IP Security

IPSec, PPTP, OpenVPN

Pawel Cieplinski, AkademiaWIFI.pl

MUM Wroclaw

Introduction

www.AkademiaWIFI.pl

WCNG - Wireless Network Consulting Group

We are group of experienced professionals. Our company Mission is:

- Provide Professional training
- Support local business
- Help our customers with their service quality

Security in Internet

Due To rapid expanion of IPv4 inter-networks people was concern about ensuring security.

First Oportunity to think about security in Internet was while IPv6 was developed.

We still do not have IPv6 commonly used, but need for security is **NOW**

IPSec

- IPSec is not a protocol, but a set of services

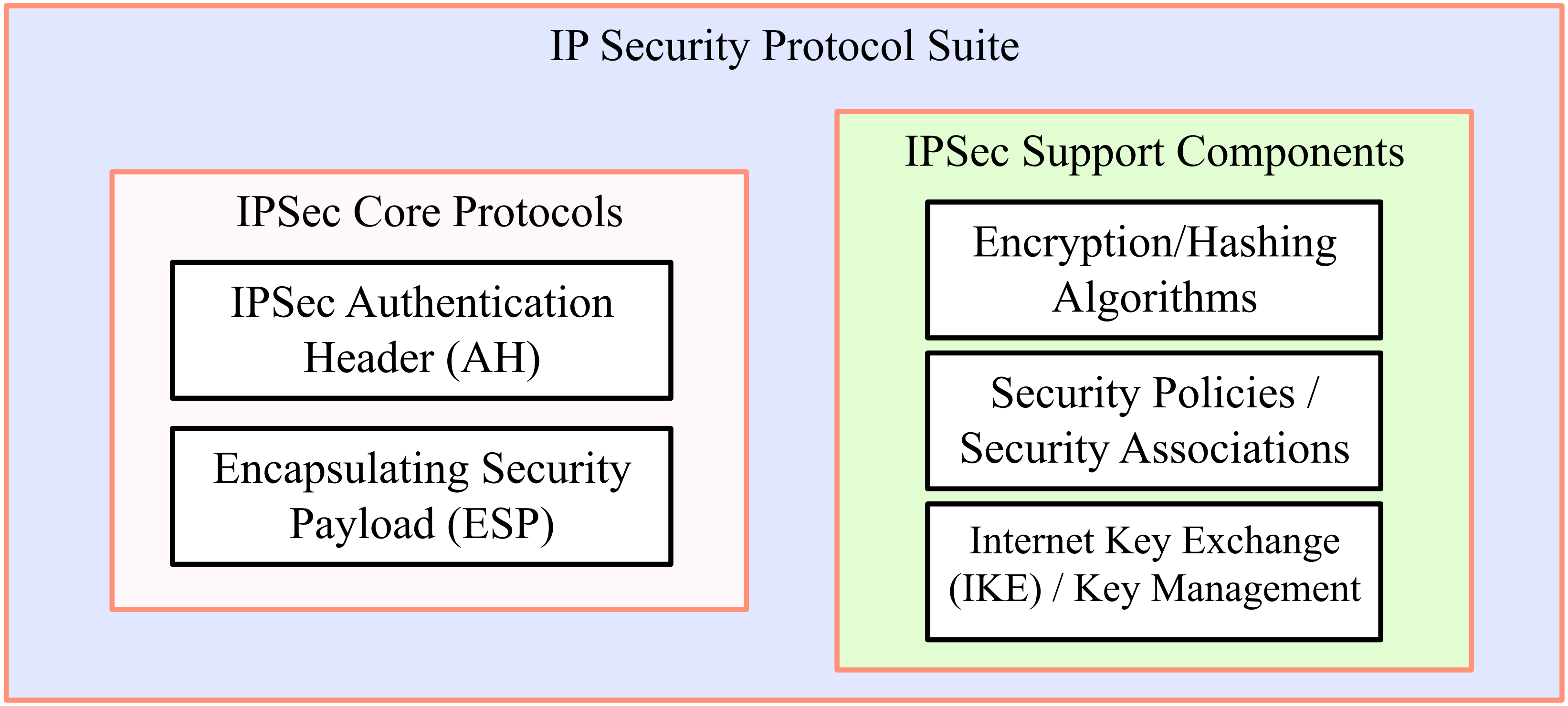
- Provides various types of protection such as:
  - Encryption of user data for privacy
  - Authentication of the integrity of a message
  - Protection for various types of attack such as replay attack
  - Ability to negotiate key and security algorithms
  - Two security modes: Tunnel and Transport

IPSec General Operation

Devices to work using IPSec must:

- They must agree on a set of security protocols to use, so that each one sends data in a format the other can understand.
- They must decide on a specific encryption algorithm
- They must exchange keys that are used to “unlock” data that has been cryptographically encoded.

IPSec Protocols



IP Security Protocol Suite

IPSec Core Protocols

IPSec Authentication Header (AH)

Encapsulating Security Payload (ESP)

IPSec Support Components

Encryption/Hashing Algorithms

Security Policies / Security Associations

Internet Key Exchange (IKE) / Key Management

IPSec Implementation Methods

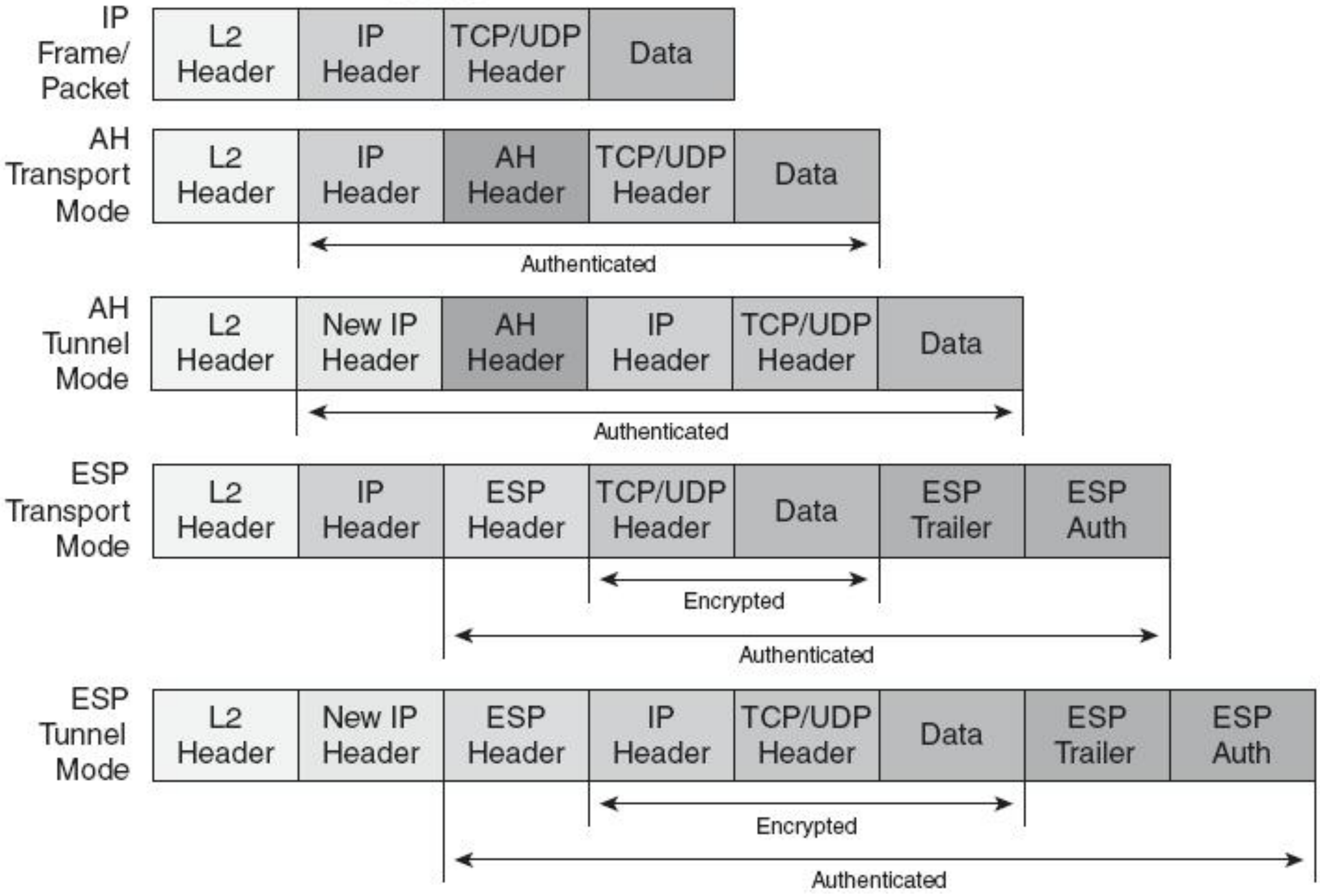
There are many implementation methods, based on various factors.

There are two option to implement IPsec on End-Hosts or on Routers

- End-host implementation:
  - Putting IPsec into all hosts gives more flexibility

- Router implementation:
  - This option is much less work

Ipsec Modes



IP Frame/ Packet: L2 Header | IP Header | TCP/UDP Header | Data

AH Transport Mode: L2 Header | IP Header | AH Header | TCP/UDP Header | Data

Authenticated

AH Tunnel Mode: L2 Header | New IP Header | AH Header | IP Header | TCP/UDP Header | Data

Authenticated

ESP Transport Mode: L2 Header | IP Header | ESP Header | TCP/UDP Header | Data | ESP Trailer | ESP Auth

Encrypted

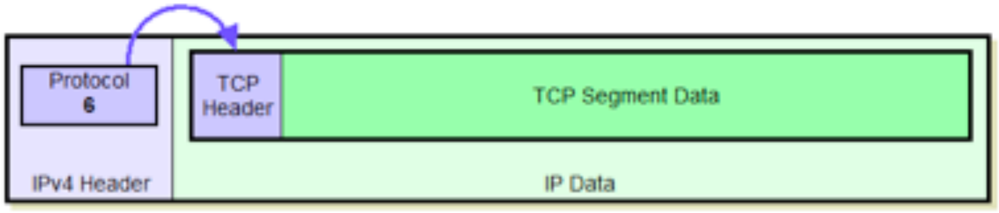
Authenticated

ESP Tunnel Mode: L2 Header | New IP Header | ESP Header | IP Header | TCP/UDP Header | Data | ESP Trailer | ESP Auth

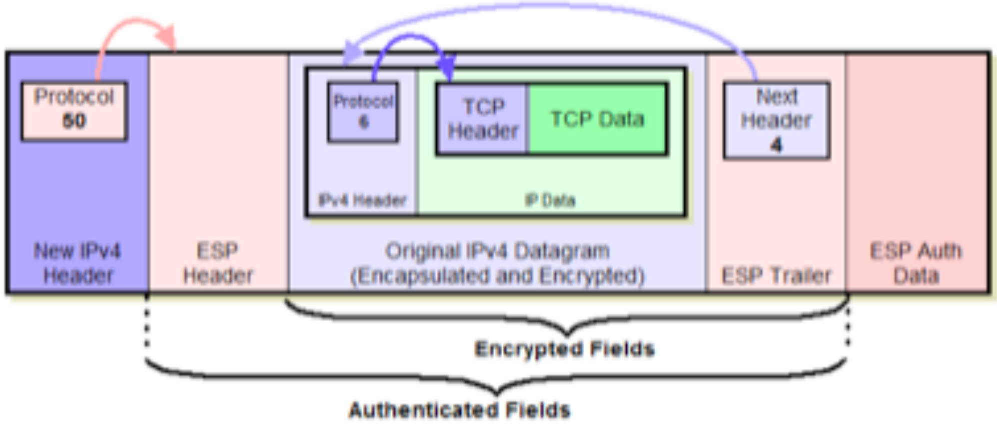
Encrypted

Authenticated

Encryption Security Payload

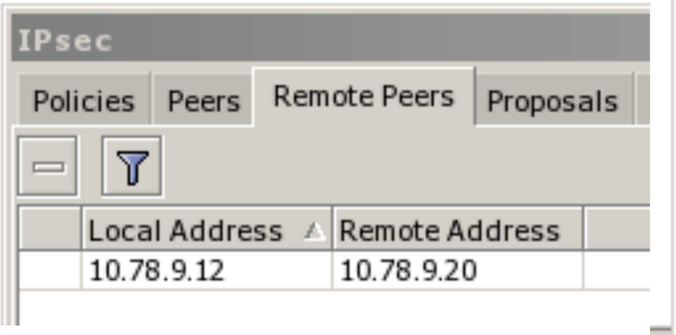


Original IPv4 Datagram Format

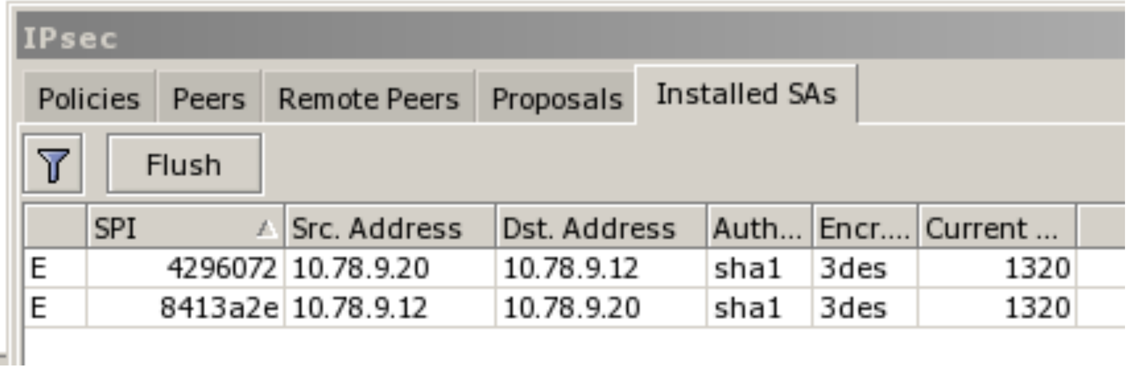


How to Configure IPSec on RouterOS

- To turn IPsec on between two Routers in transport we need to specify policy and peer using following commands:
- / ip ipsec policy add sa-src-address=[*router_src_addr]* *sa-dst-address=[router_dst_addr]* action=encrypt
- / ip ipsec peer add address=*[router_dst_addr]* secret=*"shared secret"*



	Local Address	Remote Address
	10.78.9.12	10.78.9.20



	SPI	Src. Address	Dst. Address	Auth...	Encr....	Current ...
E	4296072	10.78.9.20	10.78.9.12	sha1	3des	1320
E	8413a2e	10.78.9.12	10.78.9.20	sha1	3des	1320

IPSec in real life scenarios

- Due to complexity of IPSec and some limitation in IPv4, another VPN protocols emerged like:

- PPTP
- L2TP
- OpenVPN
- Many Priopríetary Protocols

PPTP - Point to Point Tunneling Protocol

- PPTP is extension to PPP protocol described in RFC 2637 in July 1999. It was developed by Microsoft, Ascend Communication (today Alcatel-Lucent) and 3com
- PPTP do not specify authentication and encryption. Those features relies on PPP protocol
- The intended use of this protocol is to provide similar levels of security and remote access as typical VPN products.

PPTP Specification

- PPTP Tunnel is started by communication to peer using TCP port 1723. This TCP connection is a management connection to second GRE tunnel to same peer.
- GRE is used to carry standard PPP packets, allowing to transport any protocol like IP, IPX, NetBEUI
- Microsoft implementation allow tunneled traffic to be authenticated using PAP, CHAP, MS-CHAPv1/2 and TLS
- PPP is encrypted using Microsoft Point to Point Encryption (MPPE)

PPTP Security

- Using PPTP is very tempting due to fact there is a client in Windows. However first implementation of PPTP was very weak, some of its weaknesses:

- MS-CHAPv1 is fundamentally insecure. Tools exists to extract passwords from captured MS-CHAP exchange

- MS-CHAPv2 is vulnerable to dictionary attack on the captured challenge response packets. Tools exist to perform this process rapidly

Open VPN

- OpenVPN is a free and open source (GPL) software application that implements virtual private network (VPN) solutions for creating secure point-to-point or site-to-site connections

- OpenVPN uses OpenSSL library and support SSLv3/ TLSv1 protocol, and contain many security and control features

- Goal of creating OpenVPN was „usability first”

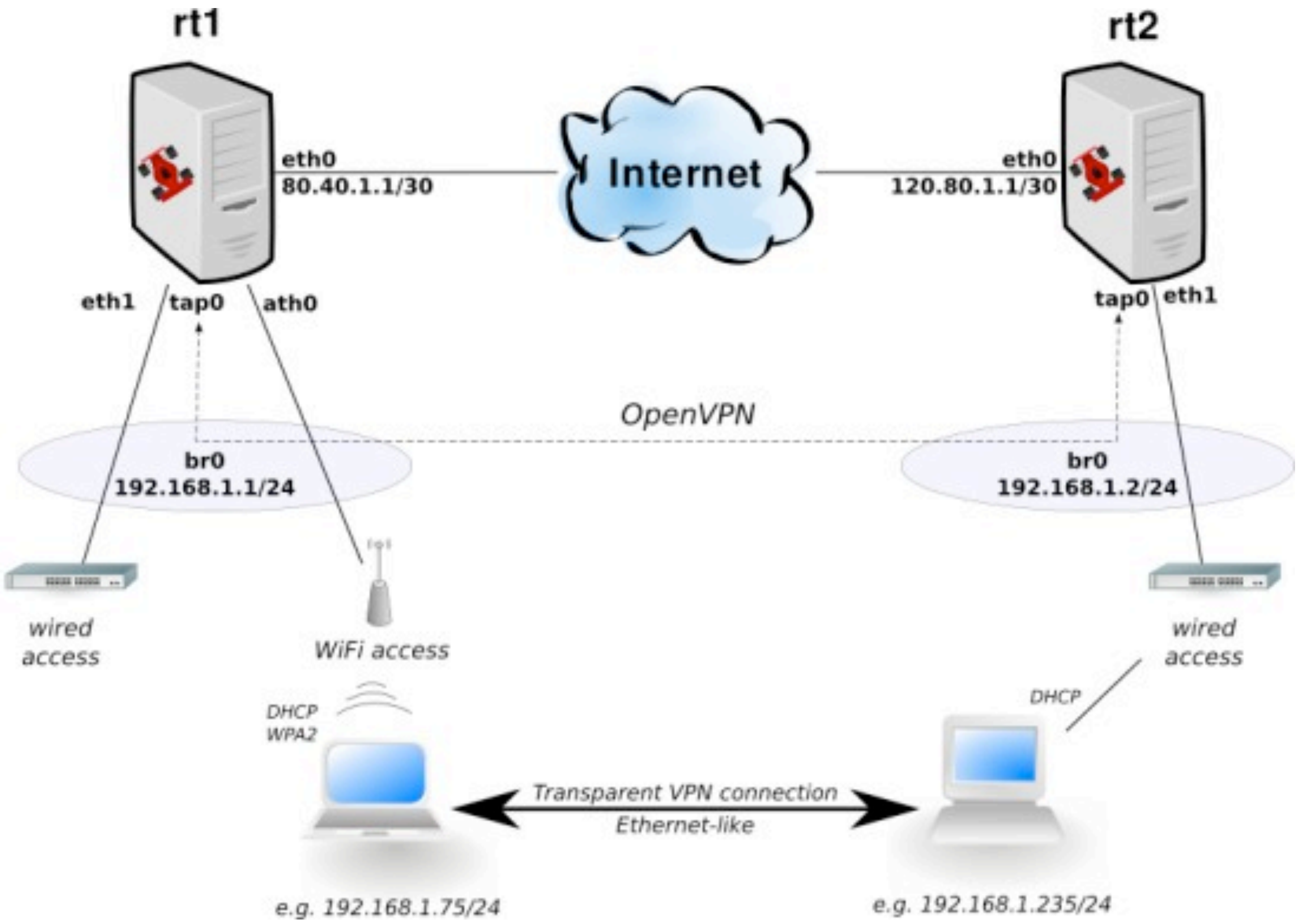
OpenVPN Specification

- Unlike most VPN, SSL runs in userspace enabling secure and reliable without complexity of VPN’s run on network level
- SSL encapsulates IP in UDP or TCP sent from virtual tun/tap interfaces and send it over the network.

OpenVPN Features

- OpenVPN tries to take advantage of all the capabilities which are possible to a user space VPN.
- Portability.
- Familiar daemon-style usage.
- No kernel modifications required.
- State-of-the-art cryptography layer provided by the OpenSSL library.

OpenVPN Specification



Advantages of OpenVPN

- OpenVPN connections can be tunneled through almost every firewall and proxy
- Only one port in the firewall must be opened to allow incoming connections
- No problems with NAT
- Transparent, high-performance support for dynamic IPs
- Simple installation on any platform
- Very active community

Mikrotik and OpenVPN

- RouterOS has only partial implementation of OpenVPN

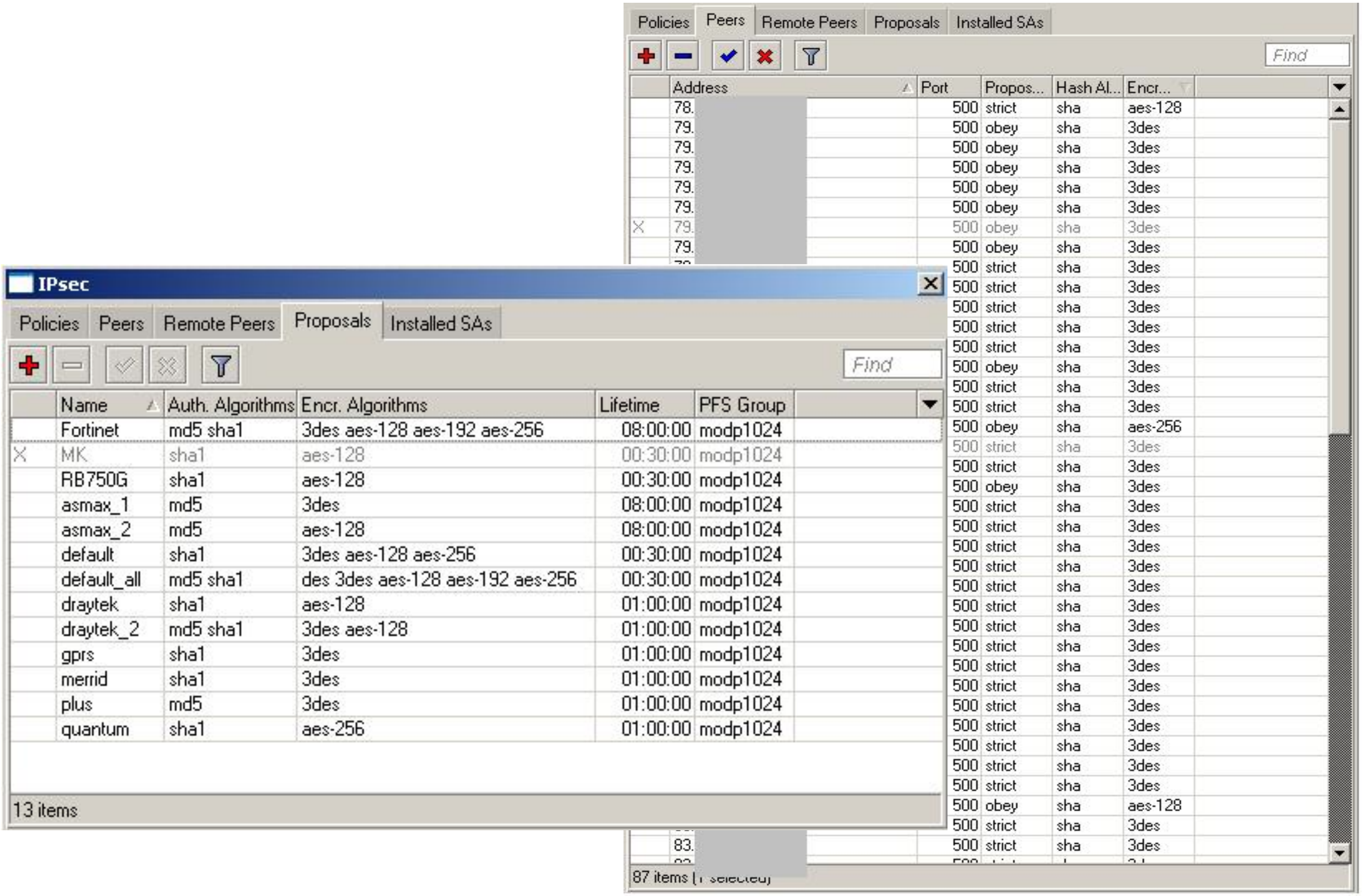
- Supported Features
  - TCP
  - bridging (tap)
  - routing (tun)
  - certificates
  - p2p mode

- Unsupported Features
  - UDP
  - LZO compression
  - server mode

Head to Head

	Ipsec	PPTP	OpenVPN
Complexity	Complex	Simple	Medium
Support for certificates	Yes	No	Yes
Authentication	Packet	Session	Packet or Session
Encryption	DES,3DES,AES	MPPE	Blowfish, AES
Bridge support	Yes*	Yes (with BCP)	Yes
Tunnel support	Yes	Yes	Yes
Transport mode	Yes	No	No

Real Life Example with RB1000



	Address	Port	Propos...	Hash Al...	Encr...
	78. [redacted]	500	strict	sha	aes-128
	79. [redacted]	500	obey	sha	3des
	79. [redacted]	500	obey	sha	3des
	79. [redacted]	500	obey	sha	3des
	79. [redacted]	500	obey	sha	3des
	79. [redacted]	500	obey	sha	3des
X	79. [redacted]	500	obey	sha	3des
	79. [redacted]	500	obey	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	obey	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	obey	sha	aes-256
		500	strict	sha	3des
		500	strict	sha	3des
		500	obey	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	strict	sha	3des
		500	obey	sha	aes-128
		500	strict	sha	3des
	83. [redacted]	500	strict	sha	3des

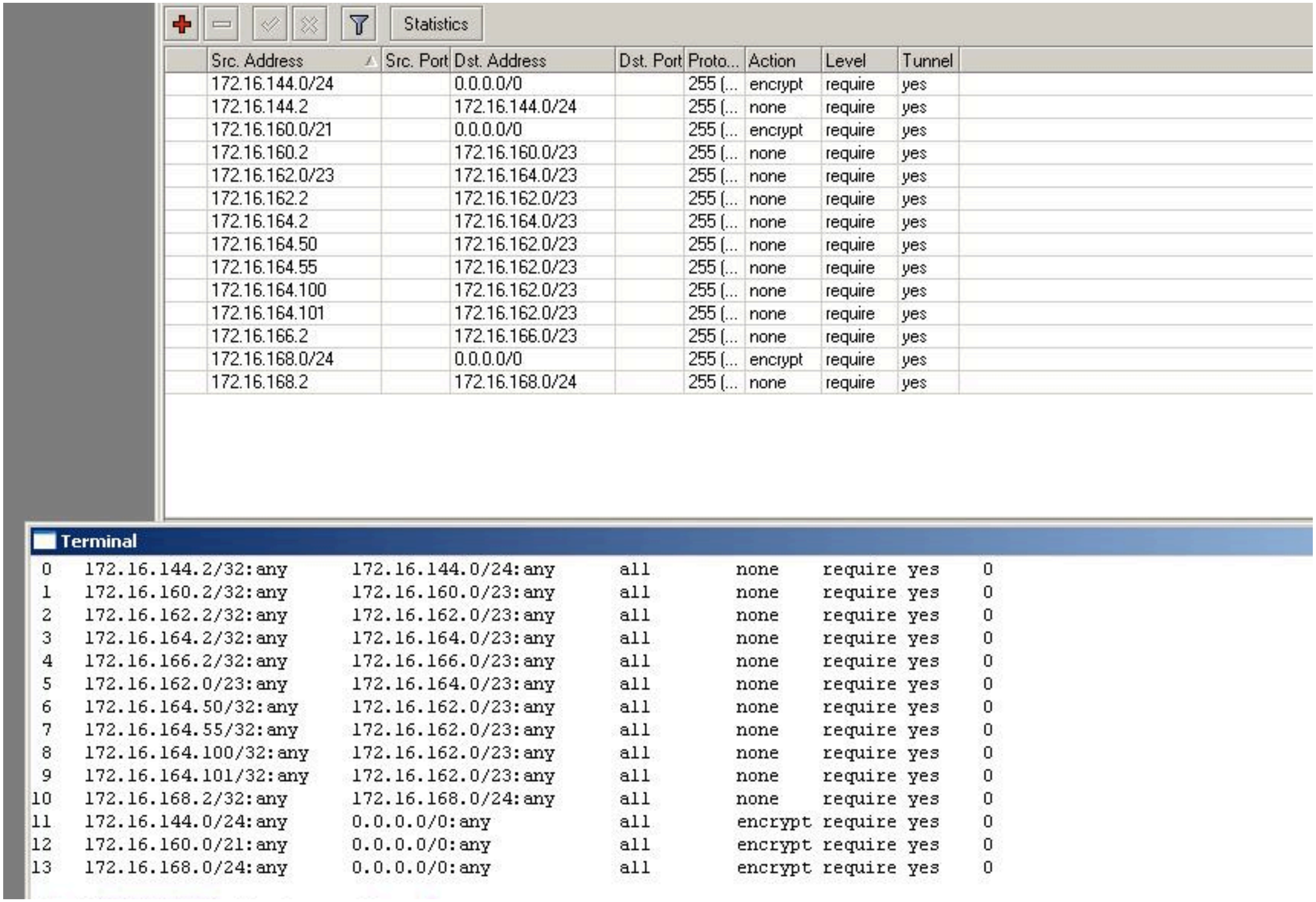
87 items [redacted]

IPsec

	Name	Auth. Algorithms	Encr. Algorithms	Lifetime	PFS Group
	Fortinet	md5 sha1	3des aes-128 aes-192 aes-256	08:00:00	modp1024
X	MK	sha1	aes-128	00:30:00	modp1024
	RB750G	sha1	aes-128	00:30:00	modp1024
	asmax_1	md5	3des	08:00:00	modp1024
	asmax_2	md5	aes-128	08:00:00	modp1024
	default	sha1	3des aes-128 aes-256	00:30:00	modp1024
	default_all	md5 sha1	des 3des aes-128 aes-192 aes-256	00:30:00	modp1024
	draytek	sha1	aes-128	01:00:00	modp1024
	draytek_2	md5 sha1	3des aes-128	01:00:00	modp1024
	gprs	sha1	3des	01:00:00	modp1024
	merrid	sha1	3des	01:00:00	modp1024
	plus	md5	3des	01:00:00	modp1024
	quantum	sha1	aes-256	01:00:00	modp1024

13 items

Real Life Example with RB1000

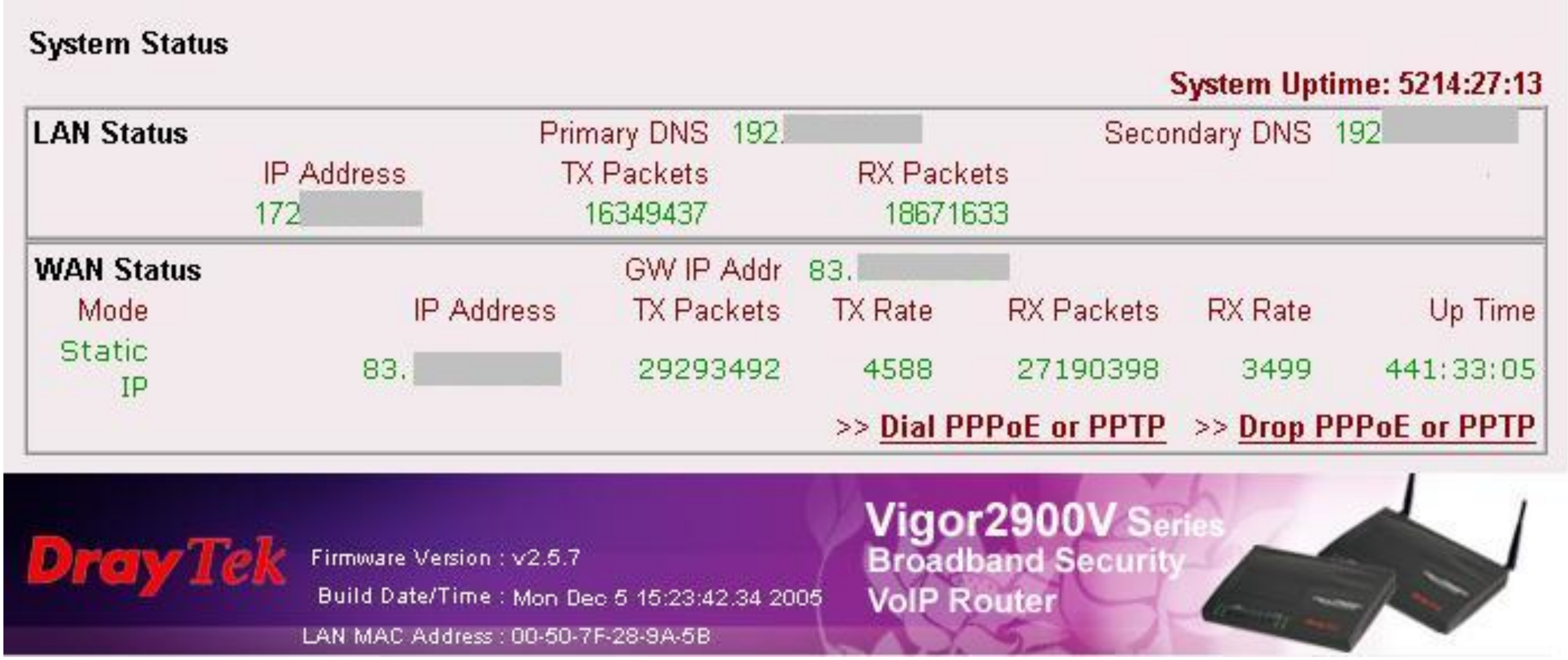


	Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel
	172.16.144.0/24		0.0.0.0/0		255 (...	encrypt	require	yes
	172.16.144.2		172.16.144.0/24		255 (...	none	require	yes
	172.16.160.0/21		0.0.0.0/0		255 (...	encrypt	require	yes
	172.16.160.2		172.16.160.0/23		255 (...	none	require	yes
	172.16.162.0/23		172.16.164.0/23		255 (...	none	require	yes
	172.16.162.2		172.16.162.0/23		255 (...	none	require	yes
	172.16.164.2		172.16.164.0/23		255 (...	none	require	yes
	172.16.164.50		172.16.162.0/23		255 (...	none	require	yes
	172.16.164.55		172.16.162.0/23		255 (...	none	require	yes
	172.16.164.100		172.16.162.0/23		255 (...	none	require	yes
	172.16.164.101		172.16.162.0/23		255 (...	none	require	yes
	172.16.166.2		172.16.166.0/23		255 (...	none	require	yes
	172.16.168.0/24		0.0.0.0/0		255 (...	encrypt	require	yes
	172.16.168.2		172.16.168.0/24		255 (...	none	require	yes

Terminal

```
 0   172.16.144.2/32:any     172.16.144.0/24:any     all        none    require yes     0
 1   172.16.160.2/32:any     172.16.160.0/23:any     all        none    require yes     0
 2   172.16.162.2/32:any     172.16.162.0/23:any     all        none    require yes     0
 3   172.16.164.2/32:any     172.16.164.0/23:any     all        none    require yes     0
 4   172.16.166.2/32:any     172.16.166.0/23:any     all        none    require yes     0
 5   172.16.162.0/23:any     172.16.164.0/23:any     all        none    require yes     0
 6   172.16.164.50/32:any    172.16.162.0/23:any     all        none    require yes     0
 7   172.16.164.55/32:any    172.16.162.0/23:any     all        none    require yes     0
 8   172.16.164.100/32:any   172.16.162.0/23:any     all        none    require yes     0
 9   172.16.164.101/32:any   172.16.162.0/23:any     all        none    require yes     0
10   172.16.168.2/32:any     172.16.168.0/24:any     all        none    require yes     0
11   172.16.144.0/24:any     0.0.0.0/0:any           all        encrypt require yes     0
12   172.16.160.0/21:any     0.0.0.0/0:any           all        encrypt require yes     0
13   172.16.168.0/24:any     0.0.0.0/0:any           all        encrypt require yes     0
```

Real Life Example with RB1000



System Status

System Uptime: 5214:27:13

LAN Status

Primary DNS 192.[redacted] Secondary DNS 192[redacted]

IP Address	TX Packets	RX Packets
172[redacted]	16349437	18671633

WAN Status

GW IP Addr 83.[redacted]

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
Static IP	83.[redacted]	29293492	4588	27190398	3499	441:33:05

>> Dial PPPoE or PPTP >> Drop PPPoE or PPTP

DrayTek

Firmware Version : v2.5.7

Build Date/Time : Mon Dec 5 15:23:42.34 2005

LAN MAC Address : 00-50-7F-28-9A-5B

Vigor2900V Series
Broadband Security
VoIP Router

Thank You for Your attention

WIRELESS NETWORK CONSULTING GROUP

References:
www.tcpipgiude.com
www.openvpn.net
www.microsoft.com
wiki.mikrotik.com

References:
www.tcpipgiude.com