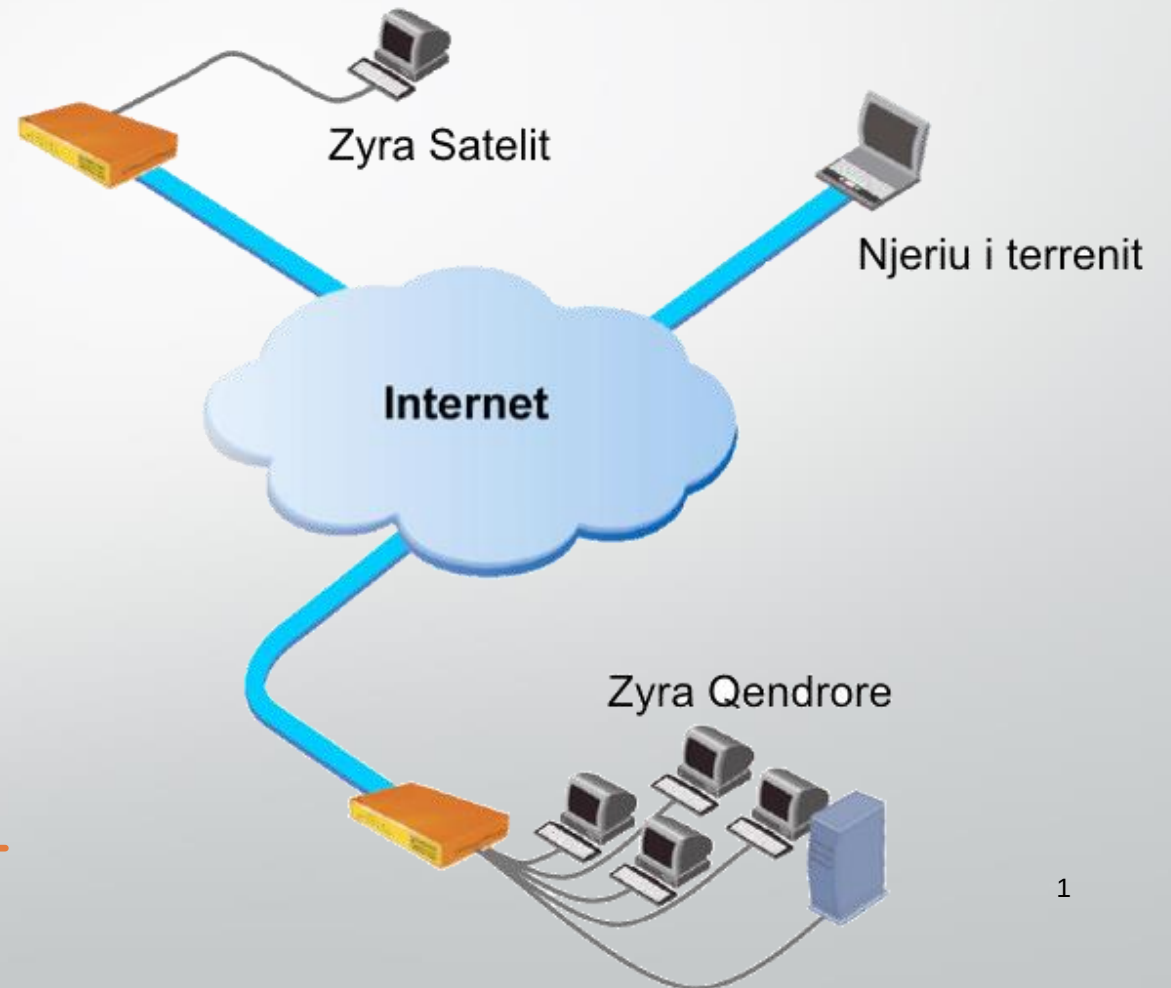


Krijimi i Tuneleve me IPSEC (VPN)



ELTON TËRSHANA

Tiranë, Nëntor 2018



Qëllimi

- Tunelet private krijohen me qëllim lidhjen e dy apo më shumë rrjeteve të vecuar nga njëri tjetri njësoj sikur të ishin brenda të njëjtit rrjet.
- Ka disa lloje tunelesh si PPTP, L2TP, PPPoE, IPSEC, EOIP (ky është protokoll i Mikrotik-ut), etj.
- Mënyra se si lidhen rrjetet janë kryesisht dy llojesh, site to site dhe road warrior (njeriu në terren).



IPSEC (Internet Protocol Security) është një bashkësi protokollesh me qëllim shkëmbim të mbrojtur të paketave përmes rrjeteve jo të siguruara sic është interneti.

DY FAZAT KRYESORE

Internet Key
Exchange, ndryshe
IKE (IKEv1, IKEv2)

Encapsulating
Security Payload,
EPS



Faza e parë

Në fazën e parë palët shkëmbejnë mesazhet IKE dhe krijojnë tunelin kur përputhen të dhënat (është e detyrueshme që palët të kenë të njëjtën orë)



Faza e parë

**Authentication
Method**

**Pre-shared key:
Medi!@IPsec_18VPN**

Exchange mode

Main (IKE v1) or IKE2

Lifetime

1d

Hash algorithm

Sha256

Encryption algorithm

Aes-128

DH Group

Modp 1024



Faza e dytë

Në fazën e dytë sigurohet enkriptimi



Faza e dytë

Authentication algorithm	Sha1
Encryption algorithm	3des
Lifetime	30m (1800s)
PFS Group	None
IPSEC Protocol	Esp
Tunnel	Yes



Paisjet

- Për ruterin qëndror duhet gjithmonë të shikojmë për opsionin “IPSEC Hardware Encryption”.
- Për paisjet dytësore mund edhe të përdorim ruter pa “IPSEC Hardware Encryption”.



Products

hEX

5x Gigabit Ethernet, Dual Core 880MHz CPU, 256MB RAM, USB, microSD, RouterOS L4



hEX is a five port Gigabit Ethernet router for locations where wireless connectivity is not required. The device has a full size USB port. This new updated revision of the hEX brings several improvements in performance.

It is affordable, small and easy to use, but at the same time comes with a very powerful dual core 880MHz CPU and 256MB RAM, capable of all the advanced configurations that RouterOS supports.

IPsec hardware encryption (~470 Mbps) and The Dude server package is supported, microSD slot on it provides improved r/w speed for file storage and Dude.

[Send purchase questions](#)

[Specifications](#)

[Support & Downloads](#)

[Gallery](#)

[Test results](#)



https://wiki.mikrotik.com/wiki/Manual:IP/IPsec#Hardware_acceleration

Hardware acceleration

Hardware acceleration allows to do faster encryption process by using built-in encryption engine inside CPU.

RouterBoard	DES and 3DES				AES-CBC				AES-CTR				AES-GCM			
	MD5	SHA1	SHA256	SHA512	MD5	SHA1	SHA256	SHA512	MD5	SHA1	SHA256	SHA512	MD5	SHA1	SHA256	SHA512
RBcAPGi-5acD2nD (cAP ac) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBD52G-5HacD2HnD (hAP ac ²) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBDiscG-5acD (DISC Lite5 ac) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBLDFG-5acD (LDF 5 ac) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBLHGG-5acD (LHG 5 ac) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBLHGG-5acD-XL (LHG XL 5 ac) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBLHGG-60ad (Wireless Wire Dish) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBM11G *****	yes	yes	yes	no	yes	yes	yes	no	no	no	no	no	no	no	no	no
RBM33G *****	yes	yes	yes	no	yes	yes	yes	no	no	no	no	no	no	no	no	no
RBSXTsqG-5acD (SXTsq 5 ac) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBwAPG-60ad (wAP 60G) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RBwAPG-60ad-A (wAP 60G AP) *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RB450Gx4 *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RB750Gr3 (hEX) *****	yes	yes	yes	no	yes	yes	yes	no	no	no	no	no	no	no	no	no
RB760iGS (hEX S) *****	yes	yes	yes	no	yes	yes	yes	no	no	no	no	no	no	no	no	no
RB850Gx2 **	no	no	no	no	yes	yes	yes	yes	no	no	no	no	no	no	no	no
RB1100AHx2	no	no	no	no	yes	yes	yes	yes	no	no	no	no	no	no	no	no
RB1100AHx4 and RB1100AHx4 Dude Edition	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
RB1200 ***	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	no
RB3011UIAS-RM *	no	yes	yes	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no
RB4011iGS+RM and RB4011iGS+5HacQ2HnD-IN	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Cloud Core Router series	yes	yes	yes	no	yes	yes	yes	no	yes	yes	yes	no	no	no	no	no

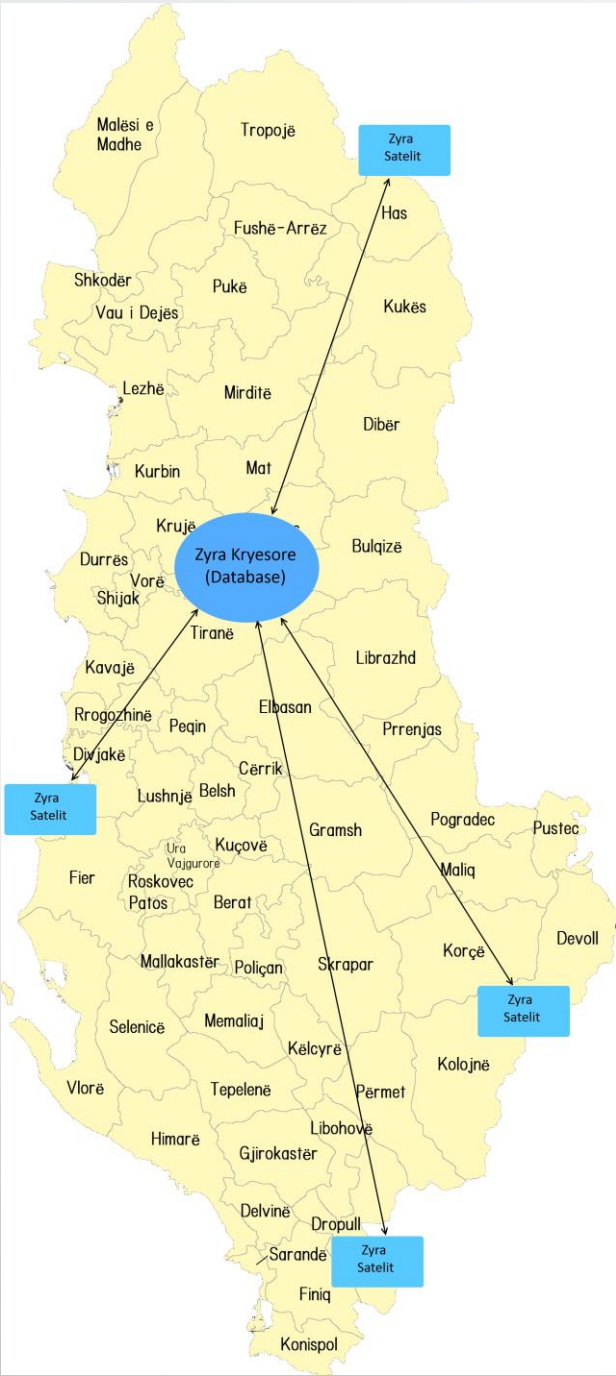
RB3011 që nga versioni 6.43.1 ROS



IPsec Performance

Packet size | 400 bytes, speed in Mbps

Mode	Configuration	hEX	RB1100	CCR1009	CCR1036
1 tunnel	AES-128-CBC + SHA1	469.3	1366.4	1260.0	1461.6
256 tunnels	AES-128-CBC + SHA1	469.3	2158.2	2599.5	10224.5
	AES-128-CBC + SHA256	472.6	2154.9	2599.5	10110.2
	AES-256-CBC + SHA1	358.4	2016.0	2576.0	10091.2
	AES-256-CBC + SHA256	359.5	2016.0	2576.0	9996.0





Percaktimi i broadcast domain

- Duhet planifikuar mirë paraprakisht broadcast domain për secilin rrjet.
 - Zyra Qëndrore: 192.168.0.0/24
 - Zyra e parë: 192.168.5.0/24
 - Zyra e dytë: 192.168.10.0/24
 - Zyra e tretë: 192.168.15.0/24



- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rtf
- Manual
- New WinBox
- Exit

IPsec					
Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users					
+ - ✓ ✗ 📁 🔍					
Address / Port		Propos...	Hash Al...	Encrypt...	
::: L2tp IPSEC					
X	0.0.0.0/0	obey	sha1	3des a...	
	1.1.1.1	obey	sha1	3des a...	
X					
R	::/0	obey	sha1	3des a...	
DR	::/0	obey	sha1	3des a...	

6 items (1 selected)

IPsec Peer <1.1.1.1>

General Advanced Encryption

Address: 1.1.1.1

Port:

Local Address:

Auth. Method: pre shared key

Exchange Mode: main

☐ Passive

Secret:

enabled responder

OK Cancel Apply Disable Comment Copy Remove



- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rtf
- Manual
- New WinBox
- Exit

IPsec					
Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users					
Address	Port	Propos...	Hash Al...	Encrypt...	
::: L2tp IPSEC					
X 0.0.0.0/0		obey	sha1	3des a...	
1.1.1.1		obey	sha1	3des a...	
R ::/0		obey	sha1	3des a...	
DR ::/0		obey	sha1	3des a...	

6 items (1 selected)

IPsec Peer <1.1.1.1>

General

Advanced

Encryption

Policy Template Group: default

Notrack Chain:

☒ Send Initial Contact

☐ NAT Traversal

My ID Type: auto

Mode Configuration:

Generate Policy: no

Lifetime: 1d 00:00:00

Lifeytes:

DPD Interval: 120 s

DPD Maximum Failures: 5

Proposal Check: obey

Compatibility Options: ☐ skip peer id validation

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled

responder



- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.tif
- Manual
- New WinBox
- Exit

IPsec					
Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users					
	Address	Port	Propos...	Hash Al...	Encrypt...
::: L2tp IPSEC					
X	0.0.0.0/0		obey	sha1	3des a...
	1.1.1.1		obey	sha1	3des a...
R	::/0		obey	sha1	3des a...
DR	::/0		obey	sha1	3des a...
6 items (1 selected)					

IPsec Peer <1.1.1.1>

General Advanced Encryption

Hash Algorithm: sha1

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
☐ ecp256 ☐ ecp384
☐ ecp521

enabled responder

OK Cancel Apply Disable Comment Copy Remove



WinBox v6.42.9 on hAP ac lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.2.2

Quick Set

CAPsMAN

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Partition

Make Supout.tif

Manual

New WinBox

Exit

IPsec

Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users

+

-

✓

✗

⌵

Find

Name	Auth. Algorithms	Encr. Algorithms	Lifetime	PFS Group
toni1	sha1	3des	00:30:00	none

4 items (1 selected)

IPsec Proposal <toni1>

Name: toni1

Auth. Algorithms:

☐ md5

☒ sha1

☐ null

☐ sha256

☐ sha512

Encr. Algorithms:

☐ null

☒ 3des

☐ aes-128 cbc

☐ aes-192 cbc

☐ blowfish

☐ camellia-128

☐ camellia-256

☐ aes-192 ctr

☐ aes-128 gcm

☐ aes-256 gcm

☐ des

☐ aes-128 cbc

☐ aes-256 cbc

☐ twofish

☐ camellia-192

☐ aes-128 ctr

☐ aes-256 ctr

☐ aes-192 gcm

☐ aes-256 gcm

Lifetime: 00:30:00

PFS Group: none

enabled

OK

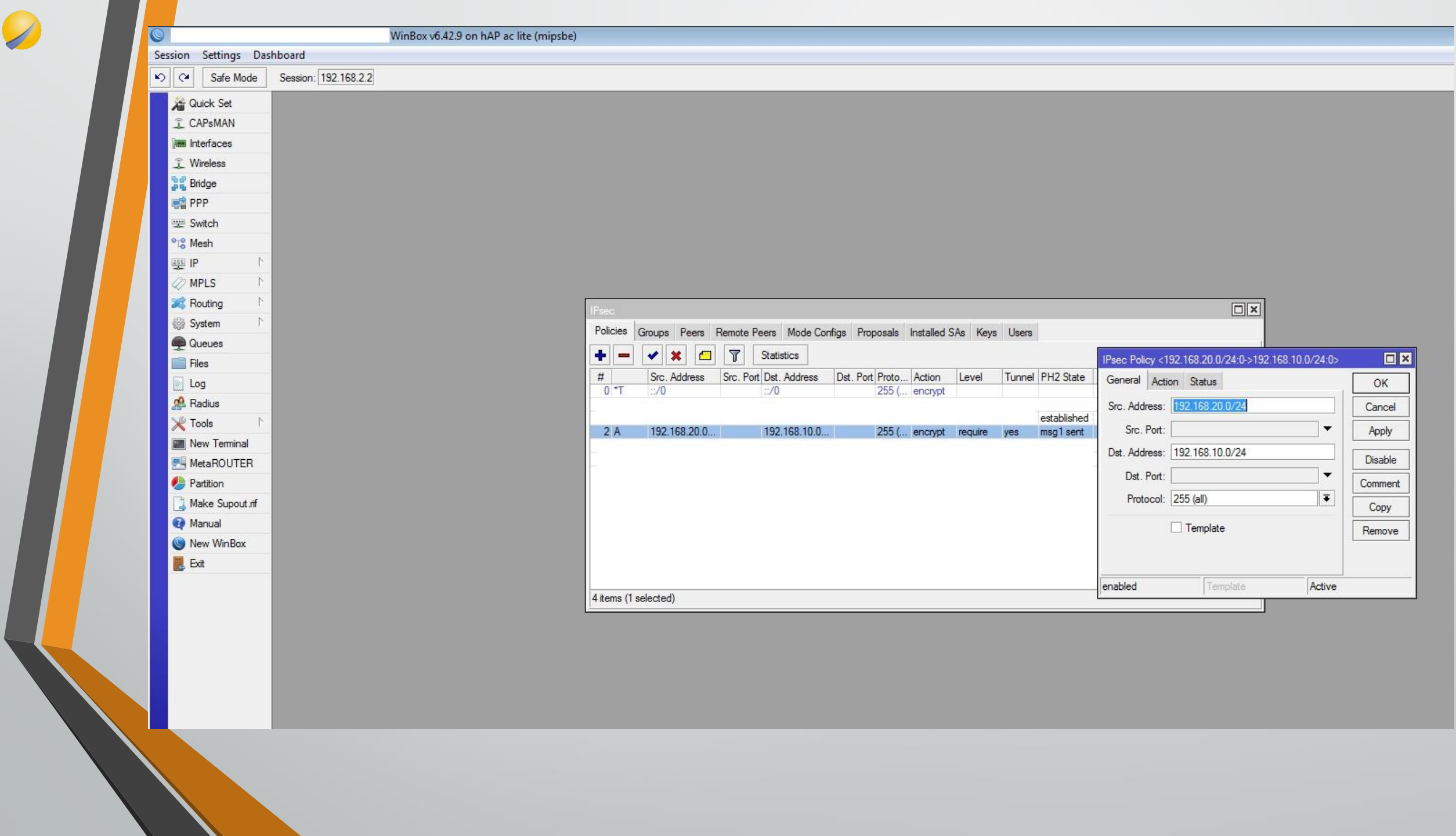
Cancel

Apply

Disable

Copy

Remove



- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rif
- Manual
- New WinBox
- Exit

IPsec										
Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users										
+ - ✓ ✗ 📁 📊 Statistics										
#	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel	PH2 State	
0	T	::/0		::/0	255 (...)	encrypt				
2	A	192.168.20.0...	192.168.10.0...		255 (...)	encrypt	require	yes	established	msg1 sent

4 items (1 selected)

IPsec Policy <192.168.20.0/24>192.168.10.0/24>

General

Action

Status

Src. Address: 192.168.20.0/24

Src. Port:

Dst. Address: 192.168.10.0/24

Dst. Port:

Protocol: 255 (all)

☐ Template

enabled

Template

Active

OK

Cancel

Apply

Disable

Comment

Copy

Remove



WinBox v6.42.9 on hAP ac lite (mipsbe)

Session Settings Dashboard

↶ ↷

Safe Mode

Session: 192.168.2.2

Quick Set

CAPsMAN

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Partition

Make Supout.tif

Manual

New WinBox

Exit

IPsec

Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users

+ - ✓ ✗ 📄 🔍

Statistics

#	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
2	192.168.20.0...		192.168.10.0...	255 (...)	encrypt	require	yes	

4 items (1 selected)

IPsec Policy <192.168.20.0/24:0>192.168.10.0/24:0>

General Action Status

Action: encrypt

Level: require

IPsec Protocols: esp

☒ Tunnel

SA Src. Address: 1.1.1.1

SA Dst. Address: 2.2.2.2

Proposal: toni1

OK

Cancel

Apply

Disable

Comment

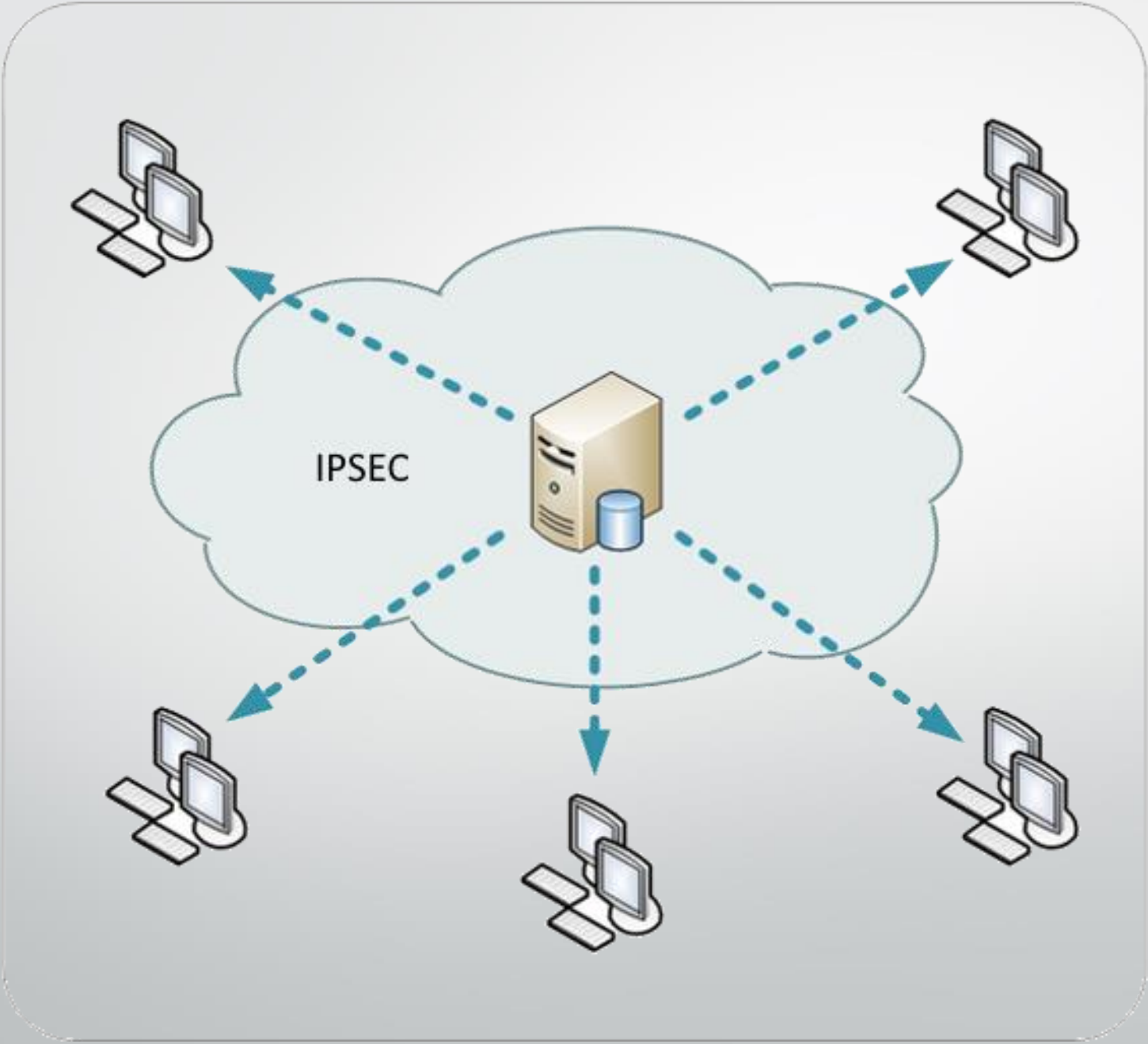
Copy

Remove

enabled

Template

Active



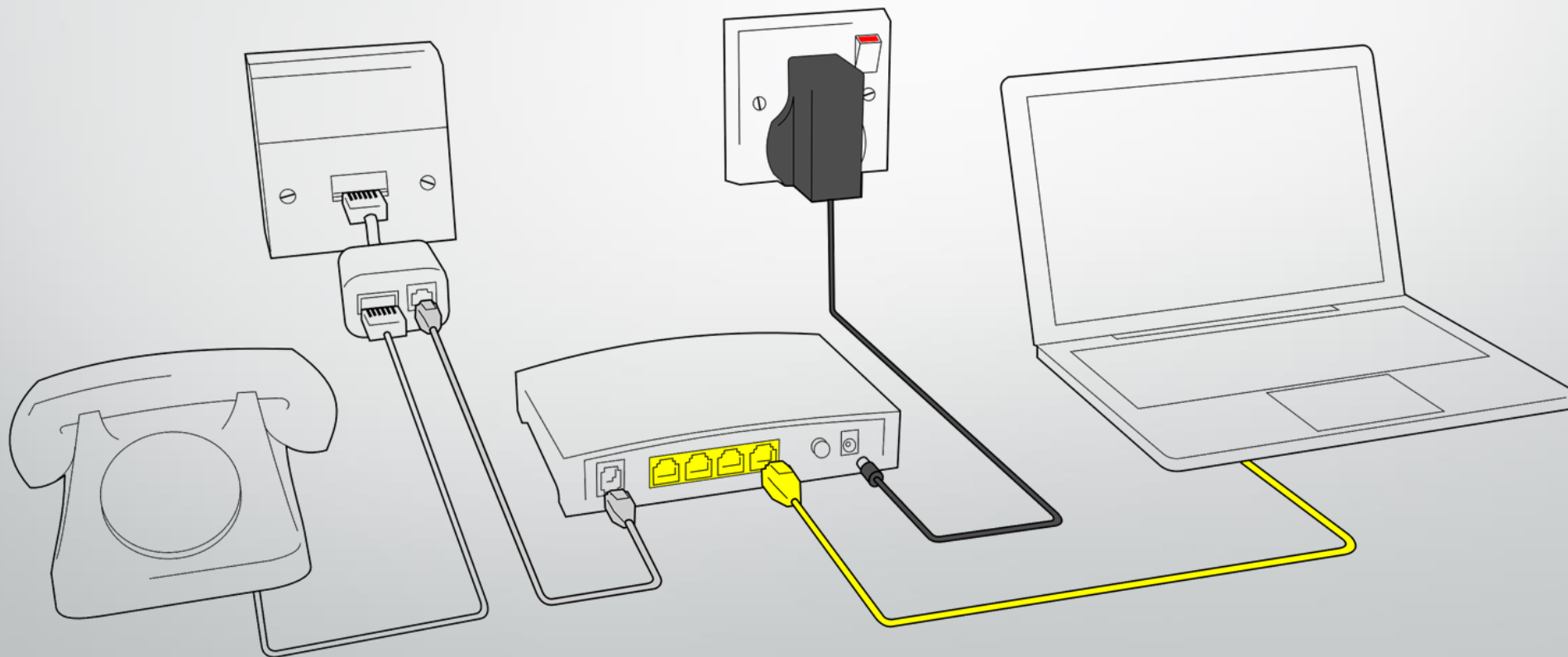


Njeriu në terren

- Është punonjës në lëvizje, si rrjedhim ka IP dinamike dhe shpesh herë pas një ruteri
- Për tu lidhur do përdorim L2TP me IPSEC



Konfigurimi në ruter





- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.tif
- Manual
- New WinBox
- Exit

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

+ - ✓ ✕ [icon] [filter]

PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server PPPoE Scan

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)
DR <><2p-toni1234>	L2TP Server Binding	1300		0 bps	0 bps	0

1 item out of 12

L2TP Server

☒ Enabled

Max MTU: 1460

Max MRU: 1460

MRRU: [dropdown]

Keepalive Timeout: 30

Default Profile: default-encryption

Max Sessions: [dropdown]

Authentication: ☒ mschap2 ☒ mschap1
☒ chap ☒ pap

Use IPsec: yes

IPsec Secret: ens.ipsec

Caller ID Type: number

☐ One Session Per Host

☐ Allow Fast Path

OK Cancel Apply

IPsec

Policies Groups Peers Remote Peers Mode

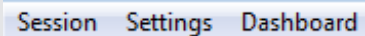
+ - ✓ ✕ [icon] [filter]

Address	Port	Propos...	Hash Al...
DR ::/0		obey	sha1

[icon] [x]

Find

[dropdown]



Safe Mode

Session: 192.168.2.2

 Quick Set CAPsMAN

Interfaces

 Wireless Bridge PPP Switch

 Mesh

 MPLS Routing System Queues

Files

 Log

 Radius

 Tools New Terminal MetaROUTER Partition Make Supout.tif

 [Manual](#)

 New WinBox Exit

IP Pool

Pools

Used Addresses



Find

Name	Addresses	Next Pool
dhcpcd_pool1	192.168.2.50-192.168.2.200	none
dhcpcd_pool2	192.168.3.50-192.168.3.254	none
ipsec	172.16.30.100-172.16.30.254	none

3 items



- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.tif
- Manual
- New WinBox
- Exit

PPP Profile <profile1>

General

Protocols

Limits

Queue

Scripts

Name: profile1

Local Address: 172.16.30.1

Remote Address: ipsec

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server:

WINS Server:

- Change TCP MSS

☐ no ☒ yes ☐ default

- Use UPnP

☐ no ☐ yes ☒ default

OK

Cancel

Apply

Comment

Copy

Remove

PPP

Interface

PPPoE Servers

Secrets

Profiles

Active Connections

L2TP Secrets

Name	Local Address	Remote Address	Bridge	Rate Limit...	Only One
default					default
default-encr...					default
profile1	172.16.30.1	ipsec			default

3 items (1 selected)



Safe Mode

Session: 192.168.2.2

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.tif
- Manual
- New WinBox
- Exit

PPP Secret <toni1234>

Name:

Password:

Service:

Caller ID:

Profile:

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK Cancel Apply Disable Comment Copy Remove

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting						
Name	Password	Service	Caller ID	Profile	Local Address	Remote Address
toni1234	toni1234	l2tp		profile1		

1 item (1 selected)



Konfigurimi në...



Windows 7



 Control Panel > All Control Panel Items > Network and Sharing Center

Search Control Panel 

[Control Panel Home](#)
[Change adapter settings](#)
[Change advanced sharing settings](#)

View your basic network information and set up connections


PC
(This computer)


Network


Internet

[See full map](#)

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

**Network**
Public network

Access type: Internet
Connections:  Local Area Connection

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.

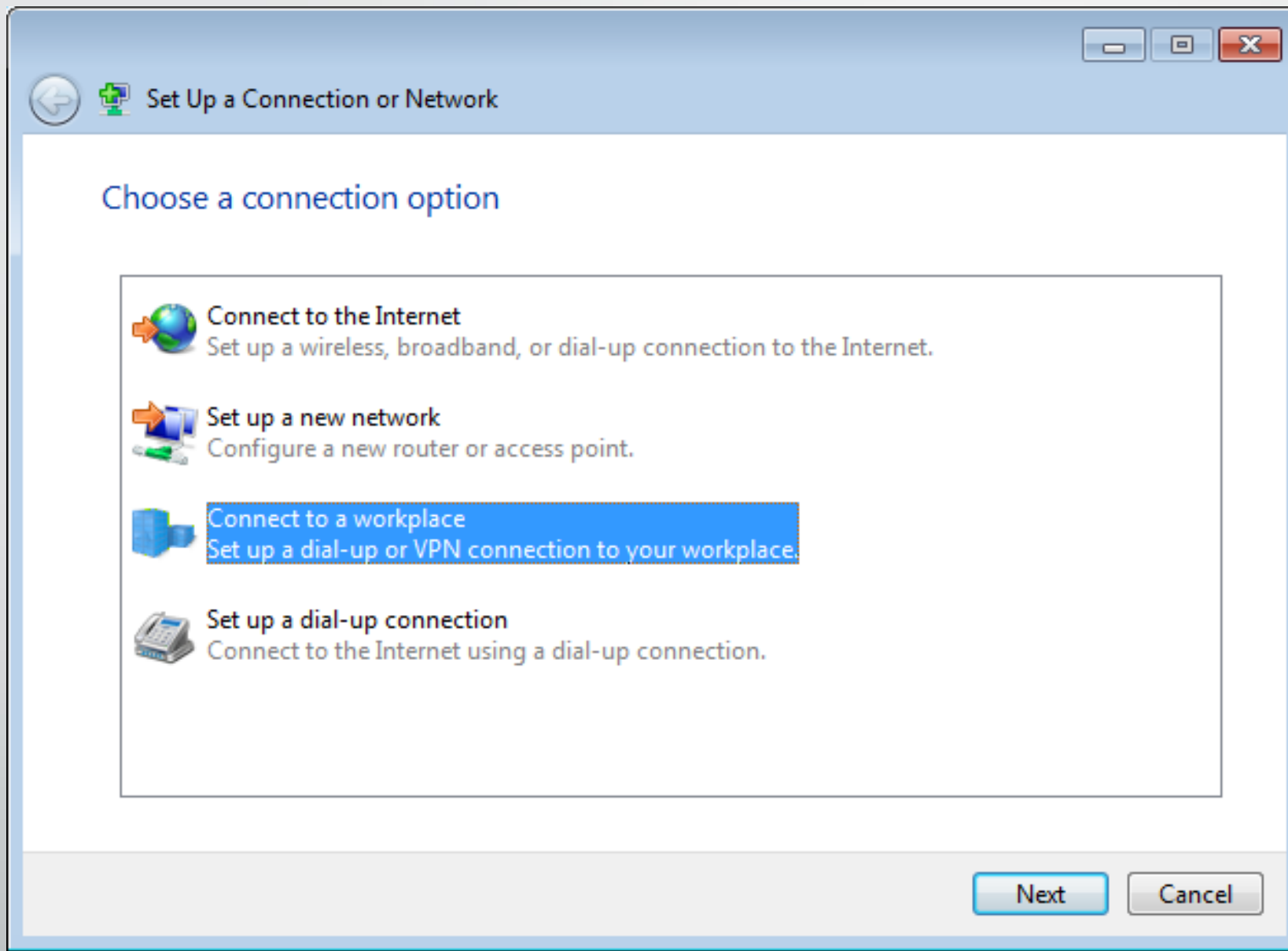
 [Connect to a network](#)
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

 [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](#)
[Internet Options](#)
[Windows Firewall](#)





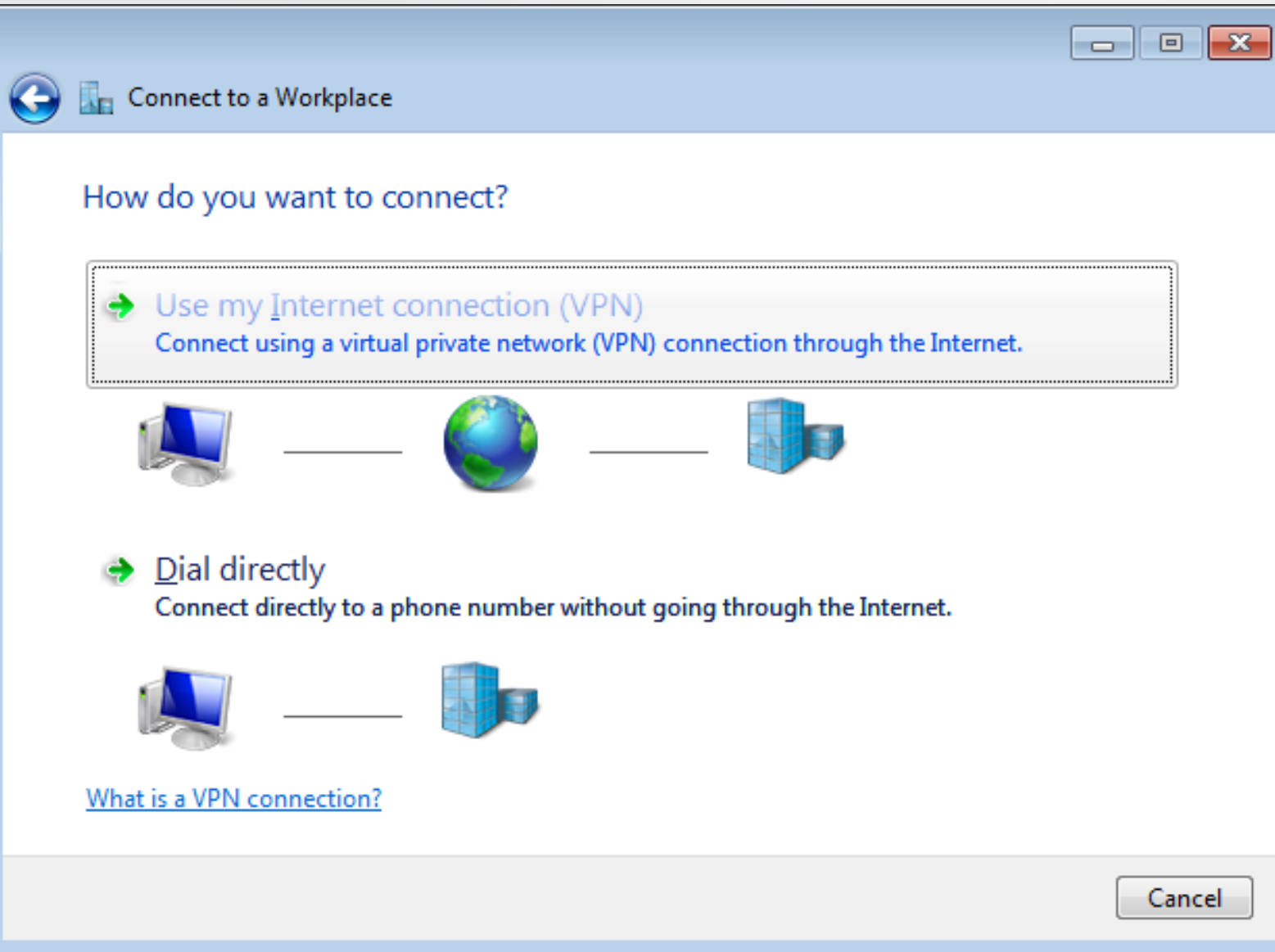
Connect to a Workplace

Do you want to use a connection that you already have?

☒ No, create a new connection

☐ Yes, I'll choose an existing connection

Next Cancel





 Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

1.1.1.1

Destination name:

VPN Connection

☐ Use a smart card

☐  Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☐ Don't connect now; just set it up so I can connect later

Next

Cancel



 Connect to a Workplace

Type your user name and password

User name:

toni1234

Password:

●●●●●●●●

☐ Show characters

☐ Remember this password

Domain (optional):

Connect

Cancel



Control Panel > Network and Internet > Network Connections

Search Network Connections

Organize Start this connection Rename this connection Delete this connection Change settings of this connection

Connect VPN Connection

VPN Connection Properties

VPN Connection Disconnected WAN Miniport (IKEv2)

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

Save this user name and password for the following users:

- ☐ Me only
- ☒ Anyone who uses this computer

Connect Cancel Properties Help

Advanced Properties

L2TP

- ☒ Use preshared key for authentication
 - Key: ens.ipsec
- ☐ Use certificate for authentication
 - ☒ Verify the Name and Usage attributes of the server's certificate

OK Cancel

Konfigurimi ne Android Samsung SM-A320FL





< MORE CONNECTION SETTINGS

Nearby device scanning
Off

Printing

MirrorLink
Connect your device to your car to access useful
apps safely while driving.

VPN
Set up and manage Virtual Private Networks (VPNs).

Ethernet

Edit VPN network

Name
ENS

Type
L2TP/IPSec PSK ▼

Server address
1.1.1.1

L2TP secret
Not used

IPSec identifier
Not used

IPsec pre-shared key
.....

☐ Show advanced options

Username

DELETE CANCEL SAVE

Edit VPN network

L2TP secret
Not used

IPSec identifier
Not used

IPsec pre-shared key
.....

☐ Show advanced options

Username
toni1234

Password
.....

☒ Always-on VPN

A DNS server must be specified to use
Always-on VPN.

DELETE CANCEL SAVE



Key

Envelope

4G+ 93% 10:05

Menu

Home

LAN

Close

Share

Cloud

Search

More

LAN > 192.168.2.40

usbstorage Folder	dr-	N/A	
public Folder	dr-	N/A	
IPC\$ Folder	drw	N/A	
caci Folder	dr-	N/A	

Session Settings Dashboard



Safe Mode

Session: 192.168.2.2

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: special dummy rule to show fasttrack counters											
0	D	pas...	forward							0 B	0
::: Test mbyllje nga jashte											
1	✓ acc...	input								884.1 KB	13 163
2	✓ acc...	input								1820 B	10
3	✓ acc...	input			1 (icmp)					52.0 KB	329
4	✓ acc...	input			17 (udp)		500			2256 B	3
5	✓ acc...	input			17 (udp)		4500			13.7 KB	44
6	✓ acc...	input			50 (ipsec...					0 B	0
7	✓ acc...	input			17 (udp)		1701			97 B	1
8	✗ drop	input						ether1		65.4 KB	400

46 items (1 selected)



Faleminderit