OpenVPN
An easy-to-configure, open source SSL VPN solution
Why OpenVPN?

- Easy to set up
- Works with NAT
- SSL/TLS and ciphers w/ openssl library
- static or public key
- portable, Open Source
Where the boys are:
Brief How-To for OpenBSD

• Plan
• Install software
• Set up CA and generate keys
• Configuration files
• Start and test
Plan

- Decide on routed* or bridged
- Routing: easier to set up and fine tune
- Bridging: non-IP protocols and broadcasts
- Number private subnet to avoid conflict
Install Software

- Install as package*
- Or from ports or source
Set up CA

- init-config
- edit ‘vars’ (country, province, city, etc)
- . ./vars
- ./clean-all
- build-ca
Generate Server Key

• `./build-key-server server`
• `sign and commit`
Generate client key(s)

- .:/build-key client1
- OR .:/build-key-pass <name>
- Don’t need challenge password
- Do sign and commit
## Overview: keys and crts

<table>
<thead>
<tr>
<th>File</th>
<th>Computer</th>
<th>Secret?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca.crt</td>
<td>all</td>
<td>No</td>
</tr>
<tr>
<td>ca.key</td>
<td>sign only</td>
<td>YES!!</td>
</tr>
<tr>
<td>server.crt</td>
<td>server</td>
<td>No</td>
</tr>
<tr>
<td>server.key</td>
<td>server</td>
<td>Yes</td>
</tr>
<tr>
<td>client1.crt</td>
<td>client</td>
<td>No</td>
</tr>
<tr>
<td>client1.key</td>
<td>client</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Keys and Carts

• Keys are secret
• The CA key (that signs the others) is really, really secret!
• Certificates are not secret
Configuration Files

- One for server
- One for each client (only on the client)
- Specifies key and.crt locations
Start and test

• “Initialization Sequence Completed”
• Try pinging
• Try services
Finalizing setup

- Configure with --chroot
- Configure to run as different user --user
- Configure rc.local to run openvpng at startup
- Modify services as needed, e.g. samba
Some things to remember...

• Only use tun interface on OpenBSD
• Add manual route if necessary
• Be mindful of firewalls
• Services may need to be adjusted
• Doesn’t work (well) on Vista yet
Much, much more at:
http://www.openvpn.net