VPN Lab Exercise (host-to-host VPN)

1 Overview

This Labtainer exercise illustrates a simple host-to-host vpn implemented with openvpn, and a static shared key.

The example network includes a client and a server with a router between them. The server offers a simple HTTP service, and the student will use wget on the client to retrieve html files from the server.

2 Lab Environment

This lab runs in the Labtainer framework, available at http://nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers or on Docker Desktop on PCs and Macs.

From your labtainer-student directory start the lab using:

```
labtainer vpnlab
```

A link to this lab manual will be displayed.

The openvpn application is pre-installed on the client and the server, and the corresponding openvpn configurtion files already exist. To create an encrypted tunnel, the student only has to execute openvpn on the client and the server.

The student will observe both unencrypted and encrypted network traffic using tcpdump on the router.

3 Tasks

3.1 Observe unencrypted traffic

Use tcpdump on the router to display network traffic:

```
sudo tcpdump -n -XX -i eth0
```

Use wget on the client to fetch the index.html file

```
wget  http://<IPADDr>/index.html
```

Where <IPADDR> is the server network address, which you can learn by running "ifconfig" on the server.

Observe the network traffic from tcpdump. Note plain-text html in the data stream.

3.2 Start the VPN

Start the openvpn program on the server:

```
sudo openvpn --config server.conf --daemon
```

Start the openvpn program on the client:

```
sudo  openvpn --config client.conf --daemon
```

Use wget again, but this time using the server's tunnel address, (which appears in interface "tun0" of output from ifconfig).

Observe the network traffic in tcpdump.

4 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under sponsorship from the National Science Foundation Award Number 1932950.