Assignment 3 – Firewall and VPN
Gunnar Yonker

1.
    a. Yes, a firewall can prevent a Smurf attack from an external network because the attack is using the broadcast IP address of the subnet. A firewall can prevent this because a firewall can simply block all of the traffic to the broadcast IP and this can be done on a firewall using a stateless packet filter. By doing this, a firewall can effectively prevent a Smurf attack.
    b. A SYN flood attack can also be blocked using a firewall because the SYN attack comes from flooding a victim with SYN packets that bog down the traffic. A firewall can be setup with a packet filter which could filter out SYN packets and prevent the flood attack from taking place.
    c. A firewall could also be used to block P2P applications such as BitTorrent. This can be done using a firewall by checking the app-level info of BitTorrent and matching it's signature to the traffic coming through so that it can be detected and identified as BitTorrent traffic and blocked. A firewall would then be using a BitTorrent firewall proxy to detect and block that traffic and this can be similarly done for other P2P applications.
2.
    a. A VPN works by being a combination of device-level components and network-level components that when used together provide a secure level of communication for the user to their connections. A VPN itself runs on the network layer of the TCP/IP layered communications stack model and is used to run a secure communication channel between two endpoints and specifically uses the IPSec open framework. If you are using a public network, it is a good idea to use a VPN that can create a protected connection to the network for any data that you are communicating. VPNs provide security features such as authentication and date privacy which is extremely important when communicating any information online. VPN's can also be configured to accomplish the tasks that you set out to do in various ways depending on what kind of security features you want implemented.
    b. SSL based tunneling typically used the port for HTTPS traffic which is port 443 which is usually allowed on most networks. This can be used to get around firewalls that block other ports, but not port 443. SSL can support both UDP and TCP protocol for tunneling.

       IPsec based tunneling uses encrypted IPSec packets that are called ESP packets. By default, these packets have no port number assigned and can get stuck in a NAT firewall unless you would manually assign a port number. This can be bypassed by formatting the ESP packet inside of a UDP packet so that the UDP port number can traverse the packet across the network firewall. IPsec works by creating a secure tunnel between two entities that have defined IP addresses.

    c. SSL based tunneling technique is more popular than IPsec tunneling because it gives users more specific access when it comes to remote access. IPsec operates at the network layer and encrypts data that is sent between any systems that can be identified by IP address. SSL operates at the transport layer and encrypts data that is sent between any two processes using port numbers as identification. SSL is also preferred because it defaults to encryption of network traffic unlike IPsec which does not explicitly do that. SSL is preferred most often because it allows the user to remotely connect to a network and all its applications while ensuring their data is encrypted. SSL is usually run through the web browser, not an application where the tunnel is connected to the web-enabled applications not the entire network like IPsec. Another benefit of SSL is that the software is often automatically upgraded on the server without needing the user to specifically update the software. If an attacker were to gain access to an SSL tunnel they would be limited to only the current application that the user was connected to, whereas if the attacker gained access to an IPsec tunnel they would have access to the entire network which makes SSL tunneling more secure in that aspect.

d. A firewall can be bypassed using a VPN by using a tunneling method much like the ones I outlined above. The VPN will use a tunneling protocol that hides any of your traffic and tunnels it through an open port such as SSL based tunneling using port 443, masking the user's traffic as HTTPS traffic. Another benefit of using a VPN to bypass a firewall is that a VPN will assign a new IP address to your traffic so that if anyone were to see where the traffic was coming from, they would think you were associated with that new IP address which provides some additional anonymity. OpenVPN is one of the best protocols that can be used to bypass a firewall because it is very flexible. VPNs also provide most often 256-bit AES encryption so that your connection is more secure.

3.

a. (1) A whitelist is when the firewall will only allow specific addresses such as IP addresses or domain names, to pass through. This is usually when you only want traffic from certain trusted users/devices to be allowed through. Blacklisting is the opposite which is when specific addresses such as IP addresses or domain names are blocked, and all other traffic is allowed through the firewall. This is used when you have specific sites or specific addresses that you want to block, but you want all other traffic to be allowed through. The table we are provided is a whitelist because the default action taken is deny if there is not a match to the given rules. The rules here allow only certain traffic through the firewall and the rest of traffic if not applied to a given rule is denied which makes this a whitelist.

b. (2) This attack would be successful because the crafted packet would satisfy one of the rules and be allowed through the firewall. The source port and dest port of the crafted packet, when compared to the rules in the table, are labeled as allowed port access. The first line of the crafted packet is satisfied in the first rule of the table provided and would be allowed. The second line of the crafted packet satisfies the second rule on the table provided. Since these rules are satisfied with the crafted packet, this packet would be allowed through the firewall and the attack could be successfully carried out by the hacker.

c. (3)

Source Add	Source Port	Dest Add	Dest Port	Protocol	ACK set	Action
External	>1023	Internal	25	TCP	Any	Allow
Internal	25	External	>1023	TCP	Yes	Allow
Internal	>1023	External	25	TCP	Any	Allow
External	25	Internal	>1023	TCP	Yes	Allow

4. Subnet of 26.8.123.0/25
    a. External firewall ruleset – Whitelist - if no rule satisfied default action is: **Deny**

Direction	Src address	Src Port	Dest address	Dest port	Protocol	Action
In	External	>1023	Internal	25	TCP	Allow
Out	Internal	25	External	>1023	TCP	Allow
Out	DMZ Mail Gateway	25	External	>1023	TCP	Allow
Out	Web Proxy Internal	Any	External	80	TCP	Allow
In	External	Any	DMZ Web Server	80	TCP	Allow
Out	Internal	Any	External	53	TCP or UDP	Allow
Out	DMZ DNS Server	Any	External	53	TCP or UDP	Allow

    b. Internal firewall ruleset – Whitelist - if no rule satisfied default action is: **Deny**

Direction	Src address	Src Port	Dest address	Dest port	Protocol	Action
In	DMZ Mail Gateway	Any	Internal Network	110	POP3 or POP3s	Allow
Out	Web Proxy Internal	Any	External	80	TCP	Allow
Out	Internal	Any	External	53	TCP or UDP	Allow
Out	Internal	Any	DMZ Server	Any	Any	Allow
In	Any Internal	Any	Any DMZ Server	Any	Any	Allow
Any	Any	Any	26.8.123.127	25	TCP	Allow