Week 10 Discussion #1

Discuss various firewall types and how each can improve system security. What information does a system administrator need to configure a firewall correctly?

First generation packet-filtering firewall's inspect packets on the network layer, and occasionally monitor the transport layer, checking packets against a set of rules. Packets that do not match are rejected and an error message is sent to the sender.

Second generation Stateful firewalls or "circuit relays" as they were originally known, consider the placement of a packet in a packet series. They are capable of determining if the present packet is part of an existing series, start of a new series, or an invalid packet. Stateful firewalls offer protections against cyber-attacks that exploit existing connections, such as denial of service attacks.

Third generation application firewalls, or proxy-based firewalls, are "closely tied to the semantics of the traffic they handle (Schneider, 1998)." The application layer filtering recognizes certain applications and protocols and can detect irregularities in traffic, such as software accessing non-standard ports or unrecognized protocols.

Dynamic packet filters merge packet filter and application gateway types of firewall. With this type of firewall, packets are evaluated individually; however, some packets may modify the rules that apply to subsequent packets, allowing for more sophisticated processing.

In order to properly configure a firewall, a network or systems administrator needs to know what applications or resources within the organization's network need to be accessible from outside of the network in order to know what traffic the firewall needs to allow to pass through.

Ingham, Kenneth and Forrest, Stephanie, *A History and Survey of Network Firewalls*, University of New Mexico, 2002.

Schneider, Fred B. *Trust in Cyberspace*, National Academies Press, Washington DC, 1998.