Chapter 30

CHOOSING THE RIGHT FIREWALL

INTRODUCTION

As the topology and threatscape of modern networks becomes increasingly complex, enterprise and administrative resources have become stretched ever thinner. Corporations and businesses are increasingly reliant on both the internal resources of the network as well as on external communications for day-to-day business functions. More and more of these functions are relegated to automation, with things like faxing, scanning, and document management integrating with network resources. Networks have truly emerged in this century as the cornerstone, if not the foundation, of critical business operations [1].

When the Internet is down, when the server is down, if faxing is offline, or if the network copier is on the blink, business literally grinds to a halt. And, typically, the reason that these things happen is because malicious software has wormed its way into the network, somewhere, and somehow. There are many avenues of intrusion, and there are many things that can ostensibly be implemented to fortify against such occurrences. But implementing all of them, and then maintaining patches, product updates, definitions, etc, for a slew of devices and products is not at the top of any network administrator's list of favorite things to be doing. The most rewarding and creative part of a Network Administrators job is to introduce and manage change, in ways that are beneficial to business, improve the ability to do business, and streamline business functions [1].

Playing babysitter to a bunch of equipment and software programs, and subsequently playing checkpoint police + border guard, doesn't fit into a philosophy of network change designed to improve competitiveness. As a result of the overwhelming market demand, most security firms that create firewall and other security products have moved toward a Secure Content Management (SCM) approach [1].

In these times, everyone (from the local florist to small law firms to multinational corporations) everyone is prey to harvesters seeking to build their own personal empires of subjugated computers around the world. With cracker-hackers-jackers running IP address scanners and automated cracking software, and with so many DSL install techs leaving the

default username and password for router access, it is actually a rather simple matter to crack into small networks. This chapter explores, in depth, the aspects of security and exemplifies several existing solutions [1].

Firewalls, from policy development through to deployment, have a wide variety of incarnations. Interestingly enough, physical firewalls (those things that are used to actually stop the spread of fire in the firefighting and fire prevention professions) are closely analogous to information security firewalls. Just as fire needs fuel, heat, and oxygen, security attacks are also dependent on several factors, each of which can be addressed by a single unit or by a more elaborate, specialized system. Such a system brings together best of breed products in a serialized approach to examining network activity, traffic, habits, and characteristics to determine if, in fact, an attack is in progress, and to prevent known types of attacks, viruses, worms, email, spam, etc, from ever entering the network [1].

Such systems are those that are discussed in this chapter. Systems that, through a single appliance or several appliances, are capable of noticing and controlling an intrusion, regardless of its methods. This chapter also highlights single products that are part of a larger whole, or collective, of products that is marketed within a firewall context. This context is referred to by some as a Secure Content Management (SCM) offering. Central management of a host of firewall duties is the goal, something intended to de-stress the life of the network administrator and simplify security controls [1].

Some sources (Task Force on Information Warfare and Information Assurance) estimate that over 40 million people on this planet are equipped with, and knowledgeable in the use of, cracking tools. It's no surprise, then, that in the last few years, permutations in methods of attack have telescoped like a power function while the solutions and varieties of methods to repulse them have experienced little growth. They have, in fact, experienced a contraction, or convergence, of sorts [1].

CONVERGENCE

As attack methods grow in complexity and sophistication, it is almost beyond the ability, if not the scope, of one manufacturer to present a solution that can effectively strip the ground, evacuate the villages, provide aerial extinguishment, patrol surrounding areas for additional threats, provide crowd control, perimeter security and damage control. Such an operation invariably requires the efforts and cooperation of multiple platforms of proficiency. Spam. Viruses. Trojans. Spyware, adware, and malware. Critical updates and Patches. Packet filtering. Forces beyond anyone's ability to control are creating virtual conflagrations on an epoch scale – they have free-reign and are here to stay for as long as there is an Internet [1].

The Criminal MeagerMind

Cyber Crime is the highway robbery of the next generation criminal, and with its high cash payoffs, light sentencing (if caught), and book and movie consultation deals, it doesn't take a mastermind to figure out how to run a scam that will lift sessions cookies and steal