Chapter 16: Virtual Private Network

Problems

16.1. What are the main differences between SSH tunnel and VPN tunnel?

16.2. To log into Syracuse University's network, Bob needs to use a TLS-based VPN. After he has established a VPN tunnel between his machine and Syracuse University's network (128.230.0.0/16), he checks the routing table on his computer. Here is what he says:

```
----------------------------------------------------------------
  Network
Destination      Netmask          Gateway          Interface
----------------------------------------------------------------
    0.0.0.0      0.0.0.0          192.168.0.1      192.168.0.13
  127.0.0.0      255.0.0.0        On-link          127.0.0.1
  127.0.0.1      255.255.255.255  On-link          127.0.0.1
128.230.0.0      255.255.0.0      128.230.153.48   128.230.153.80
128.230.153.12   255.255.255.255  192.168.0.1      192.168.0.13
128.230.153.80   255.255.255.255  On-link          128.230.153.80
192.168.0.0      255.255.255.0    On-link          192.168.0.13
192.168.0.13     255.255.255.255  On-link          192.168.0.13
192.168.0.255    255.255.255.255  On-link          192.168.0.13
```

From the above routing information, please answer the following questions (you need to explain your answer).

  (a) What is the computer's real IP address, i.e., the IP address assigned to the machine's physical network interface card?

  (b) What is the IP address of Syracuse University's VPN server?

  (c) What is the IP address of the TUN interface on Bob's machine?

  (d) Assume that Bob is behind a firewall that blocks him from accessing a web site (assume that the IP address of the web site is 8.8.8.8). Please describe how Bob can use Syracuse University's VPN to bypass the firewall. If changes need to be made to this routing table, please show exactly what changes Bob needs to make to achieve the goal.

16.3. In Figure 16.11, Machine X has established a VPN with Machine Y, which is a VPN server connected to the private network 10.0.20.0/24. With the VPN, a user on Machine X can now access machines on the 10.0.20.0/24 network. The user runs the following command on Machine X: "telnet 10.0.20.100". Figure 16.11 shows the packet flow triggered by this command. Please answer the following questions:

  (a) What is the relationship between packets ❶ and ❷?

  (b) What is the relationship between packets ❸ and ❹?

(c) What is the source IP and destination IP of packets ❶, ❷, ❸, and ❹?

(d) What routing entries are needed on Machine X?

(e) What routing entries are needed on Machine Y?

(f) What routing entries are needed on Machine `10.0.20.100`?

(g) If we break the VPN tunnel, what is going to happen to the `telnet` connection? Is it going to be broken? After a few seconds, we reconnect the VPN tunnel between X and Y, what is going to happen?
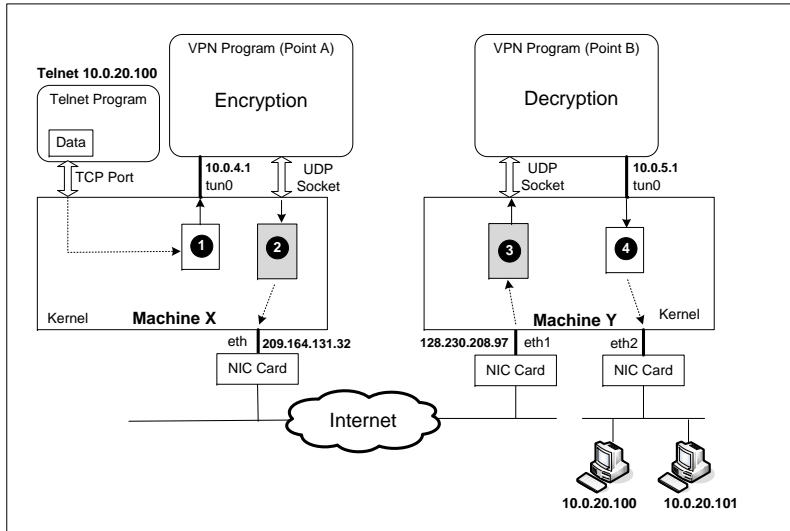
Figure 16.11: Packet flow over VPN (for Problem 16.3.)

16.4. Figure 16.12 shows a VPN setup, which allows Host U on a private network `192.168.60.0/24` to communicate with Host V in another private network `192.168.80.0/24`. Please describe the following:

(a) What routing entries need to be added to Host U, VPN Client, VPN server, and Host V? You don't need to write down the actual command, but you need to describe those routing entries.

(b) When Host V receives a packet from Host U, what is the source IP address of the packet?

(c) When VPN server receives a packet from Host U to Host V, via the VPN tunnel, what is the source and destination IP addresses of the packet?

(d) After the VPN tunnel is set up, when we ping Host V from Host U, please describe in details how the ICMP echo request packets get to Host V from Host U, and how the ICMP echo reply packets get back to Host U.
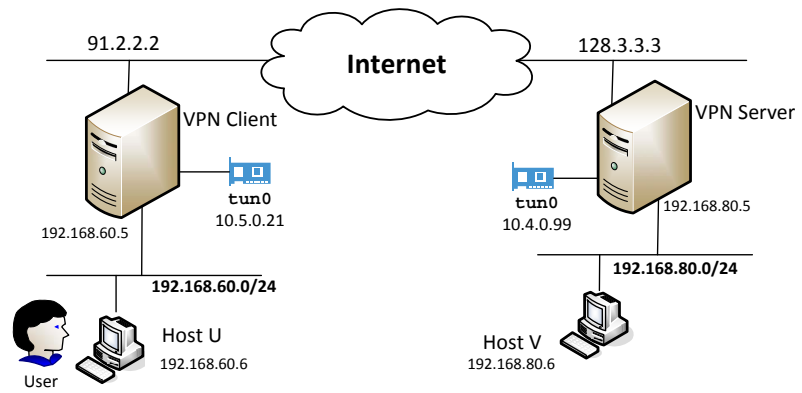
Figure 16.12: Figure for Problem 16.4.