



OpenVPN

Secure remote networks
for HantsLUG

© Adrian Bridgett <adrian@smop.co.uk>
Presentation released under GPL v3

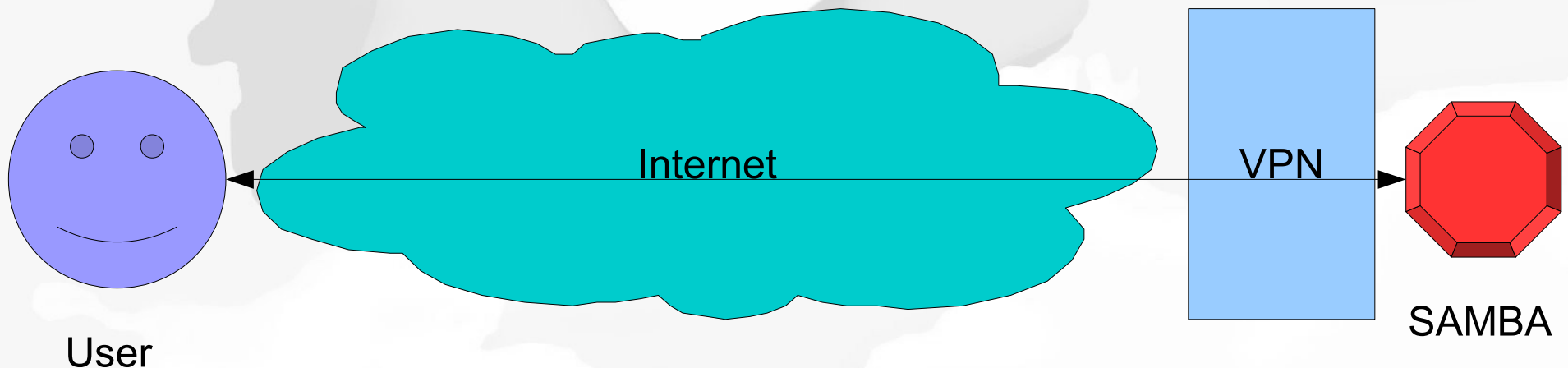
Contents



- What is a VPN
- Why OpenVPN (and why not)
- Private IPs (aside)
- X.509 certificates (aside)
- Walkthrough
- Advanced options
- Enhanced security
- Client improvements

What is a VPN

- Joins two networks together
- Using encryption
- Normally used across the internet
- Protects services (particularly insecure ones)



Why OpenVPN (and why not)

- Open Source, Free
- Very simple to setup and powerful
- Very easy to setup
- Good security and proven track record
- GUI client for Linux, Windows, Mac
- Not a standard VPN (although it uses SSL)
 - But the IPSec standard is very complex
 - And vendors (Cisco for one) add proprietary extensions anyhow

Private IPs

- You can't just randomly pick IP addresses
- However some ranges are reserved for everyone to use – these will never be on the internet
- Can still get clashes if you “join” two sites together
- See RFC-1918:
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.255.255
 - 192.168.0.0 - 192.168.255.255

X.509 Certificates



- You already use these when you visit any secure site on the internet
- Three parties:
 - Certificate Authority (CA) – approves (signs) the certificate requests
 - Server (who you are talking to)
 - Client (you!)

X.509 Certificates part II

- These use “Public Key Infrastructure”
- Clients trust all certificates signed by the CA
 - i.e. all servers
- Servers might require the clients to have valid certificates too (a VPN normally would)
- To use a certificate you must have the other part (the key)

Walkthrough

- OpenVPN HOWTO is highly recommended
- Generate CA, Server, Client certificates
- Configure server
- Configure client
- Done
- <http://openvpn.net>
- http://www.smop.co.uk/mediawiki/index.php/OpenVPN_server

Advanced options

- Server can send client options:
 - DNS servers (if you have “private DNS”)
 - Extra network routes (to reach boxes other than the VPN box itself)
 - Force all traffic through the VPN
- Default is to not allow one client to see another
- Default is “routed” network, can use “bridged”:
 - One joined network, useful for some protocols
 - But harder to configure and lock-down

Enhanced Security

- To avoid Man-In-The-Middle attacks:
 - OpenVPN 2.0: “ns-cert-type server” (client)
 - OpenVPN 2.1: “remote-cert-tls server” (client)
 - The server certificate must have been generated using build-key-server too
- Can also ask user for username/password (passed to script – e.g. Query PAM (Linux))
 - Possible (but not recommend) to use this instead of certificate
- See HOWTO about this and also “tls-auth”

Client improvements



- By default the Linux client ignores DNS entries passed back
- Instructions on how to add support (using resolvconf) at:
- <http://www.smop.co.uk/mediawiki/index.php/OpenVPN>