Introduction to Intelligent Security Systems

Alvin Lin

August 2018 - December 2018

Firewall Design

A firewall is a device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. They isolate an organization's internal network from the larger Internet, only allowing some traffic to pass while blocking others. It is a junction point between two networks and sets a border line for network administration responsibility. The term originates from firewalls and fire doors in buildings.

History

- 1764 - The term "firewall" was used to describe walls which separated the parts of a building most likely to have a fire from the rest of the structure.
- Late 1980s - The predecessors to firewalls for network security were the routers used to separate networks from one another.
- 1988 - The Morris Worm infected about 6000 systems.
- 1994 - Alice Muffett wrote a paper which provided an excellent review of the firewall policies and architectures of the time.
- 2004 - IDC coins the term UTM (unified threat management) and several security vendors following suit, beginning to market their firewalls that run multiple security functions.
- 2009 - Gartner defines the next generation firewall as a "a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks". Results of the first widespread analysis of firewall management practices are published, including statistics like "93% felt their firewalls contained

at least one category of error and 70% felt that it was likely their rulebases contained undetected errors".

- 2012 - Gartner releases a forecast that says more than 95% of firewall breachers will be caused by misconfiguration and not firewall flaws.

Software firewalls operate locally on the machine they are intended to protect while hardware firewalls are usually part of a TCP/IP router.

Functions

Firewalls can filter traffic based on their source and destination addresses, port numbers, protocols used, and packet state. They cannot prevent individual users with modems from dialing in and out of the network. They cannot protect against social engineering and dumpster diving. They can generally only work on inspectable traffic and thus are not suitable for encrypted traffic.

Generally anyone who is responsible for a private network connected to a public network should use a firewall. Any computer connected to a public network should have a firewall.

TCP/TP Layers

- Application Layer: This layer sends and receives data for particular applications, such as DNS, HTTP, and SMTP. The application layer itself has layers of protocols within in. For example, SMTP encapsulates the request RFC 2822 message syntax, which encapsulates MIME, which can encapsulate other standards such as HTML.

- Transport Layer: This layer provides connection-oriented or connectionless services for transporting application layer services between networks, and can optionally ensure communication reliability. TCP and UDP are commonly used transport layer protocols.

- IP Layer: This layer routes packets across networks. IPv4 is the fundamental network layer protocol for TCP/IP. Other common used protocols at the network layer are IPv6, ICMP, and IGMP.

- Hardware Layer: Also known as the data link layer, this layer handles communications on the physical network components, such as Ethernet.

Configurations

- **Packet Filtering Firewall**: This is the most basic feature of a firewall. Also known as a stateless inspection firewall, this is typically done using access control lists on a network router. Filtering inbound traffic is known as ingress filtering, while filtering outbound traffic is known as egress filtering. Stateless packet filters are generally vulnerable to attacks and exploits that take advantage of problems in the TCP/IP stack and protocol stack. They are unable to detect if a packet's network layer addressing information has been spoofed or altered. Some firewalls can reassemble fragmented packets before passing them to the internal network.

- **Stateful Inspection**: Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by examining certain values in the TCP headers to monitor the state of each connection. Each new packet is compared by the firewall to the firewall's state table to determine if the packet's state contradicts its expected state. This is generally used to monitor a sequence of packets.

- **Application Firewalls**: This improves upon standard stateful inspection by adding data analytics abilities through an inspection engine that analyzes protocols at the applicaton layer. Application firewalls can allow or deny access based on how an application is running over the network. They can also enable the identification of unexpected sequences of commands.

- **Application-Proxy Gateways**: An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. It uses a proxy agent that acts as align intermediary between two hosts that wish to communicate with each other, without allowing a direct connection between them. The proxy is meant to be transparent to the two hosts and interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed through the firewall. Typically, this offers a higher level of security that application firewalls.

- **Host Based Firewalls and Personal Firewalls**: Host based and personal firewalls provide an additional layer of security against network-based attacks. They monitor and control the incoming and outgoing network traffic for a single host. Host based firewalls are typically available as part of server operating systems and can also advance to intrusion prevent systems.

Architecture with Multiple Layers of Firewaalls

The goal of multiple layers of firewalls is to provide defense in depth. It can also help resolve issues where users internally have varying levels of trust. A firewall between the access points and the rest of the internal network can prevent visitors from accessing the local network with the same privileges as an employee. Placing a firewall within a network that already has one at the edge requires good planning and policy coordinate to prevent inadvertent security lapses. This increase the difficulty in detecting firewall problems.

NIST Recommendations

- Firewalls should block all inbound and outbound traffic that has not been expressly permitted by the firewall policy.
- Traffic with invalid source or destination addresses should always be blocked at the network perimeter.
- Traffic from outside the network containing broadcast addresses directed inside the network should be blocked.
- Firewall policy should be based on comprehensive risk analysis.
- Many types of IPv4 addresses should be blocked by default.
- Organizations should have policies for incoming and outgoing IPv6 traffic.

Firewall Planning and Implementation

1. **Plan**: Identify all requirements that an organization should consider.
2. **Configure**: Install necessary hardware and software and set up rules.
3. **Test**: Test a prototype of the installed solution in a test or lab environment to evaluate functionality, performance, scalability, security, and identify potential risks.
4. **Deploy**: Deploy the firewall into the enterprise environment.
5. **Manage**: Manage the firewall throughout its lifecycle, which maintenance and support for operational issues.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech