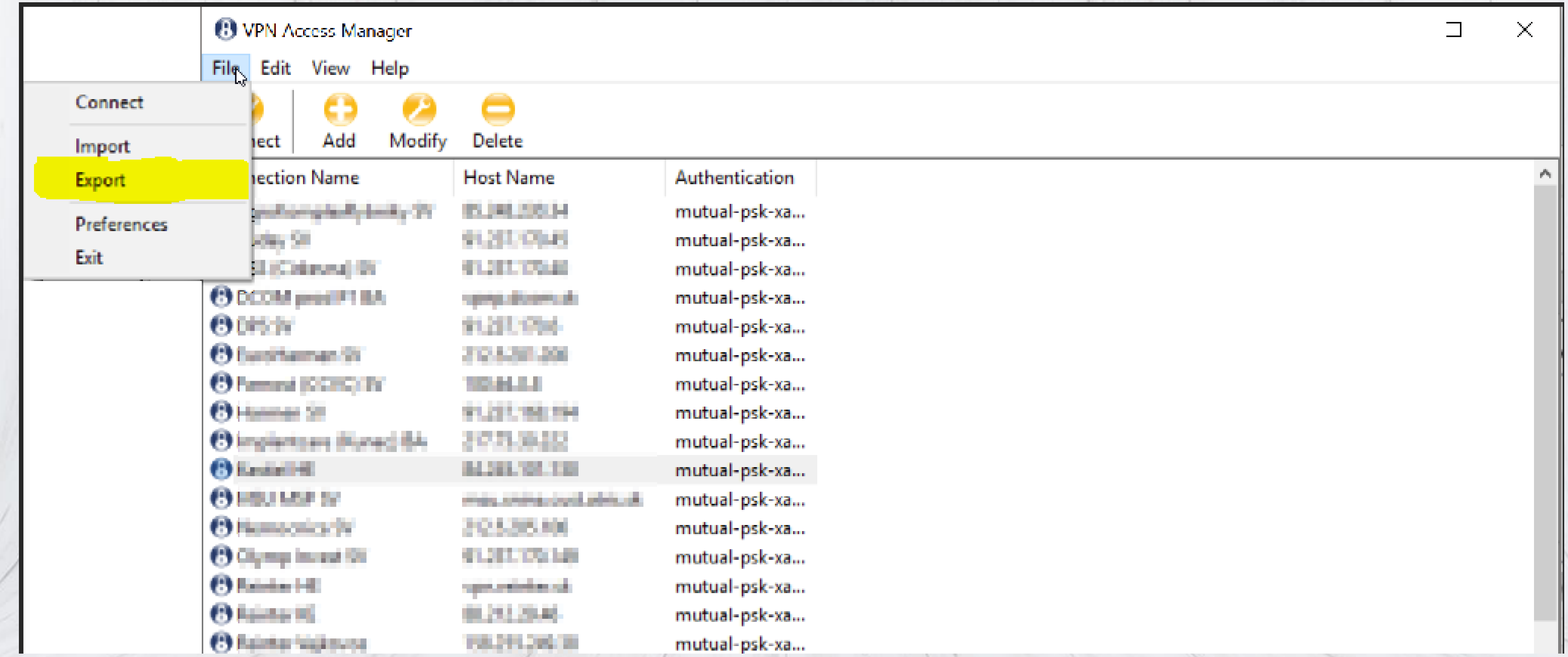
□ Maintain Persistent Security Associations

☑ Obtain Topology Automatically or Tunnel All

Remote Network Resource

Export config

- Export your config, send it to the Road Warrior



ection Name	Host Name	Authentication
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...
[redacted]	[redacted]	mutual-psk-xa...

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

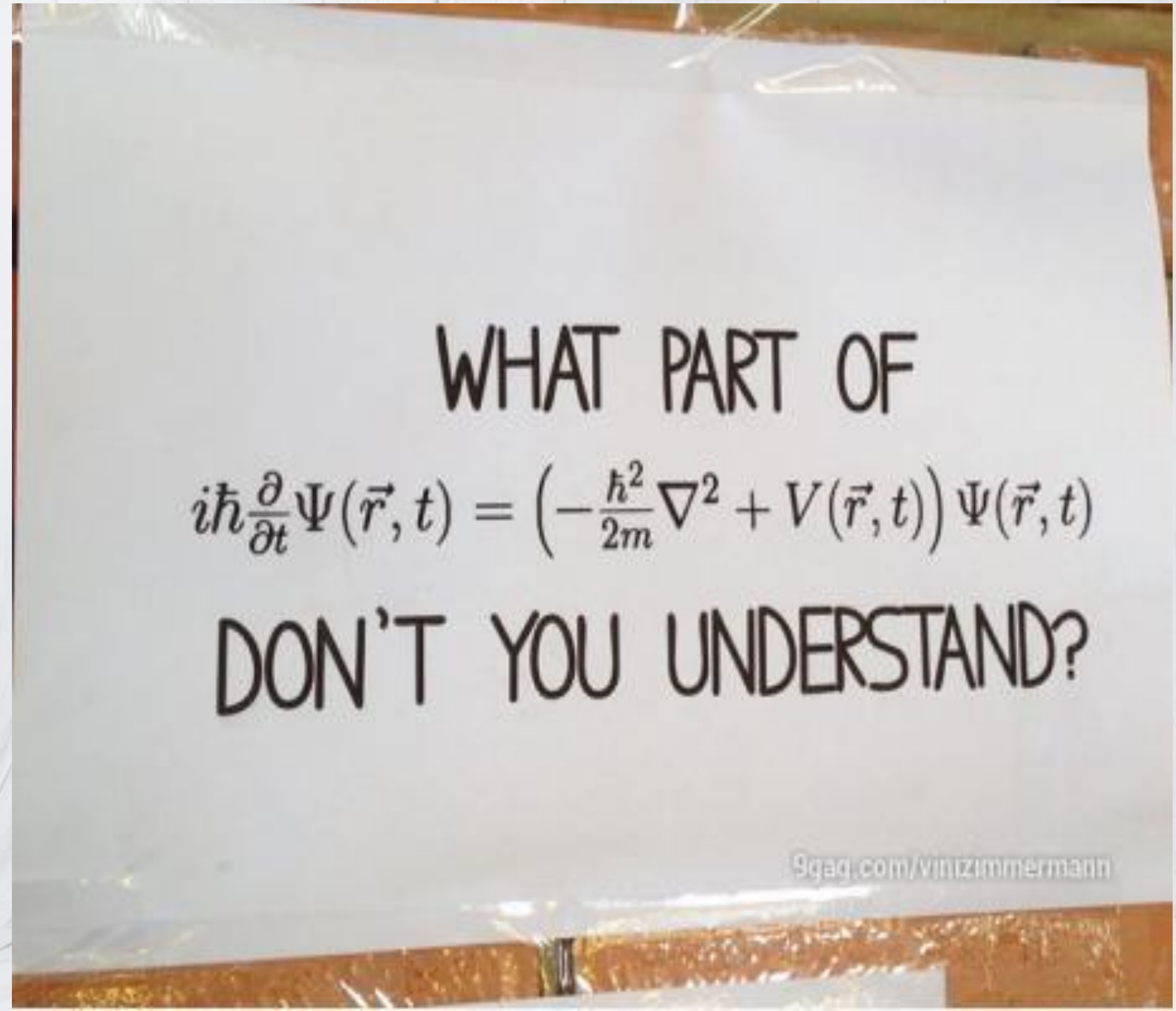
- Find all my other MUM presentations and more on: https://www.youtube.com/c/TomasKirnak/videos

  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!



WHAT PART OF

$$i\hbar\frac{\partial}{\partial t}\Psi(\vec{r},t) = \left(-\frac{\hbar^2}{2m}\nabla^2 + V(\vec{r},t)\right)\Psi(\vec{r},t)$$

DON'T YOU UNDERSTAND?

9gag.com/vinizimmermann

Tomas Kirnak
tomas@unimus.net