3.3 Firewall Implementation

Administrators must be able to evaluate implementation issues to achieve a successful security solution for their systems. Understanding the type of firewall means knowing how the firewall will evaluate traffic and decide what to allow and what not to allow. Understanding the firewall’s implementation means understanding how that firewall is set up in relation to the network it is protecting. The most widely used configurations include:

- Network host-based
- Dual-homed host
- Router-based firewall
- Screened host

3.3.1 Host Based

In the host-based (sometimes-called network host-based) scenario the firewall is a software solution installed on an existing machine with an existing operating system. The most significant concern in this scenario is that, no matter how good the firewall solution is, it is contingent upon the underlying operating system. In such a scenario, it is critical that the machine hosting the firewall have a hardened operating system. Hardening the operating system refers to taking several security precautions including:

- Ensuring all patches are updated
- Uninstalling unneeded applications or utilities
- Closing unused ports
- Turning off all unused services

In the network host-based implementation, you install the firewall software onto an existing server. Sometimes, the server’s operating system may come with such software. It is not at all uncommon for administrators to use a machine running Linux, configure its built-in firewall, and use that server as a firewall. The primary advantage to this option is cost. It is much cheaper to simply install firewall software onto an existing machine, and use that machine as your firewall.

3.3.2 Dual-Homed Hosts

A dual-homed host is a firewall running on a server with at least two network interfaces. This is an older methodology. Most firewalls today are implemented in actual routers, rather than servers. The server acts as a router between the network and the interfaces to which it is attached.

To make this work, the automatic routing function is disabled, meaning that an IP packet from the Internet is not routed directly to the network. The administrator can choose what packets to route and how to route them. Systems inside and outside the firewall can communicate with the dual-homed host, but cannot communicate directly with each other.

The dual-homed host configuration is simply an expanded version of the network host firewall implementation. That means it is also dependent on the security of the underlying operating system. Any time a firewall is running on a server of any kind, the security of that server's operating system becomes even more critical than normal.

This option has the advantage of being relatively simple and inexpensive. The primary disadvantage is its dependency on the underlying operating system.

3.3.3 Router-Based Firewall

Administrators can implement firewall protection on a router. In fact, even the simplest, low-end routers today have some type of firewall included. In larger networks with multiple layers of protection, this is often the first layer of protection. Although various types of firewalls can be implemented on a router, the most common type uses packet filtering. Users of a broadband connection in a home or small office can get a packet filtering firewall router to replace the basic router provided by the broadband company.

In many cases, this solution is also ideal for the firewall novice. A number of vendors supply router-based firewalls that can be preconfigured by the vendor based on the customer's needs. The customer can then install it between the network and external Internet connection. In addition, most of the widely known brands (Cisco, 3Com, etc.) offer vendor-specific training and certifications in their hardware, making it relatively easy to find qualified administrators or to train current staff.

Another valuable way to implement router-based firewalls is between subsections of a network. If a network is divided into segments, each segment needs to use a router to connect to the other segments. Using a router that also includes a firewall significantly increases security. If the security of one segment of the network is compromised, the rest of the network is not necessarily breached.

Perhaps the best advantage of router-based firewalls is the ease of setup. In many cases, the vendor will even configure the firewall for you, and all you have to do is simply plug it in. Most home-based routers today, such as those from Linksys, Belkin, or Netgear, have a built-in firewall, which in fact virtually all include firewall capability.

3.3.4 Screened Hosts

A screened host is basically a combination of firewalls. In this configuration, a combination of a bastion host and a screening router is used. The combination creates a dual firewall solution that is effective at filtering traffic. The two firewalls can be different types. The bastion host might be an application gateway and the router packet screener (or vice versa). This approach gives the advantages of both types of firewalls and is of a similar concept to the dual-homed host.

The screened host has some distinct advantages over the dual-homed firewall. Unlike the dual-homed firewall, the screened host needs only one network interface and does not require a separate subnet between the application gateway and the router. This makes the firewall more flexible, but perhaps less secure due to its reliance on only one network interface card. This means that it might be configured to pass certain trusted services to the application gateway portion of the firewall, directly to servers within the network.

The most significant concern when using the screened host is that it essentially combines two firewalls into one. Therefore, any security flaw or misconfiguration affects both firewalls. When you use a DMZ there are physically two separate firewalls, and the likelihood of any security flaw being propagated to both is low.