Setting up a router/firewall/VPN combo with OpenBSD 5.2 and OpenVPN 2.2.2

This file contains directions for setting up an OpenBSD 5.2 server that plays the role of firewall, router and OpenVPN server. The machine is assumed to be of the i386 architecture and to have two Ethernet interfaces, one connected to the outside world and the other connected to the protected internal network.

The following source files accompany these directions and will need to be copied to the OpenBSD machine:

|  |  |  |
| --- | --- | --- |
| **File** | **Description** | |
| $/server/etc/sysctl.conf | | Enables IP forwarding |
| $/server/etc/rc.local | | Starts OpenVPN as a daemon on boot |
| $/server/etc/rc.conf.local | | Enables packet filter and DHCP server |
| $/server/etc/pf.conf | | Specifies routing and firewall rules |
| $/server/etc/dhcpd.conf | | DHCP server settings |
| $/server/etc/resolv.conf | | List of domain name servers |
| $/server/etc/openvpn/vars-fixed | | Version of OpenVPN utility script fixed for OpenBSD |
| $/server/etc/openvpn/server.conf | | OpenVPN server configuration |

The following files will be created on the OpenBSD machine during installation:

|  |  |
| --- | --- |
| **File** | **Description** |
| /etc/myname | Sets the host name |
| /etc/hostname.{ethIn} | Configures internal network with a static IP |
| /etc/hostname.{ethEx} | Configures external network with a static IP |
| /etc/dhcpd.interfaces | Sets DHCP server to listen on internal network |

Each client machine will need one source file and three others generate on the OpenBSD machine:

|  |  |
| --- | --- |
| **File** | **Description** |
| $/client/client.ovpn | OpenVPN client configuration |
| /etc/openvpn/ca.crt | Root CA certificate |
| /etc/openvpn/client.crt | Client certificate |
| /etc/openvpn/client.key | Client key (secret) |

1. Pick a hostname for the system and set it:

hostname openvpn.zeus.local

echo "openvpn.zeus.local" > /etc/myname

1. Determine the names that OpenBSD has assigned to your two Ethernet interfaces and decide which will be the internal and external. The following directions and accompanying files use {ethIn} and {ethEx} for the internal and external interfaces. Replace with the particulars of your system.
2. Configure the external network interface with a static IP:

echo "inet 10.1.1.5 255.255.255.0 NONE" > /etc/hostname.{ethEx}

sh /etc/netstart {ethEx}

1. Configure the internal network interface with a static IP:

echo "inet 10.4.4.1 255.255.255.0 NONE" > /etc/hostname.{ethIn}

sh /etc/netstart {ethIn}

1. Copy all of the files in the $/server directory directly onto your fresh OpenBSD 5.2 install. Backing up the default files that came with your install is probably wise. Even better, manually merge the contents of the source files into the defaults so you get a better understanding of how everything is configured.
2. Modify files?
3. Set the DHCP server to run on the internal interface:

echo "{ethIn}" > /etc/dhcpd.interfaces

1. Reboot the OpenBSD machine and run the following tests:
   1. Can the OpenBSD machine ping your internet gateway?

ping 10.1.1.1

* 1. Can the OpenBSD machine resolve names and reach the internet?

ping www.google.com

* 1. Can a machine plugged into the internal Ethernet port obtain an IP address via DHCP?
  2. Can the internal machine ping the OpenBSD machine?

ping 10.4.4.1

* 1. Can the internal machine ping your internet gateway?

ping 10.1.1.1

* 1. Can the internal machine resolve names and reach the internet?

ping www.google.com

1. Install OpenVPN:

export PKG\_PATH=ftp://ftp3.usa.openbsd.org/pub/OpenBSD/5.2/packages/`machine -a`/

sudo pkg\_add -v openvpn-2.2.2p1.tgz

cp -R /usr/local/share/examples/openvpn/easy-rsa/2.0/\* /etc/openvpn/

echo "openvpn --daemon --config /etc/openvpn/server.conf" >> /etc/rc.conf.local

1. Create the root CA keys:

cd /etc/openvpn

. ./vars-fixed

./clean-all

./build-ca

|  |  |
| --- | --- |
| Country | US |
| State | CA |
| Locality | LosAngeles |
| Organization name | Zeus |
| Unit name | . |
| Common name | openvpn.zeus.local |
| Name | OpenVPN-Zeus-RootCA |
| Email address | no@email.com |

./build-key-server server

|  |  |
| --- | --- |
| Country | US |
| State | CA |
| Locality | LosAngeles |
| Organization name | Zeus |
| Unit name | . |
| Common name | Server |
| Name | OpenVPN-Zeus-Server |
| Email address | no@email.com |
| Challenge password | [blank] |
| Optional company name | [blank] |
| Sign the certificate? | y |
| 1 out of 1 certificate requests certified, commit? | y |

1. Create a set of keys for each client. For example, to generate keys for client1:

./build-key client1

|  |  |
| --- | --- |
| Country | US |
| State | CA |
| Locality | LosAngeles |
| Organization name | Zeus |
| Unit name | . |
| Common name | client1 |
| Name | Client1 |
| Email address | no@email.com |
| Challenge password | [blank] |
| Optional company name | [blank] |
| Sign the certificate? | y |
| 1 out of 1 certificate requests certified, commit? | y |

1. Generate Diffie Hellman parameters:

./build-dh

1. Start the server on the command line manually to check if it boots successfully (press Ctrl-C to shut down):

openvpn /etc/openvpn/server.conf

1. Configuring a Windows 7 client:
   1. Copy ca.crt, client1.crt, client1.key and client.ovpn to the client machine and rename them as you see fit.
   2. Download and install the OpenVPN desktop client from [www.openvpn.net](http://www.openvpn.net).
   3. Copy ca.crt, client1.crt and client1.key to the keys directory:

C:\Program Files[ (x86)]\OpenVPN Technologies\OpenVPN Client\keys

* 1. Store and edit client.ovpn anywhere you’d like. Import it into OpenVPN after you’re done and it will import the file into the profile directory:

C:\Program Files[ (x86)]\OpenVPN Technologies\OpenVPN Client\etc\profile