Global Information Assurance Certification Paper

PRIVATE INTERNET EXCHANGE

The Fastest Firewall in the World?

Introduction

There are now numerous amounts of firewalls available in today's market with a wide array of speeds, strengths and weaknesses. The limitations are based on an engineers ability to decern the needs of the client and or model and provide the correct product choice, followed by proper deployment, configuration and management. Without proper implementation, maintenance and follow-up no firewall is invincible.

Why a Firewall?

Why a firewall? Now that's a good question, The term firewall comes from a device used to protect people from fire. The firewall is a shield of material resistant to fire that is placed between a potential fire and the people it is protecting. The firewall I'm going to discuss has nothing to do with fire or flames, but a wall that is place between the Internet (UN-trusted space) and a company's Intranet (trusted space). Firewalls have been around for many years and have been gaining more popularity as the Internet grows. In simple terms the firewall is a basic computer with more than one network interface card. It will sit between two or more networks with special rules that allow certain traffic to pass to other networks. You can think of a firewall like a gate at a Military base. You have a highly secured entrance with a guard. Before entering the base you first need clearance (authorization), then you need to present identification (authentication) to the guard, and he may allow or deny access to the base, the guard will then log the transaction (accounting) just because you approached the entrance. In the IP world a firewall essentially will act like a security guard at the perimeter of your network. Adhering to a set of rules that are set forth.

The History of TCP/IP

Before we can understand how firewalls work, we'll first discuss the origination of the Internet Protocol (IP) and how computers communicate over a switched IP network. TCP/IP was developed by the Defense Advanced Research Projects Agency (DARPA) in 1970. Years later it was introduced to the world through the Berkley Software Distribution (BSD), UNIX included TCP/IP Transmission Control Protocol / Internet Protocol in their O/S and it became the foundation of what the Internet is today.

TCP/IP the Layers

The TCP/IP model consists of 4 layers; each layer provides a very important duty. The layers of protocols were designed to provide reliability, scalability and communications between heterogeneous networks. The first, the link layer, is responsible for communicating with the actual network hardware (e.g., the Ethernet card). The data that's received off the network wire gets handed off to the network layer. This is where device drivers for different interfaces reside.

The second, the network layer, is responsible for figuring out how to get data to its destination. Making no guarantee about whether data will reach its destination, it just decides where the data should be sent. The third, the transport layer, provides data flows for the application layer. It is at the transport layer where guarantees of reliability may be made. The fourth, the application layer, is where users typically interact with the network. This is where TELNET, FTP, EMAIL, IRC, WEB, etc... reside. Figure 1 has been provided to create a visual understanding of the layers and how a packet travels down through each layer when the packet is transmitted and up each layer when the packets are received at the other end. Packets are the basic unit of transmission on the Internet.

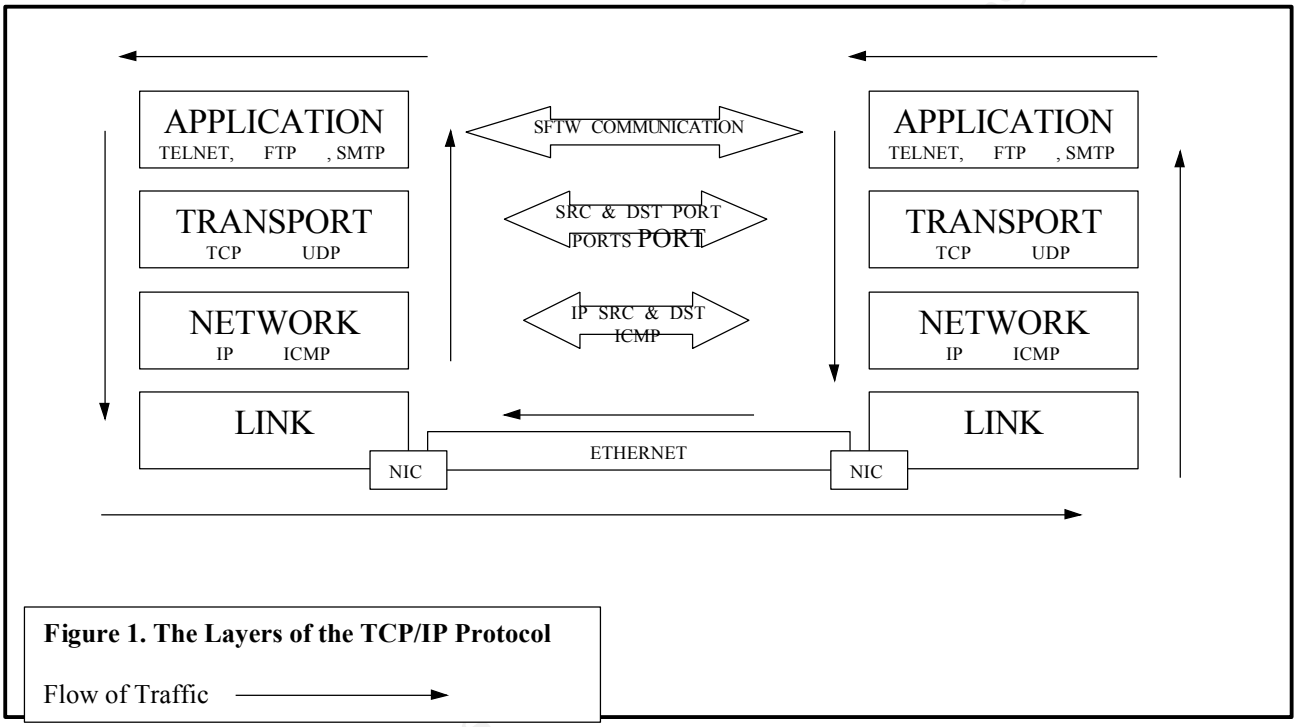

Figure 1. The Layers of the TCP/IP Protocol

How do Firewalls Work?

The Firewall sits in between two networks and acts like a gateway to either of the networks. Understanding the function of TCP/IP and how it communicates, traffic can be controlled between these networks. We can find information like the source and the destination of the traffic (network layer), what protocols are being used (transport layer), and what application are communicating (application layer). The Firewall inspects every packet that enters its interface and compares the information against a security policy or rule base. The security policy is a set of rules using TCP/IP properties to accomplish access control over an IP switched packet network.

Different types of Firewall Technologies

Any device that controls network traffic for security reasons can be called a firewall. There are three major types of firewalls, each using a different strategy to protect network resources. The most basic firewall devices are built on routers. These work in the lower layers of the network protocol stack by filtering packets (these firewalls are sometimes called screening routers or packet filtering firewalls). A second form of firewalls are Proxy server gateways or application layer firewalls. These work at the upper levels of the protocol stack, and provide proxy services on external networks for internal clients and monitor and control and traffic by looking at certain information inside packets. The third type of firewall uses state-full inspection techniques to compare the bit patterns of the packets to packets already known to be trusted. Firewalls manufactures may use one or a combination of these technologies.

Commercial Firewalls Available

Several companies have designed and manufactured firewalls for commercial use.
There are a number of basic design issues that should be addressed when choosing a firewall for implementation. For the engineer the key is to understand the needs of the client when choosing the best firewall to use. There still does not exist a gold standard firewall that outshines in all areas of protection, implementation and cost effectiveness. However from the pack of available manufacturer firewalls listed below the Cisco Secure PIX has several outstanding qualities that makes it a fierce reliable competitor in the sea of manufactured firewalls.

Firewall Name	Company Name	Web-site URL
Cisco PIX Firewall	*Cisco Systems Inc.*	www.cisco.com
Firewall-1	Checkpoint Technologies	www.checkpoint.com
Raptor Firewall	Axent Technologies	www.axent.com
Cyberguard	*CyberGuard Corporation*	Http://cyberguard.com/
Guardian	NetGuard Inc.	http://www.ntguard.com/
Netscreen 100	Netscreen Technologies	www.netscreen.com
SideWinder	Secure Computing	www.securecomputing.com

The Firewall of choice (The PIX)

The PIX Background

The PIX firewall was not the brainchild of Cisco Systems. The PIX originally developed by a company called Network Translations Inc., in 1994 did not get acquired by Cisco until the fall of 1995 and has since been flourishing under Cisco's marketing wing. It was originally developed for the dual use as a network translation device and also a firewall.

The Operating System

The PIX's operating system is a proprietary, Non-UNIX, secure, real time embedded system, and entirely less than three megabytes in size. This means that the PIX OS is specialized where it's

sole purpose is dedicated building translations and filtering packets through a designed rule base. Most other firewalls still require UNIX or Windows NT operation systems. Thus, these systems where not designed with the sole purpose for firewall use in mind.

The Hardware

The PIX is a solid state firewall this means there are no moving parts, well except one "the fan," that cools the power supply and the rest of the PIX's components. The PIX IOS (Integrated Operating System) runs on an i386 platform an industry standard for PC market. The PC 100 motherboard is usually equipped with a Pentium II 350MHz, 16 MB of flash, 128MB of RAM and three PCI expansion slots for additional NICs or the VPN accelerator card. All this powerful hardware is encased in a nineteen-inch rackable gray shell.

Access Control (packet filtering) and State-full Inspection (ASA)

Other key features of the PIX firewall is its strength of security when used with Cisco router access control lists for packet filtering. The nucleus of the PIX firewall is the Adaptive Security Algorithm (ASA) which is less complex but more robust than the standard packet filtering system. ASA offers state-full connection oriented security while tracing the source and destination address, TCP sequences as well as additional TCP flags and information which is then stored within a table of inbound and outbound packets ultimately controlled by the security policy applied. Only transmissions that match the administrators defined table will be allowed freeway access through the firewall.

Not A Router

Note the PIX firewall is NOT a router. This device does not route traffic yet it passes information determined by predefined static translation rules from one security level to another, due to it's unique sub-system the software can communicate directly with it's hardware. The PIX provides a bridge like layer I connection that filters layers II and III for access control. This feature explains the PIX Firewall's speed and ability to handle information at 370 MB / sec.

Running at the SPEED OF LIGHT

As the Internet grows and prospers the users needs are becoming a lot more demanding and important, the need for speed is increasing every day. Currently large company's infrastructures demand fast connections to the Internet and they need not only a firewall that can handle line speeds, but can handle the speeds in a secure fashion. One of the PIX's greatest features is its speed and the amount of simultaneous connections it can handle without jeopardizing security.

PIX Speed Specifications

Model	Throughput	Simultaneous Sessions

PIX 535	1 Gbps	500,000
PIX 525	370 Mbps	280,000
PIX 520	370 Mbps	250,000
PIX 515	120 Mbps	125,000
PIX 506	10 Mbps	XXXXX

Failover/Hot-Standby

The PIX offers an failover option for approximately $5000 this results in a continuous hot standby. Other commercial competitors will offer similar failover capabilities however cost for the additional firewall is the same as the primary firewall thus doubling the cost. The PIX Failover is achieved with a secondary PIX and a specialized serial (failover) cable which will allow configuration and failover information to pass from one PIX to another. "Heartbeats" are transferred back and forth through the failover and Ethernet cables to allow for the state of the PIX to be continuously monitored. With the PIX, implementation is simple and quick. Only one PIX firewall needs to be configured for failover, once that is done, the failover cable is connected, failover is turned on for the primary unit. All configuration information will sync to the secondary unit and then will provide a HOT standby firewall.

Back up and Restores

One of the most crucial parts of any computer device is the backing up and restoration of its information. Simplicity and speed are also very important. The PIX firewall is one of the fasted on the market, just like a Cisco router. Not only for backing up and restoring its config, but loading it's Operation System. The config can be backed up or restored in three different ways because the configuration is kept in a flat ASCII text format.

- Copy and Pasted into a text editor
- Transferred directly to a floppy
- Via a TFTP server

If an older PIX fails a brand new PIX (cold standby) with no config can be set up in minutes. The config can fit on a floppy the maximum PIX config at this time is about 340KB.

The PIX – Why A Firewall Appliance is the Way to Go?

- Compact
- Plug and Play
- Dedicated Device
- Single vendor for H/W and S/W

Conclusion

The role of security and protecting networks with Firewalls are evolving at ridiculous speeds.

Everyday new Firewall technologies are being developed and introduced to the industry to meet market demands. Companies are interested in security devices that can handle data transmissions at wire speeds that will plug and play right into their network, with easy to use GUI's which allows ease of management. The Private Internet eXchange (PIX) happens to meet the current demands of the market. The real question will be how long will the PIX maintain its ability to satisfy the security industry's quest for the fastest firewall in the wall?

Internet References

Under the hood of the Internet: An overview of the TCP/IP Protocol Suite
Jason Yanowitz
http://www.smeal.psu.edu/misweb/datacomm/tcp_ip.html

Firewall Technologies and Firewall Selection
Milkyway Networks
http://www.mikyway.com/libr/mwm-96-0101.html

Special Report: Firewalls For All
http://www.networkmagazine.com/article/NMG20010521S0007

General Firewall Information
http://www.cyberangels.org/net-ed/classes/firewall.html

Cisco PIX Firewalls
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

Book References

Building Internet Firewalls", O'Reilly & Associates
Chapman / Zwicky

Firewalls and Internet Security
Cheswick / Bellovin

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event