Quiz 7

CSE-644 INTERNET SECURITY

DR. SYED SHAZLI

2/28/2023

Anthony Redamonti
SYRACUSE UNIVERSITY

1) What is VPN? Why do we need it?

The virtual private network (VPN) is a method of allowing users that are physically outside the protected network to access the network by creating a tunnel through the firewall. The user will be protected by the same firewall and have access to all the internal recourses of the private network.

If someone is traveling on a business trip and needs to access the private network of their business, VPN provides a method of connecting to the private network from a physical location outside the network.

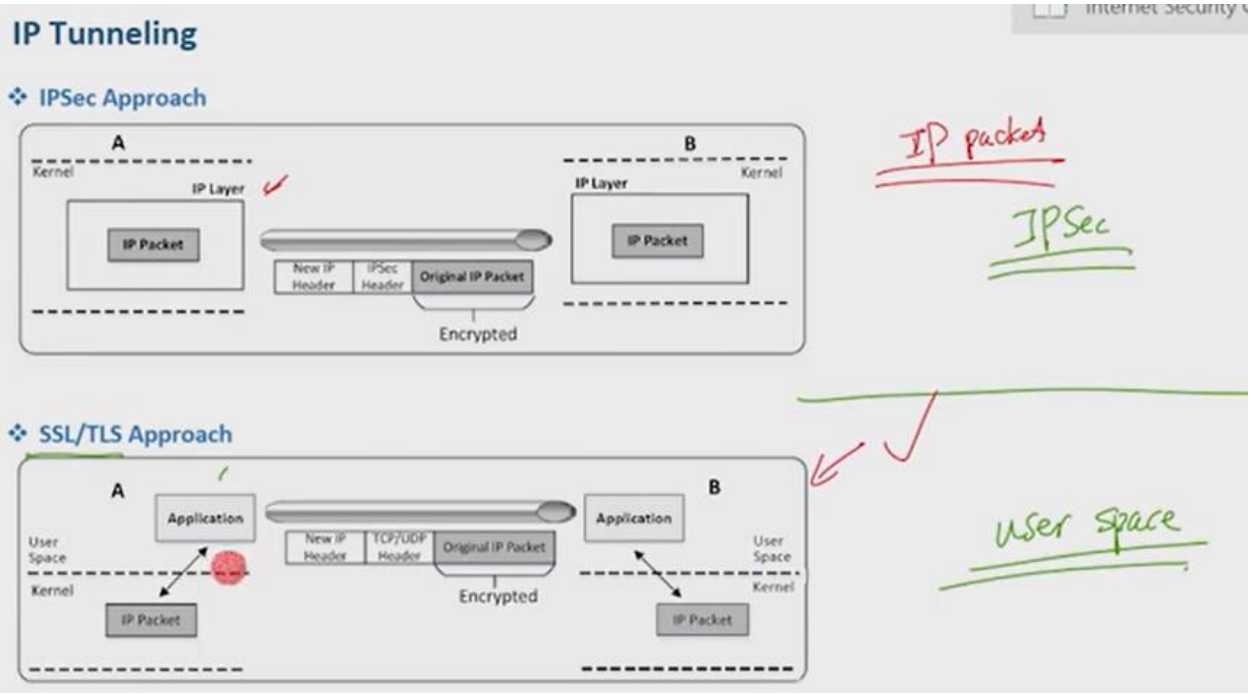
2) How does VPN work? (Briefly)

VPN works by creating a tunnel from the user's machine, through the firewall, and into the private network. How can a computer outside the private network access (via the internet) a private network that is protected by a firewall? It may expose the private network to sniffing and spoofing attacks. Secure tunneling techniques are needed to prevent such attacks.

Technique 1: Send the information from the outside by encasing it in a "safebox." We can directly give the safebox to the private network. The private network needs to know the key to open the box and needs to be able to tell if the box has been damaged (if the contents of the box have been altered).

Technique 1 is not transparent. We want the computer to access the private network in a transparent way. Instead of sending the payload directly to the private network, send it to a new dedicated server called the VPN server, which exists inside the private network.

Create a tunnel to the VPN server. Send encrypted data to the tunnel. The tunnel can be implemented inside or outside the kernel. Implementations internal to the kernel use the IPSec approach, while those outside the kernel use the SSL/TLS approach. Applications that manage the tunnel in the user-space are preferred as they are more reliable and easier to update than IPSec. Modifications to the IPSec approach would require downloading changes to the OS (difficult to implement).



3) What is IP routing table? What do you need to do if you want your ip packet to go through VPN tunnel? Why does it work?

The IP routing table is a table inside the OS that contains a set of rules (entries) that specify where IP packets will be forwarded.

The IP packets will be redirected to the VPN client, which will insert it into a safebox and establish a secure virtual channel with the VPN server. Therefore, the IP packet will not be sent to the client's NIC card but will be redirected to the VPN client. The OS provides the TUN/TAP interface which connects to the VPN client, acting as its NIC interface. The computer will route all IP packets through the TUN interface. It works at the user-space to create a virtual interface. First the interface is opened and created. Then the interface is assigned an IP address and added to the routing table.

4) Why do we need socket interface?

The TUN interface is needed to act as the NIC card for the VPN client. The OS can then redirect IP packets to the TUN interface by adding it to its IP routing table. No IP packets will reach the computer's NIC card but instead will be redirected to the TUN interface. The socket interface is needed to inject IP packets into the kernel from the user-space.