**Week 4 Essay Questions**

Your Name (First M. Last)

School or Institution Name (University at Place or Town, State)

**Week 4 Essay Questions**

1. **Network communication protocols:**

These are the standard conventional protocols to enable connection, communication and data sharing between two computing endpoints.

**ARP:** Address Resolution Protocol deals with resolving addresses of internet layer. It maps network address and physical address.

**DHCP:** Dynamic host configuration protocol is the managing assigns an internet protocol addresses to different devices on a network, in this way it enables the communication through IP.

**ICMP:** Internet control message protocol is a feedback protocol that is used to diagnose or report logical error.

**SNMP:** Simple Network management protocol is application level protocol that manages and monitors the devices on network and their functionality.

**DNS:** Domain name system is a protocol that helps resolving the names of the sites on internet using their underlying IP address. It adds efficiency provides security in the processes (Kozierok, 2005).

1. **Firewall configurations and its types**

**Bastion host:** It is a specialized computer that is deliberately exposed on the public network, as gateway it resides between inside network or outside network. It is usually part of a larger security system that has different layers of protection.

**DMZ:** Demilitarized zone is logical subnet that separates the logical area network from the other untrusted networks. Servers are located in the DMZ to provide additional security to the LAN. Usually it is deployed between the two firewalls.

**Dual-homed firewall:** It is the firewall that uses two network interfaces, in which connection is made with the internal network and the other is made with the internet. It ensures that no direct IP traffic comes between the internal network and internet.

**Screened host:** This firewall is the flexible version of firewall that is achieved at cost of its security. It is used when security is required by the network along with the flexibility.

**Screened subnet:** It is a firewall that has three components for security. It is used by the companies that need upper extra security(“Screened Host Firewall,” n.d.).

1. **Tunneling protocols**

**IPIP:**  IP in IP tunneling protocol encapsulates one IP header within outer IP header, for which outer header is added with source IP before the entry of destination point, in such a way that inner packet stays unmodified.

**SSTP:** Security Socket tunneling protocol provides mechanism to transport traffic of PPP through TLS/SSL channel to provide transport level security.

**IPsec:** This internet protocol security authenticates and encrypts packets of data that are send over IP network.

**L2TP:** It is a layer two tunneling protocol that supports VPNs by being part of delivery of services by ISPs.

**References**

Kozierok, C. M. (2005). *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*. No Starch Press.

Screened Host Firewall. (n.d.). Retrieved March 9, 2019, from http://www.vtcif.telstra.com.au/pub/docs/security/800-10/node57.html