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 expansion of IPv4 inter-networks people was concern about ensuring security.

First opportunity 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 options 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

- **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
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"`
IPSec in real life scenarios

• Due to complexity of IPSec and some limitation in IPv4, another VPN protocols emerged like:
  
  • PPTP
  • L2TP
  • OpenVPN
  • Many Prioprietary 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
OpenVPN

- 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

<table>
<thead>
<tr>
<th></th>
<th>Ipsec</th>
<th>PPTP</th>
<th>OpenVPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Complexity</strong></td>
<td>Complex</td>
<td>Simple</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Support for certificates</strong></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Packet</td>
<td>Session</td>
<td>Packet or Session</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>DES,3DES,AES</td>
<td>MPPE</td>
<td>Blowfish, AES</td>
</tr>
<tr>
<td><strong>Bridge support</strong></td>
<td>Yes*</td>
<td>Yes (with BCP)</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Tunnel support</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Transport mode</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
## Real Life Example with RB1000

![IPsec screenshot]

<table>
<thead>
<tr>
<th>Name</th>
<th>Auth. Algorithms</th>
<th>Encr. Algorithms</th>
<th>Lifetime</th>
<th>PFS Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>md5 sha1</td>
<td>3des aes-128 aes-192 aes-256</td>
<td>08:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>X</td>
<td>sha1</td>
<td>aes-128</td>
<td>00:30:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>RB750G</td>
<td>sha1</td>
<td>aes-128</td>
<td>00:30:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>asmax_1</td>
<td>md5 sha1</td>
<td>aes-128</td>
<td>08:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>asmax_2</td>
<td>md5 sha1</td>
<td>aes-128</td>
<td>08:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>default</td>
<td>sha1</td>
<td>3des aes-128 aes-256</td>
<td>08:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>default_all</td>
<td>md5 sha1</td>
<td>aes-128</td>
<td>00:30:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>draytek</td>
<td>sha1</td>
<td>aes-128</td>
<td>01:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>draytek_2</td>
<td>md5 sha1</td>
<td>aes-128</td>
<td>01:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>gprs</td>
<td>sha1</td>
<td>3des</td>
<td>00:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>merid</td>
<td>sha1</td>
<td>3des</td>
<td>00:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>plus</td>
<td>md5 sha1</td>
<td>3des</td>
<td>00:00:00</td>
<td>md5-1024</td>
</tr>
<tr>
<td>quantum</td>
<td>sha1</td>
<td>aes-256</td>
<td>01:00:00</td>
<td>md5-1024</td>
</tr>
</tbody>
</table>

13 items
### Real Life Example with RB1000

#### Table 1: Example Traffic Rules

<table>
<thead>
<tr>
<th>Src. Address</th>
<th>Srv. Port</th>
<th>Dest. Address</th>
<th>Dest. Port</th>
<th>Proto</th>
<th>Action</th>
<th>Level</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.144.0/24</td>
<td>0.0.0.0/0</td>
<td>172.16.144.0/24</td>
<td>255/443</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.144.2</td>
<td>172.16.144.0/24</td>
<td>255/443</td>
<td>none</td>
<td>encrypt</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.160.0/21</td>
<td>0.0.0.0/0</td>
<td>172.16.160.0/24</td>
<td>255/443</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.160.2</td>
<td>172.16.160.0/24</td>
<td>255/443</td>
<td>none</td>
<td>encrypt</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.162.0/23</td>
<td>172.16.164.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.162.2</td>
<td>172.16.162.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.164.2</td>
<td>172.16.164.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.164.50</td>
<td>172.16.164.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.164.55</td>
<td>172.16.164.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.164.100</td>
<td>172.16.162.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.164.101</td>
<td>172.16.162.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.166.2</td>
<td>172.16.166.0/23</td>
<td>255/443</td>
<td>none</td>
<td>none</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.168.0/24</td>
<td>0.0.0.0/0</td>
<td>172.16.168.0/24</td>
<td>255/443</td>
<td>encrypt</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>172.16.168.2</td>
<td>172.16.168.0/24</td>
<td>255/443</td>
<td>none</td>
<td>encrypt</td>
<td>require</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
Real Life Example with RB1000

<table>
<thead>
<tr>
<th>System Status</th>
<th>System Uptime: 5214:27:13</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN Status</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>TX Packets</td>
</tr>
<tr>
<td>172</td>
<td>16349437</td>
</tr>
<tr>
<td><strong>WAN Status</strong></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>IP Address</td>
</tr>
<tr>
<td>Static IP</td>
<td>83.</td>
</tr>
</tbody>
</table>

>> 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
Thank You for Your attention

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