



As a VPN Server

Παναγιώτης Θεοχάρης

[panos@netspot.gr](mailto:panos@netspot.gr)



# Ποιός είμαι

- BSc in Computer Information Systems
- Στον χώρο της πληροφορικής από το 1990
- Ασχολούμαι με δίκτυα, VoIP, εφαρμογές δικτύων και με
- Χρησιμοποιώ Mikrotik από το 2005
- Εξειδίκευση σε Hot Spots, Long Range Wifi Links, Firewalls, vpns,

# Ποιός είμαι

- Πιστοποιήσεις από την Mikrotik :
- **MTCNA** - MikroTik Certified Network Associate
- **MTCWE** - MikroTik Certified Wireless Engineer
- **MTCTCE** - MikroTik Certified Traffic Control Engineer

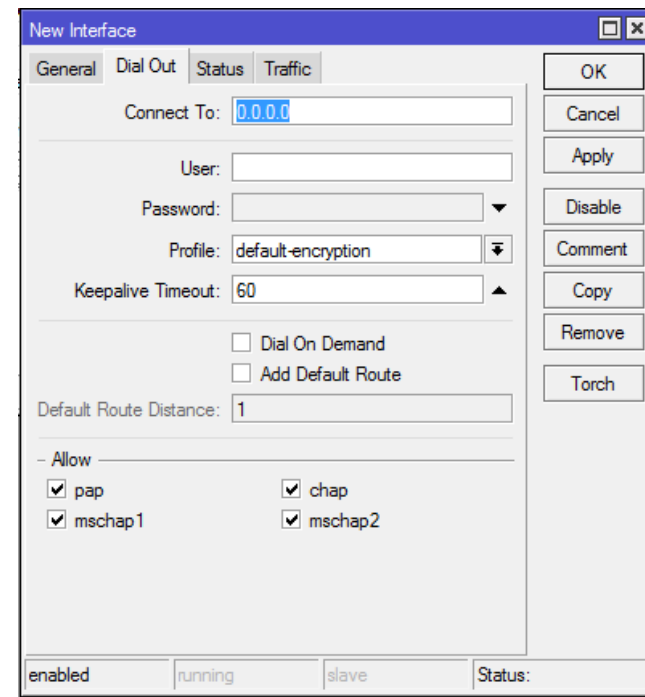
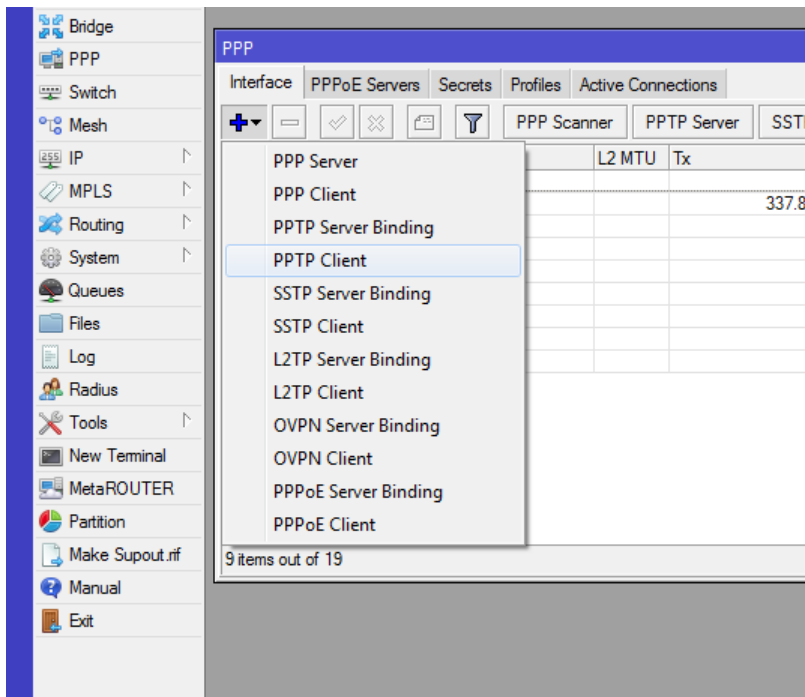


# Δυνατότητες ως Vpn

- PPP (Advanced PPP features MLPPP, BCP)
- Point to Point Tunnels :
  - PPPoE
  - PPtP
  - L2TP
  - SSTP
  - OpenVPN
- IPSec Tunnel & Transport
- Simple Tunnels :
  - IPIP
  - EoIP

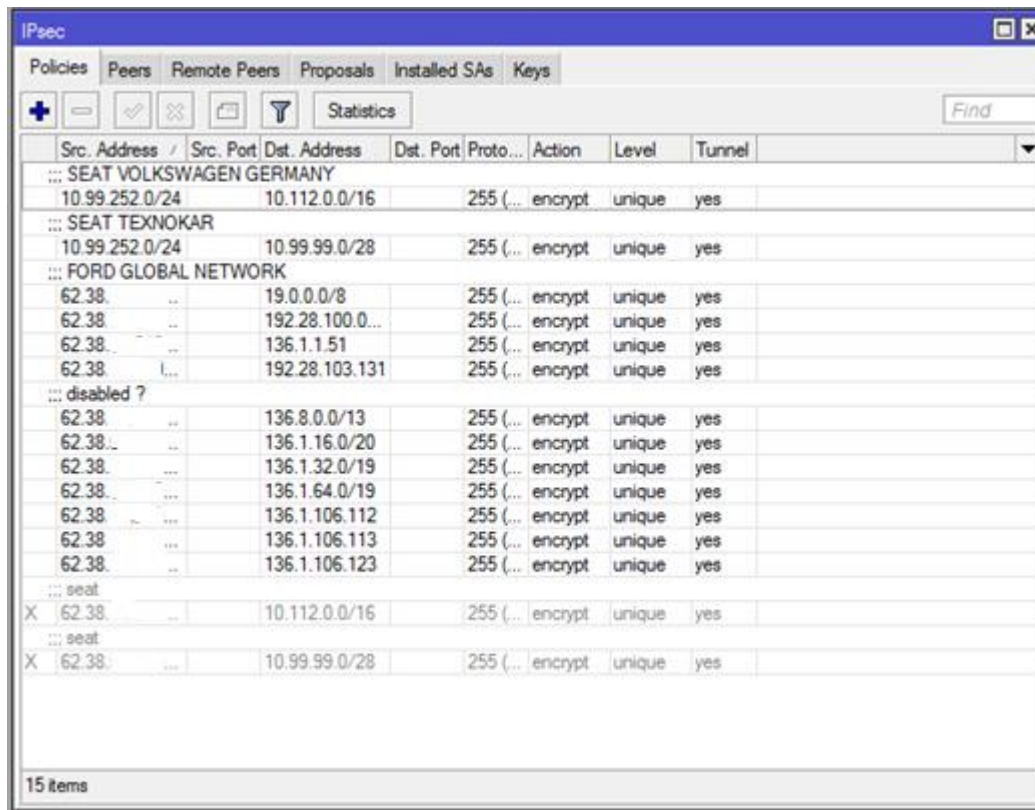
# Δυνατότητες ως Vpn Client

- Εξαιρετικά απλή ρύθμιση



# Δυνατότητες ως Vpn Client

- Πλήρη συμβατότητα με άλλους vendors, πχ Cisco



The screenshot shows the IPsec configuration window with the 'Policies' tab selected. The table lists various IPsec policies with their source and destination addresses, ports, protocols, actions, levels, and tunnel status.

	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
...	SEAT VOLKSWAGEN GERMANY							
	10.99.252.0/24		10.112.0.0/16		255 (...)	encrypt	unique	yes
...	SEAT TEXNOKAR							
	10.99.252.0/24		10.99.99.0/28		255 (...)	encrypt	unique	yes
...	FORD GLOBAL NETWORK							
	62.38...		19.0.0.0/8		255 (...)	encrypt	unique	yes
	62.38...		192.28.100.0...		255 (...)	encrypt	unique	yes
	62.38...		136.1.1.51		255 (...)	encrypt	unique	yes
	62.38...		192.28.103.131		255 (...)	encrypt	unique	yes
...	disabled ?							
	62.38...		136.8.0.0/13		255 (...)	encrypt	unique	yes
	62.38...		136.1.16.0/20		255 (...)	encrypt	unique	yes
	62.38...		136.1.32.0/19		255 (...)	encrypt	unique	yes
	62.38...		136.1.64.0/19		255 (...)	encrypt	unique	yes
	62.38...		136.1.106.112		255 (...)	encrypt	unique	yes
	62.38...		136.1.106.113		255 (...)	encrypt	unique	yes
	62.38...		136.1.106.123		255 (...)	encrypt	unique	yes
...	seat							
X	62.38...		10.112.0.0/16		255 (...)	encrypt	unique	yes
...	seat							
X	62.38...		10.99.99.0/28		255 (...)	encrypt	unique	yes

15 items

# Δυνατότητες ως Vpn Server

- Διαφορετικά πρωτόκολλα για διαφορετικές χρήσεις

protocol name	OSI layer	max MTU	protocol using	as bridge port	topology	security	Mikrotik version	suitable for
EoIP	L3	1500	TCP	yes	PtP	no	> 2.9	connecting subnets cross intranet
IP tunnel (IpIp)	L3	1480	TCP	no	PtP	no	> 2.9	
PPtP	L2	1420	GRE, TCP	yes (BCP)	PtMP	yes	> 2.9	for connecting clients to central server
L2tP	L2	1420	UDP	yes (BCP)	PtMP	yes	> 2.9	for connecting clients to central server
SSTP	L2	1500	TCP	yes (BCP)	PtMP	yes	> 5.0	for connecting clients to central server

# Simple Tunnels

- Ipv6,
- σύμφωνα με το [RFC 2003](#)
- Χρήσιμο για
  - α) σύνδεση (bridge) intranets μέσα από το ίντερνετ
  - β) για ειδική μεταχείριση και αποφυγή source routing
- Δεν παρέχει encryption



# Simple Tunnels

- EoIP,
- Propriety της Mikrotik με το GRE & [RFC 1701](#)
- Χρήσιμο για
  - α) σύνδεση (bridge) LANs μέσα από το ίντερνετ
  - β) σύνδεση (bridge) subnets μέσα στο intranet
  - γ) σύνδεση (bridge) LANs μέσα από encrypted tunnels
  - δ) σύνδεση (bridge) LANs πάνω από ad-hoc wireless networks
- Παιρνούν όλα τα δεδομένα μέσα από αυτό (TCP,UDP, κλπ)
- Δεν παρέχει encryption

# IP Sec

- Ασφαλή μεταφορά δεδομένων μέσα από το Internet
- Φτιαγμένο από το Internet Engineering Task Force
- 3 κύρια μέρη :
  - **Authentication Header (AH)** [RFC 4302](#)
  - **Encapsulating Security Payload (ESP)** [RFC 4303](#)
  - **Internet Key Exchange (IKE)** protocols. Dynamically generates and distributes cryptographic keys for AH and ESP.

# IP Sec

- Authentication Header (AH)
- AH πρωτόκολλο για το authentication όλου ή μέρους των πακέτων, ανάλογα με τον τρόπο μεταφοράς (tunnel ;h transport mode).
- Η ύπαρξη του AH επιτρέπει τον έλεγχο για την εγκυρότητα του μηνύματος αλλά δεν το κωδικοποιεί. Αντίθετα το ESP παρέχει και encryption
- Υπάρχουν δύο διαθέσιμοι αλγόριθμοι για το AH:  
SHA1  
MD5

# IP Sec

- Encapsulating Security Payload (ESP)
- Πρωτόκολλο που χρησιμοποιεί μοιραζόμενο κλειδί (shared key) για το encryption
- Έχει δικό του authentication αλλά μπορεί να λειτουργεί και μαζί με το AH
- Χωρίζεται σε τρία μέρη, ESP Header, ESP Trailer, ESP Authentication Data
- Υπάρχουν δύο διαθέσιμοι αλγόριθμοι και πάλι :  
SHA1  
MD5

# IP Sec

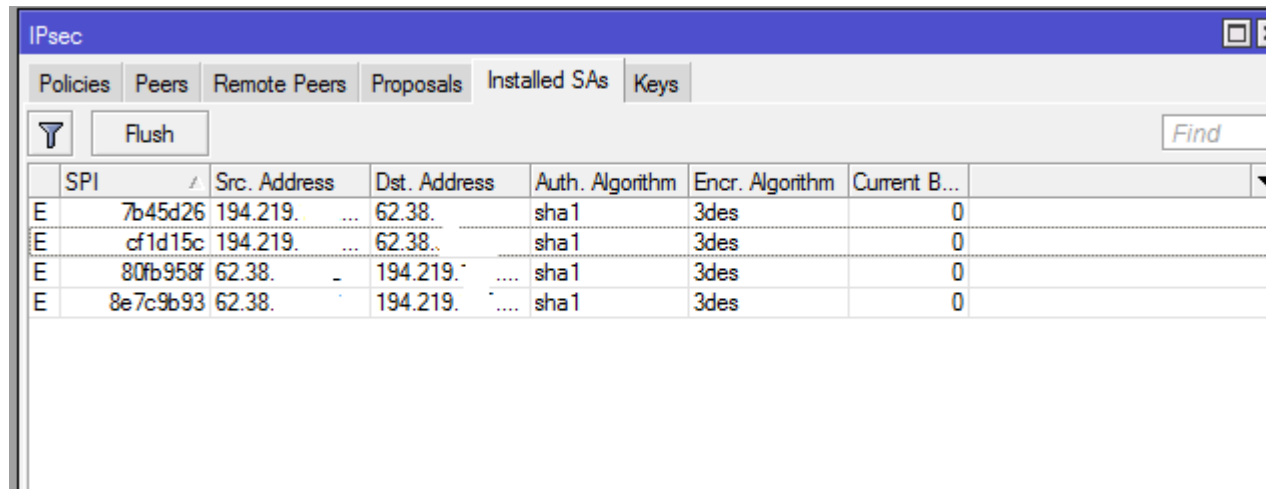
- **Encryption algorithms**
- **DES** - 56-bit DES-CBC encryption algorithm;
- **3DES** - 168-bit DES encryption algorithm;
- **AES** - 128, 192 and 256-bit key AES-CBC encryption algorithm;
- **Blowfish** - added since v4.5
- **Twofish** - added since v4.5
- **Camellia** - 128, 192 and 256-bit key Camellia encryption algorithm added since v4.5

# IP Sec

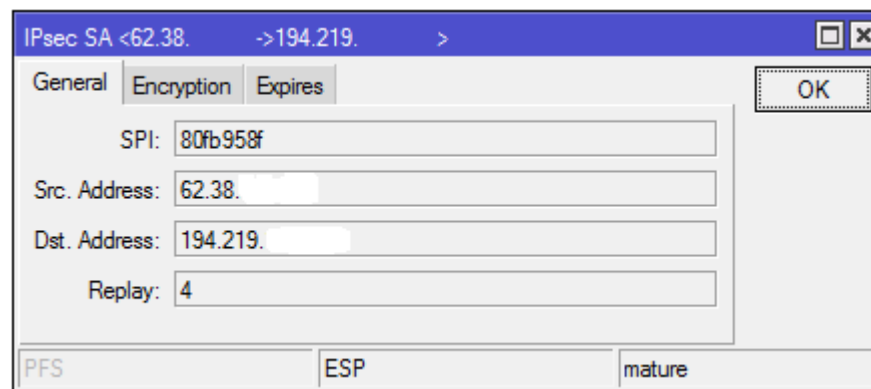
- **Hardware Encryption**
- **RB1000**
- **RB1000AHx2**
- **Cloud Core Routers**
- Internet Key Exchange (IKE)
- Πρωτόκολλο που παρέχει authentication keying για το Internet Security Association and Key Management Protocol (ISAKMP) framework. (Security Associations –SA)
- Phase 1 & Phase 2

# IP Sec

- **Security Associations (Sas)**



	SPI	Src. Address	Dst. Address	Auth. Algorithm	Encr. Algorithm	Current B...
E	7b45d26	194.219. ...	62.38.	sha1	3des	0
E	cf1d15c	194.219. ...	62.38..	sha1	3des	0
E	80fb958f	62.38.	194.219. ....	sha1	3des	0
E	8e7c9b93	62.38.	194.219. ....	sha1	3des	0



IPsec SA <62.38. ->194.219. >

General Encryption Expires

SPI: 80fb958f

Src. Address: 62.38.

Dst. Address: 194.219.

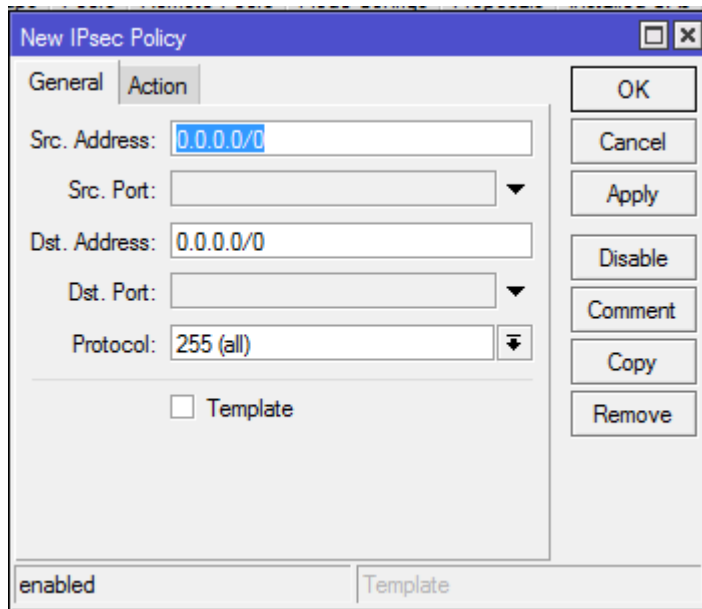
Replay: 4

OK

PFS ESP mature

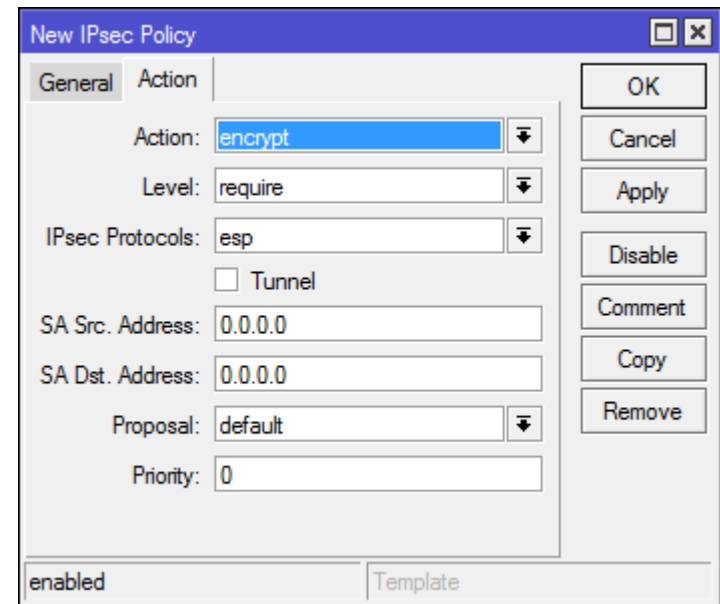
# IP Sec

- Δηλώνουμε τα subnet που θέλουν να επικοινωνήσουν, καθώς και τις (πραγματικές) Ips των άκρων



The 'New IPsec Policy' dialog box is shown with the 'General' tab selected. It contains the following fields and controls:

- Src. Address:** 0.0.0.0/0
- Src. Port:** (empty dropdown)
- Dst. Address:** 0.0.0.0/0
- Dst. Port:** (empty dropdown)
- Protocol:** 255 (all)
- ☐ Template
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status:** enabled
- Template:** Template



The 'New IPsec Policy' dialog box is shown with the 'Action' tab selected. It contains the following fields and controls:

- Action:** encrypt
- Level:** require
- IPsec Protocols:** esp
- ☐ Tunnel
- SA Src. Address:** 0.0.0.0
- SA Dst. Address:** 0.0.0.0
- Proposal:** default
- Priority:** 0
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status:** enabled
- Template:** Template



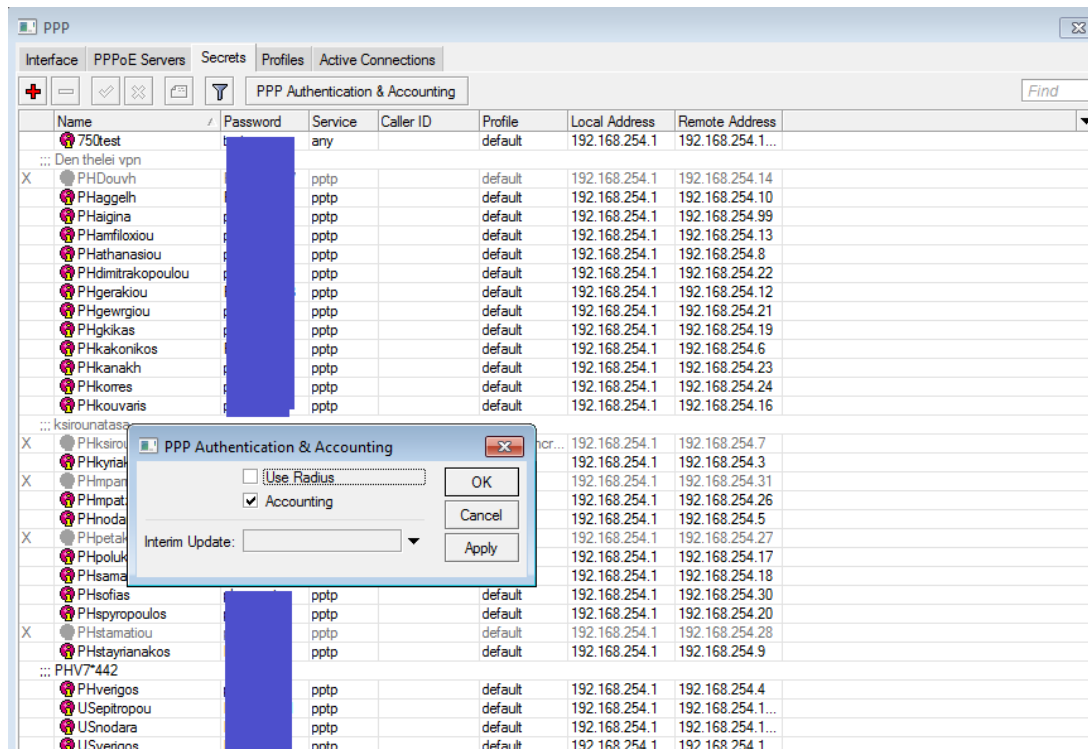
# Point to point tunneling

- **PPTP**
- Το πιο διαδεδομένο πρωτόκολλο, σύμφωνα με το [RFC 2637](#)
- Χρησιμοποιεί το PPP and MPPE (Microsoft Point to Point Encryption) για να δημιουργεί encrypted links
- Χρησιμοποιεί Multilink PPP (MP) δίνοντας την δυνατότητα για MRRU (Maximum Received Reconstructed Unit) προσφέροντας την δυνατότητα να μεταφέρουμε πακέτα 1500 mtu αλλά και μεγαλύτερα.
- Encryption με MPPE 40bit RC4 and MPPE 128bit RC4

# Point to point tunneling

- **PPTP**

Περιλαμβάνει PPP authentication και accounting για κάθε pptp σύνδεση, είτε τοπικά είτε με χρήση radius



# Point to point tunneling

- **L2TP**
- Σύμφωνα με το [RFC 2661](#)
- Ίδιες δυνατότητες με το PPtP
- Προσφέρει Layer 2 επικοινωνία μεταξύ των τερματικών σε ένα packet-switched δίκτυο, δημιουργώντας ένα Local Access Concentrator – LAC (modem bank, ADSL DSLAM κλπ) το οποίο προωθεί τα πακέτα μέσω τούνελ σε ένα Network Access Server - NAS.
- Χρησιμοποιείτε συχνά ως L2TP over IPsec (standard τρόπος υλοποιήσεις της Microsoft)

# Point to point tunneling

- Secure Socket Tunneling Protocol (SSTP)
- Πρωτόκολλο της Microsoft
- Παρόμοιες δυνατότητες με το PPTP
- Συμβατότητα με Windows και Linux (clients για vista, 7,8)
- Δημιουργεί ένα PPP Tunnel επάνω από ένα κανάλι TLS 1.0
- Χρησιμοποιεί την πόρτα 443, οπότε **περνάει από τα συνήθη firewalls και proxies !**
- Χρησιμοποιεί Certificates με 472bits RSA Keys

# Point to point tunneling

- OpenVPN (OVPN)
- Open Source εφαρμογή, κυρίως για DD-WRT
- Παρόμοιες δυνατότητες με το PPtP
- Συμβατότητα με Linux
- Χρησιμοποιεί Certificates, Pre-Shared Keys, ή απλά username/password
- Χρησιμοποιεί OpenSSL encryption, SSLv3/TLSv1

# Point to point tunneling

- Point to Point Protocol over Ethernet (PPPoE)
- Χρησιμοποιείτε κυριώς από ISPs
- Multilink PPP (MLPPP);
- MLPPP over single link (ability to transmit full-sized frames);
- BCP (Bridge Control Protocol) support - allows sending of raw Ethernet frames over PPP links;
- MPPE 40bit and MPPE 128bit RSA encryption;
- pap, chap, mschap v1/v2 authentication;
- Υποστήριξη RADIUS για client authentication & accounting
- Μέγιστο MTU 1492

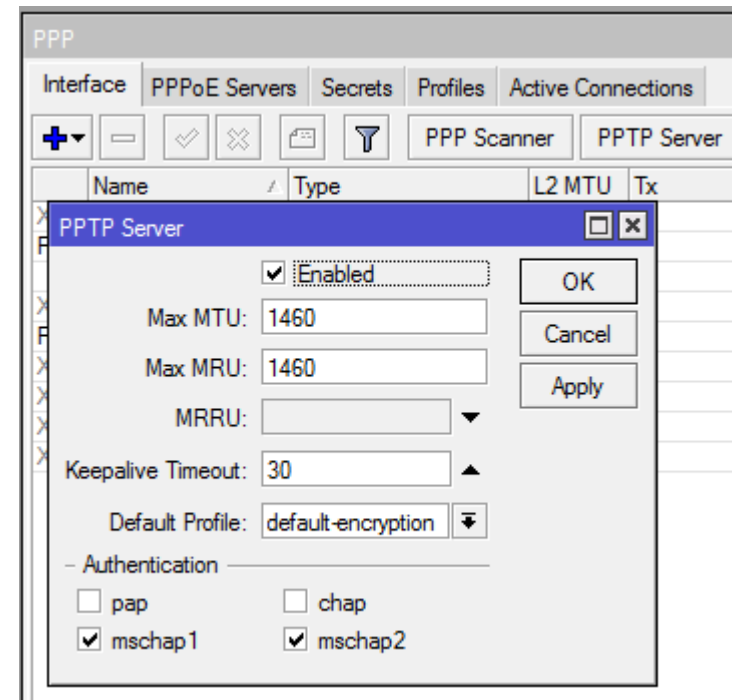
# Χρησιμοποιώντας PPTP

Παραμετροποίηση σε 4 + 1 μέρη

- PPTP Server
- PPP Secret  
Τοπικά ή σε Radius
- PPP Profiles
- Routing
- Έλεγχος κίνησης μέσω Firewall

# Παραμετροποίηση PPTP Server

- 1) Ενεργοποίηση
- 2) Επιλογή Μέγιστου MTU/MRU  
Επιλογή για MRRU
- 3) Default PPP Profile
- 4) Τρόποι authentication





# Παραμετροποίηση PPP Profile

PPP Profile <default>

General Protocols Limits Queue

Name: default

Local Address: 192.168.0.1

Remote Address: pool

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Incoming Filter:

Outgoing Filter:

Address List:

DNS Server:

WINS Server:

- Change TCP MSS

☐ default ☐ no ☒ yes

default

OK Cancel Apply Comment Copy Remove

PPP Profile <default>

General Protocols Limits Queue

- Use MPLS

☒ default ☐ no ☐ yes ☐ required

- Use Compression

☒ default ☐ no ☐ yes

- Use VJ Compression

☒ default ☐ no ☐ yes

- Use Encryption

☒ default ☐ no ☐ yes ☐ required

Session Timeout:

Idle Timeout:

Rate Limit (x/tx):

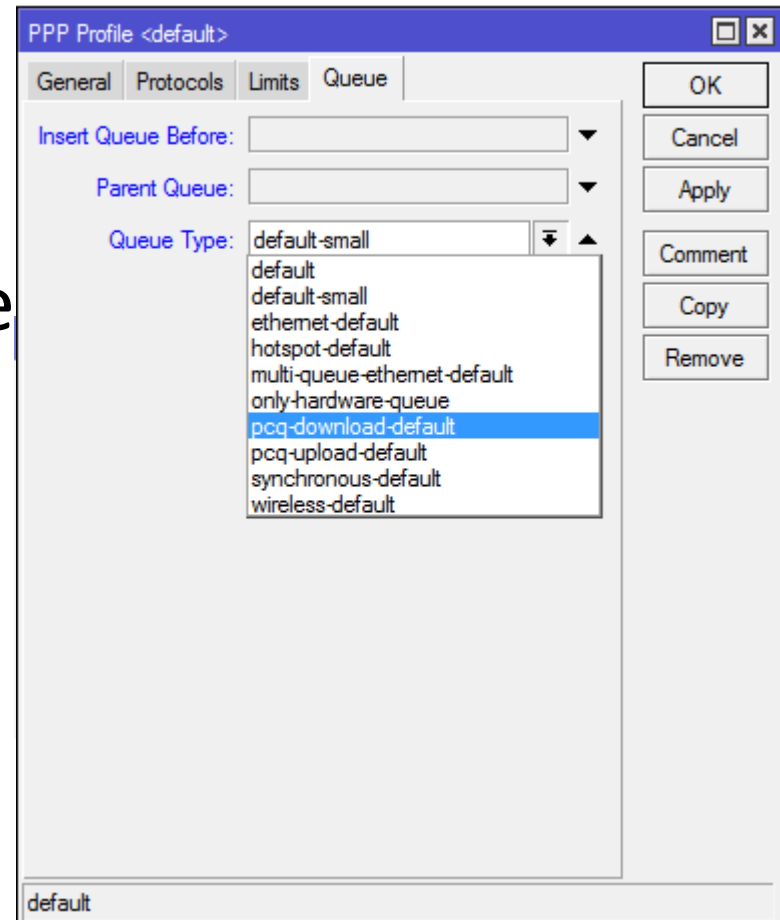
- Only One

☒ default ☐ no ☐ yes

OK Cancel Apply Comment Copy Remove

# Παραμετροποίηση PPP Profile

- Δυνατότητα δημιουργίας αυτόματης ουράς (Queue)
- Επιλογή τύπου queue
- Επιλογή αρχικής queue



# Παραμετροποίηση PPP Profile

- Επιλογή user/pass
- Τύπου PPP
- PPP Profile
- IP Δνσεων
- Περιορισμού traffic

any  
async  
l2tp  
ovpn  
pppoe  
pptp  
sstp

The screenshot shows a 'New PPP Secret' dialog box with the following fields and buttons:

- Name: ppp1
- Password: (empty)
- Service: any (selected)
- Caller ID: (empty)
- Profile: default
- Local Address: (empty)
- Remote Address: (empty)
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: (empty)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled

# Παραμετροποίηση PPP Routing

- Σε περίπτωση που δεν κάνουμε bridging θα πρέπει να ξέρουν τα δίκτυα πως θα επικοινωνούν
- PPP Secret > Routes  
Για να ξέρει ο server πως θα πηγαίνει στο subnet του πελάτη
- Στο PPtP Client, θα πρέπει να προσθέτουμε το κατάλληλο route στο Ip>Route

# Παραμετροποίηση PPP

- Να προτιμάτε την χρήση pool ώστε να ορίζεται για διαφορετικά subnets, διαφορετικούς κανόνες στο firewall
- Ελέξτε την κίνηση ανά IP αλλά και τις πόρτες που χρειάζεται.

Πχ :

SQL : TCP 135, 1433, 1434, 443, 445, 4022 κλπ

Voip : TCP 5060, UDP 10000-20000 κλπ

# Παραμετροποίηση PPP

- Προσοχή τα Windows PC έχουν την τάση να βγαίνουν στο internet από το νηρ σας !

The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. Below the tabs, there are buttons for adding (+), removing (-), enabling (checkmark), disabling (X), and a folder icon. There are also buttons for 'Reset Counters' and 'Reset All Counters', and a 'Find' search box. The main table lists the configured filter rules:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	reject	input	10.10.50.11							0 B	0
... accept traffic from vpn connection to intranet											
1	acc...	forward	192.168.75.0/24	192.168.0.0/16						1522.1 MiB	2 215 952
2	acc...	forward	195.168.75.0/24	172.16.0.0/16						0 B	0
... drop traffic to internet from vpn clients											
3	acc...	forward	192.168.75.201	0.0.0.0/0						0 B	0
4	reject	forward	192.168.75.0/24	0.0.0.0/0						24.4 MiB	355 386

# MPLS & VPN

- MultiProtocol Label Switching
- Δυνατότητα για δρομολόγηση των πακέτων όχι βάσει των header των πακέτων, αλλά με ετικέτες (labels) που τοποθετεί στο πακέτο.
- Συμβατότητα με linux & cisco
- Προσφέρει γρηγορότερη δρομολόγηση σε περίπτωση πολλαπλών router.

# Περιορισμοί Licence

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	<a href="#">no key</a>	<a href="#">registration required</a>	<a href="#">volume only</a>	\$45	\$95	\$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited



# Σας ευχαριστώ !

Πάνος Θεοχάρης

[panos@netspot.gr](mailto:panos@netspot.gr)

*MikroTik*  
Certified Consultant

