**FIREWALLS - GENERAL EXPLANATION**

"You need security. You want to stop those hackers? You want to sleep well? You want to be the envy of your friends? You want to get a new head of hair? You need our brand-new, super-duper, ultra-secure, user-friendly firewall! On special just 99.99!" Sound like a sales pitch does'nt it? But all too often this is how firewalls are sold, as a be-all and end-all to network security. Firewalls aren't, and I'm sorry to tell you, they never will be. They have their place, but they are just one piece in the entire security process. Here we will go through the basics about firewalls so that you can be more informed when those snake-oil security salesmen come back.

*What a Firewall does*
Lets start with the idea of a *service*. A service is an application which is used across a network. These services generally relate to a specific application. For example, FTP (File Transfer Protocol) is an application, which offers the FTP service to clients. Now a computer can use many different types of services all streaming in and out of it's network card. It does this by keeping all the services separate, and this is done through the use of ports.

A *port* is the channel along which a service runs, and it by separating services by these channels, or ports, that a computer can separate all the data entering it's network card into meaningful streams. Now there are a large number of ports, a total of 65535, and there are some generally accepted ranges with certain uses;

| Port Range | Known As | Description |
|---|---|---|
| 0 - 1023 | "well known ports" | The services using these ports are well known and established. These service include FTP, Telnet, SSH, HTTP, etc |
| 1024 - 49151 | "registered ports" | These ports are used by vendors that have registered specific ports for use with their software |
| 49152 - 65535 | "dynamic ports" | These ports are generally used for short term connections or private connections |

And through these ports travel the data packets, and firewalls look at these packets and the data contained within them in order to decide what to do. Lets take a simplified look at a normal IP packet header;

| Size of the packet and the header length |
|---|
| How many fragments make up the data |
| Type of transport and port number |
| Sender information |
| Receiver information |
| Any options used |
| Data |

*General Types of Firewall*
Firewalls have a couple of different types, which we'll go through. But the first thing to realize is that any firewall ruleset has to use one of two basic permission policies, these are;

1. *"Allow all But"*, with this all traffic is allowed through the firewall except for the traffic you explicitly deny
2. *"Deny all Bu*t", with this all traffic through the firewall is denied except for the traffic you explicitly allow through

*Packet filtering* is the most basic type of firewalling. These firewalls can allow or deny packets based upon the source or destination of the packet, and the port or service of the packet, basically the informatin found in the header of the packet. While these firewalls process traffic very quickly, they are also very easy to subvert using

proper IP headers with malicous data payloads.

*Stateful inspection* is a more secure type of firewalling where the firewall knows about the state of a connection (in simple terms this relates to tracking the packet flags -SYN, SYNACK, ACK, FIN, RST - and ensuring that the correct sequence occurs). This means that the firewall knows whether a certain packet is related to a currently allowed session or not. This means that you can open up a port in your firewall that is unidirectional because the firewall knows enough to allow in related packets, and to deny unrelated traffic to an otherwise open port. This type of firewall also helps against port scanners because your rules can not only specify ports but also packet types, which straight away can nullify many of the more sneaky port scans.

*Application proxying* is where the packet does not actually travel through the firewall. Rather the client connects to the firewall, and the firewall makes the connection to the desired server. This type of firewall is very secure as it filters on source, destination, port, state and the actual commands used within the proxied application. The problem is the large strain this places on the firewall and the fact that not all services can be proxied.

These firewall types can are used in different implementations of firewalls;

1. Personal firewalls, these are installed on workstations and personal computers and are very useful for remote workers and as another line of defense for your network
2. Appliance firewalls are firewalls where you buy the "box", plug it in and configure it as needed via some interface. There is no specific computer or installing of software. These are very popular due to their ease of use and setup.
3. Traditional firewalls, these are dedicated machines with specific firewalling software. These tend to complicated, but are also feature rich and highly configurable.

*Firewall Problems*
As I said at the start, firewalls are not the be-all and end-all of your network security. The following points are some of the downsides of firewalls;

- A firewall can be a single point of failure. If your firewall goes down you could lose connectivity and/or your security
- Most firewalls cannot inspect encrypted traffic
- A firewall can be a bottleneck for your network. Since all traffic has to go through it, the speed as which it process the data could slow down your network speeds
- Firewalls are not fun. Most "fun" services which users want -IRC, Instant messaging, P2P, etc- tend to be heavily restricted
- Most firewalls do not stop viruses.
- A firewall with a poorly thought out set of rules is as actually worse than no firewall, because it creates the illusion of security without the reality.

Well, thats about it for a quick overview of firewalls. As always I hope it has been helpful and gives you many new ideas about how to ask the proper questions of those snake-oil firewall salesmen.