IPTables: Site-to-Site VPN - Lab Guide

1 Overview

A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network.

A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.

OpenVPN is an open source tool that can be used to create VPN conections. It uses a custom protocol based on SSL and TLS.

Site-to-site VPNs are used to connect networks across another untrusted network such as the internet.

In a site-to-site VPN, end hosts send and receive normal unencrypted TCP/IP traffic through a VPN terminating device.

In most cases, the devices in both networks don't need to do any more steps to exchange data with the devices in the other network.

We will enhance the lab Host-to-Site VPN to establish the VPN connection between Site1-Router and the HQ-Router through the ISP network.

2 Lab Environment

This lab runs in the Labtainer framework, available at http://my.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.

From your labtainer-student (/labtainer/labtainer-student) directory start the lab using:

```
labtainer sparta-vpn3
```

A link to this lab guide will be displayed.

3 Network Configuration

IP addresses and routing are configured on all devices.

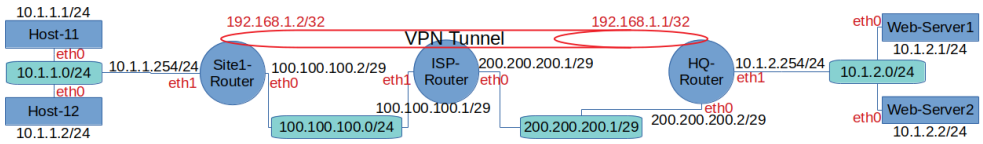

Figure 1: Network topology for routing-basics lab

The network is composed of (find the main components of this network based on its topology):

-
-
-
-
-
-
-

The OpenVPN application is pre-installed on the host and the server, and the OpenVPN configuration files already exist.

4 Credentials

- **Host-11**:
  - **Username:** user-11
  - **Password:** user-11
- **Host-12**:
  - **Username:** user-12
  - **Password:** user-12
- **Web-Server1**:
  - **Username:** web-admin
  - **Password:** web-admin
- **Web-Server2**:
  - **Username:** web-admin
  - **Password:** web-admin
- **Site1-Router**:
  - **Username:** admin
  - **Password:** admin
- **ISP-Router**:
  - **Username:** admin
  - **Password:** admin
- **HQ-Router**:
  - **Username:** admin
  - **Password:** admin

5 Lab Tasks

5.1 Checking/Testing the Initial Configuration

Its your task to test the configuration and to report what does/not work

5.2 Capturing the Traffic

Lets use **tcpdump** which is a command line tool that can capture TCP/IP and other packets being transmitted or received over a network interface.

In the ISP-Router terminal, run the following command:

```
sudo tcpdump -n -XX -i eth1
```

Lets run tcpdump on Web-Server1 so we can monitor the traffic received on the server:

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

Lets run tcpdump on Web-Server2 so we can monitor the traffic received on the server:

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

5.3 Configuring the VPN - HQ-Router

- Check VPN configuration

  ```
  ls
  ```

  Notice that there are two files:

  - gateway.conf: it contains the OpenVPN configuration that will be used during establishing the VPN connection with the VPN-Gateway.

    ```
    cat gateway.conf
    ```

    The file content is as follows:
    - The first line ‘dev tun‘ is the defining the type of the device/interface that will be created during the VPN establishment. In this case, we are using tunnel interface.
    - The second line ‘ifconfig 192.168.1.1 192.168.1.2‘ defines the IP addresses of both end of tunnel.
    - The third line ‘secret static.key‘ points to the file where the shared static key is stored.
    - The fourth line ‘push ”route 10.1.2.0 255.255.255.0”‘ advertises to the vpn-client that this network can be reached through the VPN-tunnel.
    - The fifth line ‘route 10.1.1.0 255.255.255.0 192.168.1.1 1‘ adds a new routing record to route thr traffic to this network through the tunnel interface. The ‘1‘ at the end of the line gives this route a higher priority than all other previous routes to the same network.
  - static.key: it contains the same secret key that exists on the client and will be used to establish the VPN connection with the hq-router.

    ```
    cat static.conf
    ```

- Establishing the VPN connection.

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

5.4 Configuring the VPN - Site1-Router Side

- Check VPN configuration

  ```
  ls
  ```

  Notice that there are two files:

  - site1.conf: it contains the OpenVPN configuration that will be used during establishing the VPN connection with the VPN-Gateway.

    ```
    cat site1.conf
    ```

    The file content is as follows:

    * The first line ‘remote 200.200.200.2‘ is the OpenVPN Gateway that it will connect to.
    * The second line ‘dev tun‘ is the defining the type of the device/interface that will be created during the VPN establishment. In this case, we are using tunnel interface.
    * The third line ‘ifconfig 192.168.1.1 192.168.1.2‘ defines the IP addresses of both end of tunnel.
    * The fourth line ‘secret static.key‘ points to the file where the shared static key is stored.
    * The fifth line ‘push ”route 10.1.1.0 255.255.255.0”‘ advertises to the vpn-gateway that this network can be reached through the VPN-tunnel.
    * The sixth line ‘route 10.1.2.0 255.255.255.0 192.168.1.1‘ adds a new routing record to route thr traffic to this network through the tunnel interface. The ‘1‘ at the end of the line gives this route a higher priority than all other previous routes to the same network.

  - static.key: it contains the secret key that will be used to establish the VPN connection with the VPN-Gateway. This is a shared key, that means the VPN-Gateway should have the exact key in order to successfully establish the connection.

    ```
    cat static.conf
    ```

- Start the VPN connection on the VPN-Gateway.

  ```
  sudo openvpn --config site1.conf --daemon
  ```

6 Testing the connectivity

- On HQ-Router (Check IP configuration and network interfaces)

  ```
  ip addr
  ```

  What is the result ? How many interfaces on the this machine ?

- On Site1-Router (Check IP configuration and network interfaces)

  ```
  ip addr
  ```

  What is the result ? How many interfaces on the this machine ?

- On Host-11, Host-12 (Ping Host-11,Host-12 -> Web-Server1, Web-Server2)

```
    ping 10.1.2.1
wget 10.1.2.1
ping 10.1.2.2
wget 10.1.2.2
```

  What is the result ? Why do we used the private IP addresses not the tunnel ones ?

- Check the router terminal to see whether you still can find unencrypted text in the packets captured by the router.

  Check whether you can see the IP addresses (10.1.1.1, 10.1.2.1 or 10.1.2.2). Why can't you see any of them ?

- Check the server terminal and check which IP addresses you can see in the log. Can you see the IP address 10.1.1.1 ? Why ?

7 Submission

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

```
stoplab sparta-vpn3
```

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.