An Introduction to the Tunneling Protocols

Alexandre Dulaunoy and various

ASBL CSRRT-LU (Computer Security Research and Response Team Luxembourg)
http://www.csrrt.org/

17th February 2006

OpenVPN - Introduction

- OpenVPN is not an IETF standard but...
- provides an open tunneling protocol over a single UDP or TCP stream
- works over NAT and/or dynamics IP
- provides only an ESP (IPsec terminology) like approach
- flexible authentication scheme (from static-key to X.509 certificate)
- TUN/TAP interface, works at user-level (versus kernel-level IPsec)

OpenVPN - mode of operation

- Authentication : secret key only or X.509 certification
- Mode : client or server or server-bridge
- Routing : client-to-client, server-to-client (default), iroute/route?
- Configuration : client-config (X.509), management interface,

OpenVPN hands-on

- one client, one server (mixed OS or non-mixed OS)
- shared secret keys authentication
- use a secure channel to exchange the shared keys

OpenVPN hands-on

- one client, one server (mixed OS or non-mixed OS)
- X.509 authentication
- use a secure way to handle the key enrollment process

OpenVPN hands-on

- multiple clients (fixed IPs), one server
- X.509 authentication
- use a secure way to handle the key enrollment process
- routing for a dedicated network on the server

OpenVPN hands-on

- multiple clients (fixed IPs), one server
- X.509 authentication
- use a secure way to handle the key enrollment process
- routing for a dedicated network on the server
- client must reach another client using the server

Q and A

- Thanks for listening.
- http://www.csrrt.org.lu/
- adulau@foo.be