Global Information Assurance Certification Paper

Firewall Network Appliance
Craig Simmons
October 10, 2000

Introduction

This paper will discuss the firewall network appliance. What they are. How they compare to the traditional firewalls. What the advantages of using them are and who can benefit from them.

Firewall Appliances

Firewall appliances offer perimeter based network security. Like regular firewalls they can be application gateways, packet filters, or circuit level gateways. In fact firewall appliances are just as diverse as any firewall product.

The need for firewalls

The need for security has never been greater. Every week there are new advisories about the vulnerabilities of users connected to the Internet. If you are on the Internet chances are someone has already tried to access your system. Whether a port scan or a network map. Someone out there has probed your network. Firewalls are a method for keeping a network secure. A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. They keep the bad guys out and allow the good guys access to the Internet in a secure fashion. At this point no one should be questioning the need for security for computer networks and systems connected to the Internet. The idea that you may be liable for damages to other systems if a hacker uses you as a launch point for an attack is reason enough to secure your network. Since liability lies in not taking necessary steps to secure your network. Everyone needs security. The problem is security can be am expense proposition. Firewalls require expense hardware, expense software, and personnel with technical knowledge. Which don't come cheap either. The solution is firewall network appliances.

What are they

Traditionally you had to run a firewall software package on top of a general-purpose operating system to get a decent level of security for your network. Whether it was Unix or Windows NT, it was still the same, you needed a security system, but you got a whole lot more. Because the firewall application ran on top of the operating system, other services were always running underneath. Plus, shell access was possible on a Unix host and potential vulnerabilities existed throughout the system. Windows NT has a myriad of vulnerabilities. Although it is possible to harden an operating system by shutting down unnecessary services and patching holes, its not always 100 percent effective. And there is a lot of room for human error. Many systems that are breached are because the system administrator did not properly configure them.

A firewall network appliances is a devices that has the dedicated function of a firewall. They typically have multiple network interfaces. Physically most are about the size of VCR and can be rack mounted. They may also have serial ports for console connections or other features. Inside they contain a CPU memory and secondary storage devices like a hard drive. Most of these components can be recognized as off the shelf that can be part of any PC. The multiple interfaces are setup to separate the outside network for the inside. They are also typically configured remotely. Many vendors are using the Linux operating systems. This helps keep the cost lower by eliminating software licensing. Although Service Strategic Inc. has build an appliance with embedded Windows NT. There are solid-state devices that have no moving parts at all. The can reduce vulnerability even further by eliminating the chance of mechanical failure.

How firewall network appliances compare to full blown firewall implementations

Some might think that firewall appliances are just stripped down versions of a full-blown firewall and in order to have any real security a traditional firewall must be used. Not true. Examining Axent Technologies VelociRaptor Firewall Appliance allows a direct comparison. The VelociRaptor Firewall is a stand-alone Linux-based firewall appliance that provides the proven security of Axent's Raptor Firewall. The VelociRaptor Firewall comes equipped with four network interfaces, two serial ports, and a front LCD panel. Memory, CPU, and, drive configurations may vary based on model. Raptor Firewall V6.5 software and the Linux operating system are preloaded onto the VelociRaptor appliance making the unit ready for use right out of the box. The VelociRaptor appliance is a proxy-based firewall that works at the application level using a set of application-specific security proxies. Built-in support for Virtual Private Network tunnels allows the VelociRaptor administrator to create secure network level sessions. Additionally, packet filtering on

a per-interface and per-tunnel basis provides increased flexibility to system administrators and end users. Similar to the Raptor Firewall, the VelociRaptor Firewall appliance provides an easy-to-configure and easy-to-manage graphical user interface called the Raptor Management Console (RMC). The RMC is designed as a snap-in module for the Microsoft Management Console. You install RMC on a remote Windows NT system and logon to VelociRaptor for secure remote management sessions

Testing several of the features that are commonly used in most configurations reveals that the same features are available and the user interface is identical to Raptor running on a traditional setup. Expertise in one product would cover you for both. The appliance offers the same features at a fraction of the price.

What advantages are there?

Full-featured product with lower cost. They are most beneficial to small to mid-sized business and educational facilities that have dedicated Internet connections. Also perfect for deploying within larger organizations to segregate divisions that are remotely located or are internal and need extra security. May fit well into multi tiered security solutions. Minimal maintenance and upkeep is required. All in one solution. There is no additional hardware to buy, no operating system and no licensing costs. Specially designed to be a Firewall and firewall only. Carries a small footprint. Do not include unnecessary hardware or software that increase cost and add possible vulnerabilities. By doing away with system extras, the firewall vendors can concentrate on making a secure system with little chance for error.

Who are firewall appliances best suited for?

Firewall Appliances are great solutions for small to mid–sized organizations. Who want to or already have their business on the Internet. Since they typically require little maintenance they are perfect for shops where maintaining the firewall is just one of the network administrators many jobs. We've seen that appliances offer all the features we've come to expect in a firewall at a reduced cost. Are firewall appliances the next step in the firewall evolution? One day will there only be appliances? It's hard to say. The devices do have the capability. What we can say is that appliances make security affordable for everyone. Security that no one can afford to be without.

List of Products

VelociRaptor (currently Beta 1.0)
http://www.axent.com

GB-100
http://www.gnatbox.com/

SonicWall
http://www.sonicwall.com/

GuardianPro *e*NT
http://www.ssimail.com/

LuciGate
http://www.lucidata.com/

FoxBox
http://www.netwolves.com/

References

"Firewall Appliance hardware controls access, hackerproof, low cost; secure, Independent, Network Security, IP Filter" URL http://www.lucidata.com/firewall.htm (August 11th 2000)

Schultz, Kevin "Firewall Appliances: Look Ma! No Moving Parts" CMP Media Inc Copyright © 2000. URL http://www.internetwk.com/reviews/rev070599.htm July 5, 1999

Vicom Technology Ltd "Firewall Q&A" Copyright © 2000
URL http://www.vicomsoft.com/knowledge/reference/firewalls1.html#1

Global Technology Associates "GB-100 Firewall Appliance" Copyright © 2000

URL http://www.gnatbox.com/Pages/GB100.html

"NetWolves FoxBox - Internet Security Firewall Network appliance prevents hacker intrusion and Allows Internet Access, Internet Connection"
URL http://www.netwolves.com/app_internet_access.html

*Service Strategies Inc."*NT Firewall Appliance" Copyright © 1998,1999,2000
URL http://www.ssimail.com/NT_firewall_appliance.htm (April 10, 2000.)

Axent Technologies Inc "Raptor Systems, Inc - Customer Support" Copyright 1999
URL http://www.raptor.com/cs/

SonicWALL, Inc "SonicWALL Product Overview" Copyright © 2000
URL http://www.sonicwall.com/products.html

Last Updated: July 26th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event