eSoft

Technical White Paper:
Who Needs Firewall Protection?

"Without the protection of a firewall, which serves as a buffer between an organization's internal network and myriad external networks—including the Internet—any network is vulnerable to threat or misuse by a multitude of entities."

eSoft, Inc • 2990 Gateway Dr., #950 • Norcross, GA 30071
770.448.0334 • Fax 770.448.4547
www.esoft.com

Who Needs Firewall Protection?

Overview

If your company uses the Internet, chances are that you need a firewall. Fast becoming the most popular form of electronic communication, the Internet brings the entire world to your door. Information security experts suggest that you invest in some method of network security, so you can make sure that it is opportunity knocking at that door, and not a cyber criminal in disguise.

What is Firewall Protection?

A firewall is the most important line of defense between a company's network and the outside world. It serves as a buffer between an organization's internal network (Intranet) and external networks (Internet). Just as Internet use by businesses has escalated sharply in recent years, so too has the occurrence of network security breaches. Firewalls can provide protection for classified information by using different types of application proxies, which are designed to check every connection that crosses the firewall. Many firewall appliances also offer email filtering, web site filtering, security scanning services, and real-time alerting when a breach is attempted.

Who's Behind the Attack?

What threatens the security of a computer network? And who is most at risk? Without the protection of a firewall, any network is vulnerable to threat or misuse by outside entities. These intruders range from *cyber vandals*—often computer-savvy youth intent on causing mischief—to *cyber criminals* who illegally penetrate systems with the express purpose of damaging those systems or obtaining resources. Overall, you should be aware of possible attacks from anyone with the capability, technology, opportunity and intent to do harm. Profiles may include terrorists, insiders, disgruntled employees and hackers.

Types of Threats

The most widespread forms of security breaches—and often the most easily detectable—included laptop computer theft, employee abuse of Internet privileges, and telecommunications fraud. More sophisticated security breaches include unauthorized access by insiders, theft of proprietary information, financial fraud, sabotage of data or networks, and system penetration from outside.

Indeed, many information security experts feel that the biggest threat to both the public and private sector are information terrorists—those who specialize in corporate misinformation and bribery. These can include rival companies who eavesdrop on online meetings as well as a company's own staff. Some experts suggest that the planting of misleading and fraudulent data is the biggest threat posed to companies and governments in this new age of information warfare.

These same types of threats jeopardize organizations both large and small. As evidenced by the recent highly publicized attacks against Yahoo, CNN, eBay, Amazon.com, and Buy.com, no

company is completely immune. Larger companies like these generally take more than adequate precautions with their network security to fend off external attacks. However, hackers are always finding new ways to beat the system, even if it is by taking a very indirect route. In this instance, they used a technique called *Distributed Denial of Service*.

Denial of Service attacks—flooding a web site with thousands of bogus requests so that it no longer has the resources to respond to legitimate requests—represent another tactic common to both cyber vandals and their more ominous counterparts. After an attack, victims are left to ponder whether the act was just mischievousness or, more disturbing, a real attempt to manipulate and/or sabotage vital corporate information.

To launch this kind of attack, hackers enlist the unwitting assistance of dozens, hundreds, or even thousands of smaller unprotected systems with dedicated full-time Internet connections (DSL or cable modems, for example) spread out around the globe. Taking advantage of the lax security on these systems and their lack of firewall protection, the perpetrator disseminates an attack program that surreptitiously installs itself and lies dormant on these systems, awaiting the attack command from a central control point. When the command is given, all of these *agent* systems launch coordinated denial of service attacks against the specified target. The huge volume of bogus traffic makes the target server unresponsive to real requests, and the fact that it comes from so many sources, often with forged or randomized return addresses, makes it very difficult to block the attack at the target, or track down its origins. One might think that this is an enormous endeavor, orchestrated by hundreds of people. Surprisingly, it is often only a single individual or small group of individuals who are working together.

Even the most sophisticated firewalls available today are powerless to block this kind of attack. Prevention must come instead from protecting the agent systems from being co-opted in the first place. One sure way to prevent this kind of an attack is to install a firewall in front of every network with a high-speed Internet connection. It is also imperative to take advantage of available security scanning tools to find and fix weaknesses in the security of systems that have to remain directly exposed to the Internet. If your network has no holes in it, the hackers have no way to get in and take control of your systems.

Do You Need a Firewall?

Organizations that are contemplating the Internet as an integral business component should ask themselves two simple but important questions. First, *would access to the Internet offer value to both our customers and our staff?* If so, *is the business information we store on our computer network worth protecting?*

In today's *e*-marketplace, more often than not, the answer to both questions is a resounding YES! If this is the case for your company, then consider this, *what would a security breach cost the firm in terms of money, lost productivity, or public relations liability?* Doesn't it make sense to obtain the best insurance you can afford to protect your network and information resources?

Firewall Features

When looking to purchase a firewall, there are many features that you will want to consider. For example, eSoft's Interceptor Firewall Appliance includes robust policy-based access control, remote user and remote office VPN, real-time alerting, spam

filtering, web site filtering, reporting tools and much more. Whether it's internal or external security risks, you will want to find a solution that protects your network and safeguards your Internet communications with premium security. To many companies, ease-of-use and affordability are also big factors to weigh in the decision making process.

Secure VPN Technology

Virtual Private Networks allow you to use the public Internet to securely connect remote offices and remote employees at a fraction of the cost of dedicated, private telephone lines. There are two major uses for VPNs. The first is to connect two or more geographically separated networks, such as those at a main office and a remote branch office. The second is to allow employees or authorized users to access a network from a remote PC, such as traveling laptop or home computer. Both of these uses permit access to protected network resources by authorized users. eSoft's Interceptor Firewall Appliance provides solutions geared toward the unique requirements of each.

Internet Usage Policy: E-Mail/Web Filtering

Keep your employees' minds on their work, and keep your peace of mind. With a firewall that has e-mail and web filtering, and management reporting, you can ensure that your employees are not spending their time inappropriately surfing the net. You can also monitor e-mail usage so that you aren't getting Spam e-mail--unsolicited or mass mail messages--that wastes your employees' time and slows down your network.

How We Can Help

eSoft’s mission is to help small to medium-sized businesses simply, reliably and inexpensively harness the power of the Internet. We market the Interceptor Firewall, Appliance along with the TEAM Internet line of connectivity products. Our products incorporate all of the aforementioned features and capabilities, and more, into a turnkey package that includes all the hardware, software, and services you need to safely connect your small business to the Internet. We have marshaled our considerable expertise in network security and Internet technologies to create products that do not require expertise in either area to be used effectively. The products are virtually self-configuring, requiring answers to only a few simple questions to be up and running. Even the ongoing administration of the products is managed entirely through an intuitive web-based user interface, making our solutions easy, cost-effective, and smart for your company.

For more information, please contact us at:

eSoft, Inc.
295 Interlocken Blvd., #500
Broomfield, CO 80021
303.444.1600
Fax 303.444.1640
E-mail: info@esoft.com
www.esoft.com