

TELEMANUALS

**Are
They
Good
Enough?**

Today, most businesses, regardless of size, believe that access to the Internet is imperative if they are going to compete effectively. Even though the benefits of connecting to the Internet are considerable, so are the risks. With the tremendous explosion of network usage and Internet connectivity, most of the corporations, small and medium businesses and for that matter, home users are heavily dependant on data networks for business and other personal applications.

Data networks are vulnerable to a series of threats posed by hackers. Corporation are at risk of their intellectual properties, electronic payments,

alright . Other sessions are dropped and a detailed log is maintained.

Evolution

Firewalls generally protect a network from attacks. Historically companies would tolerate a decrease in network throughput in exchange for security, given the threat of attack and cost of system downtime. As a result firewall technology has been developed with the focus placed on functionality.

The original idea was formed in response to a number of major Internet security breaches that occurred in the late 1980s. The earliest of this form was the development of “packet filter firewall” that would analyze network traffic at the transport protocol layer. Each IP network packet would examine to see if it matches one of a set of rules defining what data flows were allowed. Later three colleagues from AT&T Bell Laboratories helped develop the second generation of firewalls known as “circuit level firewall” that validated the fact that a packet was either a connection request or a data packet belonging to a connection, or virtual circuit, between two peer transport layers. As it was also able to determine if a packet was either a new connection or data that is part of an existing connection, it was also referred as “stateful firewall”. Later on arrived the third-generation firewall technology “application layer firewall” also known as proxy based firewalls that would evaluate network packets for valid data at the application layer before allowing a connection. It examined the data in all network packets at the application layer and maintained complete connection state and information sequence. In addition, an application layer firewall could validate other security items that only appeared within the application layer data, such as user passwords and service requests. A “dynamic packet filter firewall” was a fourth-generation firewall technology that would allow for modification of the security rule base on the move.

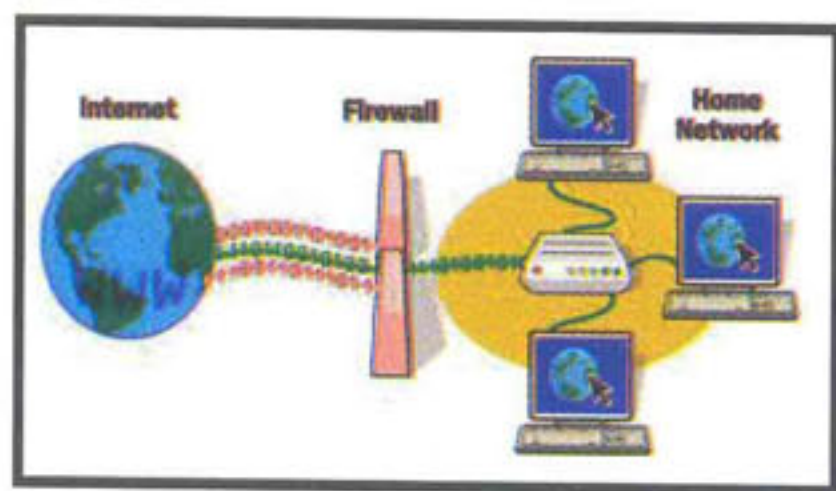
According to Digvijaysinh Chudasama, VP—Sales, Cyberoam, firewall has gradually evolved

information and customer database and various other forms of tangible and intangible assets. In response to these risks, a whole industry has formed during the last several years to meet the needs of businesses wanting to take advantage of the benefits of being connected to the Internet while still maintaining the confidentiality, integrity, and availability of their own private information and network resources. This industry revolves around firewall technology.

Firewall is the first level of gate which act as security guard who is trained on who should be allowed and who should be rejected. And also, allow the users with varied privileges. Firewall is typically configured with a set of rules which defines the corporations data network details and allows only those sessions which appears to be

As Firewalls become a default security feature of every Internet security system today, its effective usage and deployment is still a disputed subject. In this article, we discuss the various advantages and its limitations along with the latest trends.

from a single-point security application to an extensive network security feature with the Unified Threat Management appliances with Anti-Virus functionality.



Graphical Representation of a Firewall Security System

Pros and Cons

Pros:

Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections, and block services that are known to be problems.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the “outside” world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect you against any type of network-borne attack if you unplug it.

Firewalls are also important since they can provide a single “choke point” where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective “phone tap” and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc.

Because of this, firewall logs are critically important data. They can be used as evidence in a court of law in most countries. You should safeguard, analyze

and protect your firewall logs accordingly.

This is an important point: providing this “choke point” can serve the same purpose on your network as a guarded gate can for your site’s physical premises. That means anytime you have a change in “zones” or levels of sensitivity, such a checkpoint is appropriate. A company rarely has only an outside gate and no receptionist or security staff to check badges on the way in. If there are layers of security on your site, it’s reasonable to expect layers of security on your network.

Cons:

Firewalls can’t protect against attacks that don’t go through the firewall. Many corporations that connect to the Internet

are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape, compact disc, DVD, or USB flash drives can just as effectively be used to export data. Many organizations that are terrified (at a management level) of Internet connections have no coherent policy about how dial-in access via modems should be protected. It’s silly to build a six-foot thick steel door when you live in a wooden house, but there are a lot of organizations out there buying expensive firewalls and neglecting the numerous other back-doors into their network. For a firewall to work, it must be a part of a consistent overall organizational security architecture. Firewall policies must

Hardware vs Software

Firewalls basically come in two different “flavors”—hardware and software. Firewalls are intended to be a “traffic cop” of sorts in that; they monitor incoming and outgoing Network traffic. Firewalls help keep “bad stuff” from accessing your computer and/or your Internet connection.

These days, the Internet is becoming less and less secure. Brand new computers, right out of the box, will almost certainly become infected, hacked, etc., if they are simply plugged into a hi-speed Internet connection with no form of protection.

As a convenience, many AntiVirus manufacturers have now created Software Firewalls as part of their “security suites.” This however, can be a double-edge sword. The key difference between a Software Firewall and a Hardware Firewall is this—a Software Firewall must be installed on your computer just like any other application software is, while a Hardware Firewall is a stand-alone device that connects to your hi-speed “modem.” The benefits of using a Software Firewall are, you simply install from a CD or download and you have a Firewall. The downsides are, this Software Firewall is now consuming a HUGE chunk of your system’s resources (Physical Memory, Hard Drive access times, etc.) This can bring many systems to a screeching halt.

The benefits of using a Hardware Firewall are, it does not run on your PC directly rather, it is its own stand-alone box. This leaves your PC to do what it is meant to do—run application software. There really aren’t any downsides to a Hardware Firewall as far as configuration goes because all of the major manufacturers of Firewalls (i.e., Linksys, DLink, NetGear, etc.) provide you with “1-click” setup wizards. They are no more difficult to configure than a Software Firewall is.

If anything, they are easier now-a-days.

Ultimately, all Software and Hardware must be configured to some extent. The key is, do you want your PC to be dragged down via tons of other Software, or do you want it to truly be there to help you?



be realistic and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: they shouldn't be hooking up to the Internet in the first place, or the systems with the really secret data should be isolated from the rest of the corporate network.

Another thing a firewall can't really protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he's just as likely to export it through a telephone, FAX machine, or Compact Disc. CDs are a far more likely means for information to leak from your organization than a firewall. Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall, if he can find a "helpful" employee inside who can be fooled into giving access to a modem pool. Before deciding this isn't a problem in your organization, ask yourself how much trouble a contractor has getting logged into the network or how much difficulty a user who forgot his password has getting it reset. If the people on the help desk

believe that every call is internal, you have a problem that can't be fixed by tightening controls on the firewalls.

Firewalls can't protect against tunneling over most application protocols to trojaned or poorly written clients. There are no magic bullets and a firewall is not an excuse to not implement software controls on internal networks or ignore host security on servers. Tunneling "bad" things over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated. Security isn't "fire and forget".

Lastly, firewalls can't protect against bad things being allowed through them. For instance, many Trojan Horses use the Internet Relay Chat (IRC) protocol to allow an attacker to control a compromised internal host from a public IRC server. If you allow any internal system to connect to any external system, then your firewall will provide no protection from this vector of attack.

Hardware or Software?

Do we need a combination of Hardware and software firewall or any one is enough? According to Sajan Paul, Head—Technology and Consulting, Enterprise Solutions, Nortel India, it really depends on the performance level required. Software firewalls tend to

add unpredictable jitter and delay; they are not suitable for high volume real traffic. Software based firewalls are cost effective and may be used for low volume data traffic.

There is a third type of firewall which uses hardware acceleration for all traffic while having the flexibility like a software firewall.

Addressing the issue, Digvijaysinh says that Firewall on a custom built hardware is a norm nowadays i.e. a hardware firewall. A combination of hardware and software in a firewall allows the software to best exploit the hardware potential and a hardware design to be customized so as to make the best possible use of software. This would help deliver highly efficient results. From the applicability point of view too, its always best advised to have a combination and save on operational costs and complexity.

Future of Firewall

Next-Generation firewall products are incorporating the latest security capabilities and advanced technology and are designed to address the challenge of today's heightened corporate threat environment.

According to Sajan Paul, Firewalls are going to be more application aware and high performance oriented. It could also accommodate many of the other security frameworks in a more integrated way.

Digvijaysinh believes that firewall has gradually evolved to become an integral part of Unified Threat Management. With a lot of business communication taking place over the Internet, performance and security remain the integral part for future that would also include enhancing capabilities and delivering for multi-application layers, VoIP, Video on IP, etc.

As the focus on threats change from the combating outsider threats to developing proactive measures to handle insider threats, third generation UTM's would require identity based firewall functionality that would help provide boundless network security. ★

By: 'InfoSecurity' Bureau.