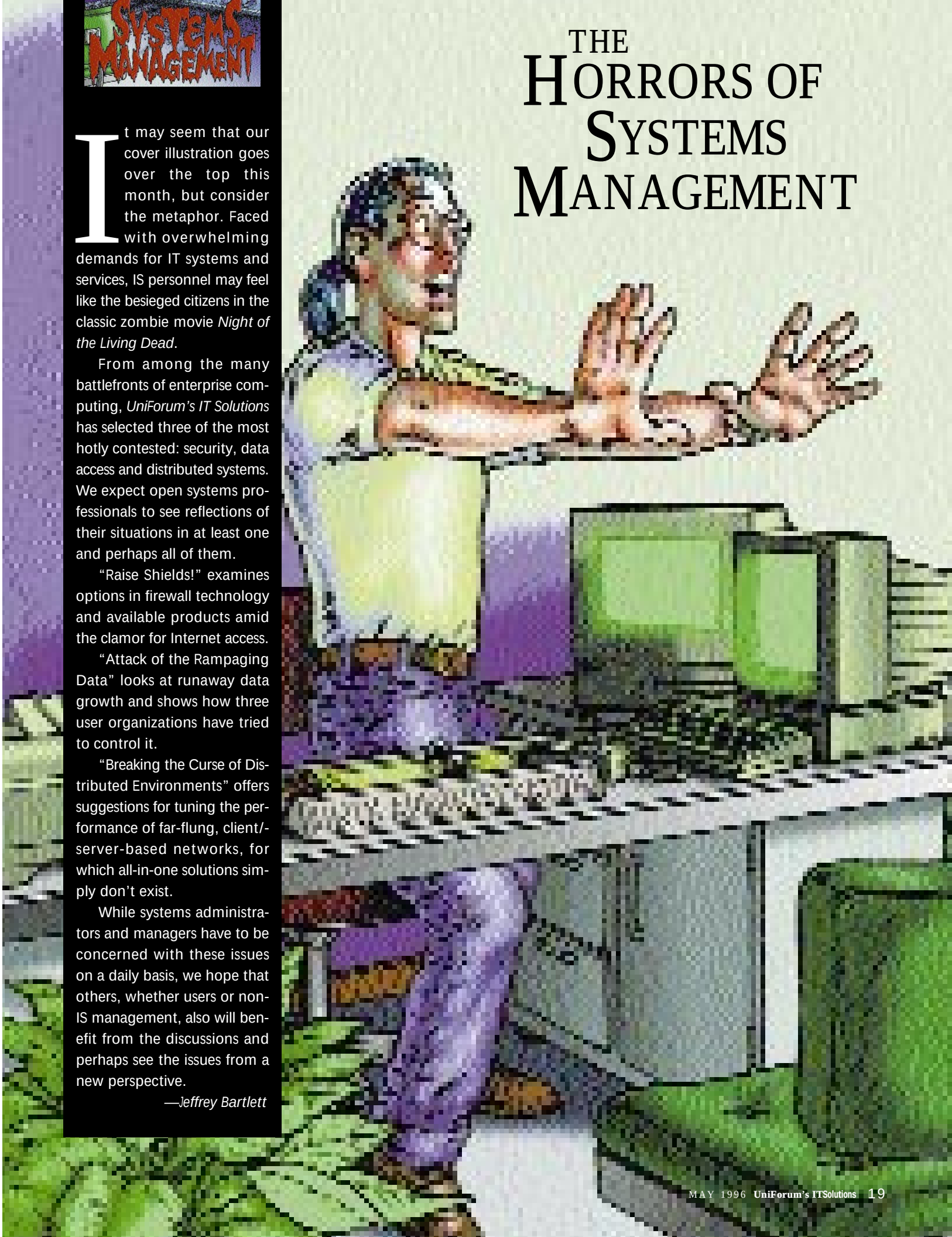
GO TO PAGE 19

THE HORRORS OF SYSTEMS MANAGEMENT



It may seem that our cover illustration goes over the top this month, but consider the metaphor. Faced with overwhelming demands for IT systems and services, IS personnel may feel like the besieged citizens in the classic zombie movie *Night of the Living Dead*.

From among the many battlefronts of enterprise computing, *UniForum's IT Solutions* has selected three of the most hotly contested: security, data access and distributed systems. We expect open systems professionals to see reflections of their situations in at least one and perhaps all of them.

"Raise Shields!" examines options in firewall technology and available products amid the clamor for Internet access.

"Attack of the Rampaging Data" looks at runaway data growth and shows how three user organizations have tried to control it.

"Breaking the Curse of Distributed Environments" offers suggestions for tuning the performance of far-flung, client/-server-based networks, for which all-in-one solutions simply don't exist.

While systems administrators and managers have to be concerned with these issues on a daily basis, we hope that others, whether users or non-IS management, also will benefit from the discussions and perhaps see the issues from a new perspective.

—Jeffrey Bartlett

Raise Shields!

Firewalls are a necessary part of most TCP/IP networks today and will be into the near future. Here is a guide to filling your organization's needs.

By Rik Farrow

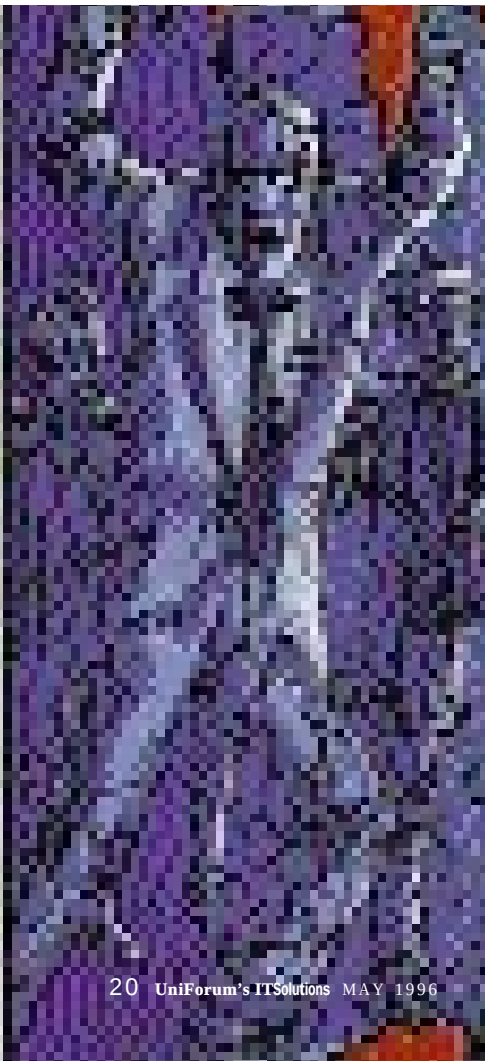
When I was a child, I dreamed of force fields. There would be a force field in my bedroom window, which would let through cool breezes, fresh air and pleasant views while keeping out bugs, humidity and burglars.

When I grew up, I saw force fields—the shields used by the Starship Enterprise in *Star Trek*. A model of flexibility, the Enterprise's shields were transparent to visible light and radio waves, yet mostly impervious to directed energy blasts from photon torpedoes and disruptors. Internal force fields surrounded prisoners, allowing visible light and sound to pass through, but not bodies or weapons fire.

Force fields are still science fiction, but a networking equivalent has been evolving over the last 10 years and has become essential for safely connecting to the Internet today. Ideally firewalls are just like their fictional counterparts—totally transparent until you want them to be otherwise. Exactly the network traffic you require can pass through, and everything else will be blocked. When an attack occurs, alarms are sent to the control panel or even to off-site individuals through pagers. The firewall can also maintain complete logs of everything that occurs so you can reconstruct past activity.

Actual firewall products can do these things, but each product is different and so are their abilities to block unwanted network traffic, issue alarms, create useful logs or support common network services. Administration and management are also key issues, especially since this technology can be both arcane and continually changing as new threats arise.

In the near future, we will be able to rely more on encryption for security solutions. But for now, firewalls are the shields of choice. Because both user organizational requirements and product capabilities vary, it takes planning to ensure that your force field does the job.



Requirements and Policy

The way to begin your firewall shopping list is by defining your requirements. Presumably, if you are connected—or plan to be connected—to the Internet, you know which Internet services (application protocols) you are or will be using. The most commonly used Internet services are Hypertext Transfer Protocol (HTTP, for the World Wide Web), Simple Mail Transfer Protocol (SMTP, for e-mail), and File Transfer Protocol (FTP), Telnet and Netnews (all for Usenet). There are variations of HTTP, such as SHTTP and HTTP-S, for secure Web transactions and other services as well. If you are looking for internal firewalls, the issue is the same.

When choosing a firewall, it is important to know how much flexibility you require. While most products support the five basic services listed above, you might require a completely nonstandard protocol, for example, to support a client/server application. Some database vendors, such as Oracle, have begun to provide their own software for passing TCP/IP requests securely through firewalls. But not all firewall products support add-on software, some because of the underlying functionality and others because of a rigid, built-in security policy that prevents other software from running.

Fundamentally related to your requirements for a firewall is the *policy*, a written statement that spells out which activities are permitted and which are forbidden

on your computers and networks. Even if you don't have a written policy, you will always have at least one (and probably many) unwritten security policies that define appropriate behavior. When it comes to enforcing your policy, a written policy avoids confusion and lets everyone know where they stand.

A firewall becomes an agent for enforcing your security policy. If your policy says that users are not allowed to use Internet Relay Chat (IRC), the firewall can block that service. If your policy states that users can copy files from the Internet using FTP but not send files, some firewalls can support this policy. But most firewalls cannot block the transmission of data—for example, e-mail—that contains information you would like to embargo. If you want to prevent e-mail from describing your new pharmaceutical product, you might wish to scan for keywords in outgoing e-mail. Today's firewall products do not scan data for keywords and so can't help with your security policy in this area.

Your policy might also stipulate the keeping of records. Most firewall products have audit and log capabilities, but these vary widely in scope. The logging capabilities are closely tied to the type of filtering the firewall product supports. Some types of firewalls not as closely coupled are better at producing alarms and creating summary reports of logs.

Firewall Types

Three technologies are used in firewall products today for access control: packet filters, circuit gateways and application gateways. Each has advantages and disadvantages, and they may be combined into hybrid products.

Packet filters, the most venerable of these technologies, are used in routers and some other products. They take their name from their ability to examine *TCP/IP headers*, the data structures that begin every packet sent across the Internet. Packet filters can operate by examining source and destination Internet addresses, permitting you to selectively allow or deny packets to or from selected hosts or networks. For incoming traffic, people occasionally ask for a list of "evil" Internet sites where hackers lurk, so they can block them out. There isn't such a list (hackers most often use other people's sites for launching attacks), and blocking traffic on the basis of network source address has limited uses. But filtering on addresses is useful for blocking IP source-address spoofing attacks, which have become common.

Packet filters can also examine the transport layer header for the source and destination port address. The *port address* determines which application has sent or will receive the packet, and Internet servers have assigned port addresses. Filtering on the port address allows you to permit or deny access based on the service requested. But remote users can send packets from any port, which permits masquerading as an approved service. And rogue servers can be set up internally by insiders or by software that includes a hidden payload.

The advantage of packet filtering solutions is their flexibility. You can create access control rules to support almost any application. But there are also many downsides. Some applications—for example, FTP—are difficult to filter because of their design. The access control rules can quickly become complex, difficult to manage and nearly impossible to test for correctness. According to Brent Chapman, author, with Elizabeth Zwicky, of *Building Internet Firewalls* (O'Reilly & Associates, 1995), you can test access control lists to see if they support the services you require, but you cannot test them for all combinations.

Logging on routers is usually inadequate, because routers do not keep track of connections and log only blocked packets. Routers log all successfully blocked attacks but are silent about successful attacks (in which the packets were permitted to pass through).

Some vendors' packet filtering solutions, such as that of Checkpoint Technologies, have added an easy-to-use administration interface, along with improved filtering capabilities. Checkpoint describes its design as "stateful inspection," because the product keeps track of the immediate past activity and can provide—through packets based on the recorded past—an improvement over most other packet filters. Sun's Sunscreen includes a form of stateful inspection in a hybrid product. These products also include complete logging and alarm capabilities not found in router-based packet filters.

Fred Avolio, vice president for Trusted Information Systems (TIS) of Rockville, MD, which sells the Gauntlet firewall, points out another disadvantage of packet filters. "Think of a packet filter as a drawbridge in a castle wall. While you can raise the drawbridge, if someone cuts the ropes holding up the drawbridge, it falls down in the *open* position," says Avolio. Obviously, most people would prefer a security solution whose failure mode is in the closed position. If the access control rules on a router are deleted or deac-

Using Encryption Today

Encryption offers the ability to protect data and authenticate Internet traffic. Encrypted data cannot be disclosed or modified without the appropriate key, and messages can be digitally signed to provide authenticity.

The science of cryptology is an arcane and complex art, best left to experts. Within the last year, we have seen Netscape stumble when it used a predictable random-number generator for creating keys. More recently, Kerberos version 4 was found to have a similar problem; session keys could be guessed by using about two minutes of compute time.

You can successfully leverage encryption today by using firewall products that support it. The way firewall encryption generally works is that you configure the firewall to recognize addresses of other firewalls that support similar encryption. You probably will have to provide keys for each of the remote sites you want to use encryption with, which makes today's interfaces clunky and unmanageable for large networks; using symmetric keys means you will need (n-1) factorial keys to support n sites.

Among the firewall vendors including encryption today are Checkpoint, Raptor, Sun, TIS and V-One. Other vendors sell encryption as an option, and many router vendors, including Cisco, Digital, Livingston Enterprises, Morning Star Technologies and Network Systems, also can provide encrypting tunnels.

When choosing a vendor that offers encryption capabilities, look for support of standards. While there are only proposals for automatic key exchange mechanisms today, there are standard algorithms for encryption, including DES, DES3, IDEA, RC2 and RC4. Avoid proprietary encryption algorithms, which will permit you to talk to only the same vendor's products. What's more, proprietary algorithms haven't stood the test of public perusal and may have undiscovered failings.

tivated, the failure mode leaves the gate to your enterprise wide open. Failure mode is an important consideration in any security mechanism.

Also popular are *circuit gateways*: applications that run on a computer, typically a Unix system, and relay packets from one network to another. Circuit gateways use access control rules to determine which host may use the gateway and can log information about the host name, identity of the user, number of bytes transferred, time and remote host. The most popular circuit gateway, a public domain product named SOCKS, is a flexible solution. Some popular applications, like Netscape's Internet browser, come SOCKS-ready. But its major disadvantage is that each client application must be modified to use the SOCKS server. Another disadvantage to SOCKS is that the server can provide only coarse-grained logging. Circuit gateways do not understand the applications they support, so they can't log the names of files transferred using FTP or prevent users from sending files.

You Can See Through It

Circuit gateways and packet filters are, by their nature, transparent. End users don't know the firewall is there—unless they attempt to use a forbidden service, in which case the attempt silently fails. One disadvantage of total transparency is that such products cannot authenticate users. Some transparent solutions attempt to identify users with a protocol known as *identd* or *authd*. The identity daemon can report the user name related to a particular network connection. But the *identd* specification (RFC 931) permits always replying with the name "unknown" and also is easy to spoof (a single line in a Unix configuration file will accomplish this).

Application gateways are considered the most secure firewall technology. They recognize the contents of each packet and can provide fine-grained control and logging of each application. For example, each request to download a file from an FTP server or a Web page can be logged, and requests to send files with FTP can be blocked. If malicious software attempts to "tunnel" through the firewall by using an acceptable application's port address, the gateway software won't recognize the malicious application as valid and will refuse to pass the packet. For example, a packet filter or circuit gateway might permit any packet destined for port 53, the Domain Name Server (DNS) address, but a DNS application gateway will pass only valid DNS requests or responses.

The main disadvantage of application gateways is the lack of flexibility. There must be an application gateway for every Internet service your require. If you have custom TCP/IP applications, you'll need custom application gateways for them. Some vendors, such as TIS, make this relatively easy by providing source code with their products, while others provide a loophole—packet filters or circuit gateways in hybrid configurations which can pass any service, with some additional risk. These include ANS, Blackhole, Checkpoint, Digital, IBM and Sunscreen.

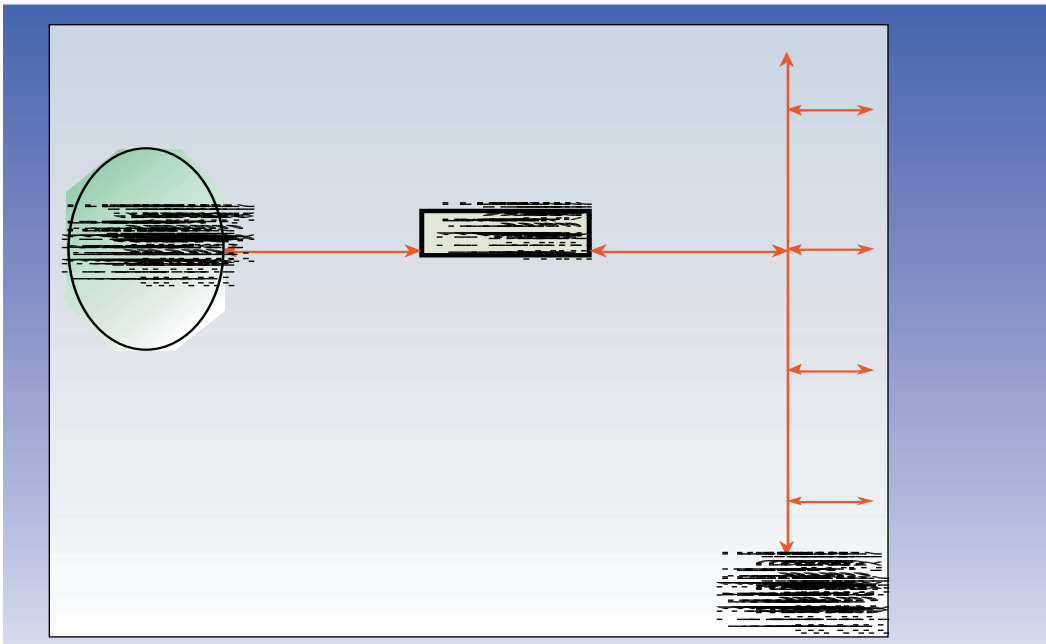
Some people consider the lack of flexibility in a positive light. You can't accidentally enable dangerous services if no application gateway exists to support those services. Also, the failure mode of the application gateway is desirable. "It's like a portcullis in a castle wall; it's failure mode is that it drops closed," says Avolio. If the application gateway shuts down, no traffic passes through.

Amateurs Beware

Firewall products vary in the amount of installation assistance included with them. Some require vendor installation (such as from Sun, TIS and V-One), while others offer it as an option ranging upward from $1,000. Training also is optional with most products, although those requiring on-site installation always include some training in the package.

Firewall configuration is not for the uninitiated; it can be complicated. Some vendors provide hopefully foolproof administrative interfaces which help you do the right thing, although at the expense of some flexibility. For example, Borderware from Border Network Technologies of Toronto completely hides the underlying Unix system but always requires strong authentication for certain incoming services. Borderware has implemented a security policy in its design, which you cannot override by mistake or on purpose. Conversely, the interface to Checkpoint's Firewall-1 lets you do whatever you want, including permitting dangerous services—delivering flexibility at the price of a less foolproof built-in policy.

You can even build your own firewall out of freely available components. The Firewall Toolkit (ftp.tis.com), Freestone (ftp.sos.com) and SOCKS (ftp.nec.com) contain most of the necessary components but none of the know-how. The risks here are many. I once was asked to check on a firewall that had been installed by a local Internet service provider (ISP). The consultants had used the Firewall Toolkit running on an unmodified Unix system. The toolkit itself was correctly configured, but the system it was installed on had



Packet filtering solutions, such as routers, provide the most flexibility as a firewall, but they have innate weaknesses. In this example, the router permits some traffic to all hosts in the trusted network, exposing all hosts to possible attacks. Also, the failure mode of packet filtering solutions is poor— if the packet filtering software is disabled, the trusted network is left open to attack.

login accounts with simple passwords and other security problems. You could log in directly to this firewall by guessing a simple account name and password, and then have unfettered access to the internal network. Unless your organization has access to people experienced in network programming and security, it's wise to leave firewall building to pros.

Some clients wonder about having their ISP provide security. Unless the ISP sells security services, this is rather like asking the fox to guard the henhouse. Some service providers, such as ANS and BBN Planet, include firewalls in their service offerings. These are full-featured firewalls, not do-it-yourself kits added to provide an illusion of security. If your ISP is competent and trustworthy, you might consider contracting with it for security.

Control Panels

Administration is a key firewall component. Some firewall products (although few any more) require you to edit files using the Unix *vi* editor. Most provide some degree of ease of use. Regardless of the simplicity of the control panel, you should also look for secure, remote administration.

Most large sites situate their firewalls where their Internet connection enters the facility—a logical choice. But if the firewall doesn't support secure, remote administration, you may find yourself trooping down to a wiring closet or the machine room in the basement more often than you'd like. While the configuration of the firewall is unlikely to change often once configured, other things require frequent tending. For example, depending on the type of authentication you have chosen, you may have to administer the authentication system.

Look for products that use either an encrypted link or strong authentication before committing changes. Just last summer, a popular product was compromised because it permitted remote administration via Telnet (not encrypted) on an unusual port address. Port scanners are common in hacking (and security) software toolkits, and finding the unusual port takes less than a minute. The second part of the attack consisted of software that monitored traffic to that port and captured the password being used. The vendor has remedied this problem, but not all products have strong solutions.

You will also want to routinely monitor logs. A unmonitored firewall is like a castle gate without guards. If attackers are given time, it is more likely they can break down the castle gate or, in this case, find a vulnerability you may have left when configuring the system. Vendors do not offer guarantees that their products will never be penetrated. You must pay attention to logs and watch for unusual activity. Some products feature a powerful array of reducing scripts for logs. Interlock from ANS of Reston, VA, can produce usage summaries detailed enough for charging internal users for the Internet connection. TIS' Gauntlet focuses upon picking out exceptions—extraordinary conditions in log files.

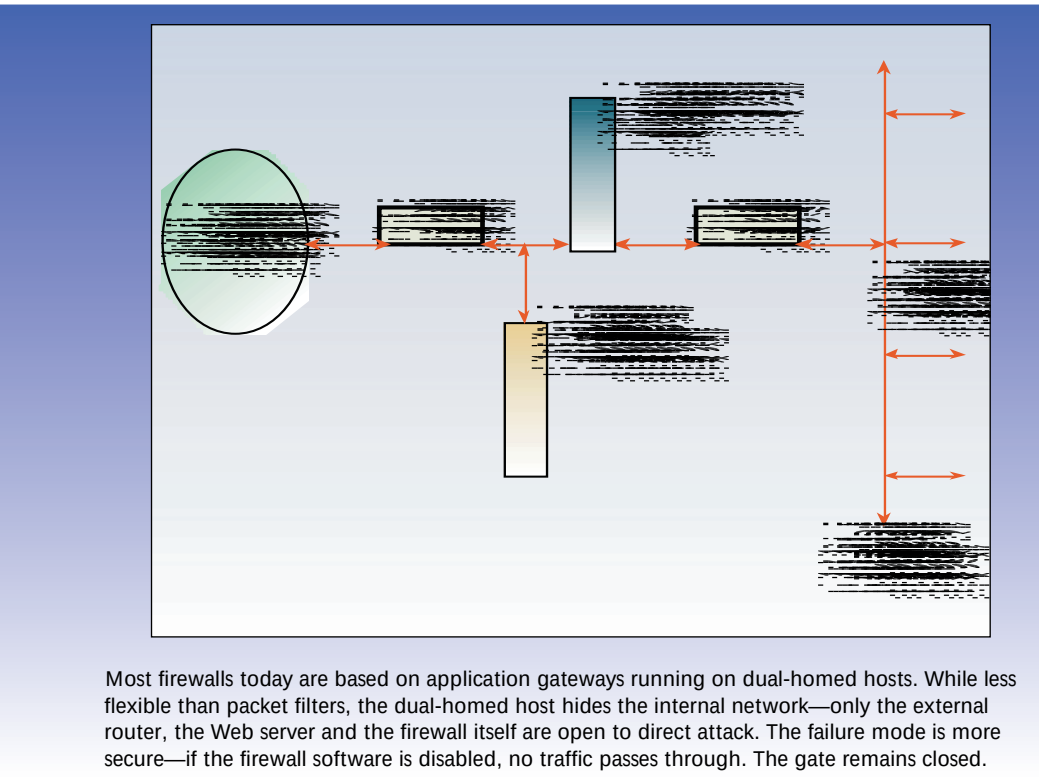
You don't want alarms going off in a wiring closet either. Most firewall products support alarm capabilities, including the ability to set thresholds and time-of-day behaviors, and even dial pagers through modems. ANS, Checkpoint, Digital, Harris, IBM, Raptor, Secure Computing and TIS are among the vendors who support pager activation. Flexible alarm capabilities are a must for firewall products. This is another area where router-based packet filters are weak, in that they require a separate host and custom software to generate alarms.

The Future

Firewalls don't appear to have all the power, flexibility and control of starship force fields and shields. But in the short run, they are an essential component of an Internet connection for any business. Firewalls are also appropriate for intranets, for example, for separating accounting and financing from the development group or filtering traffic from a recently merged competitor's network.

The future of Internet security, however, will be based upon encryption and strong authentication. The next version of TCP/IP (IPv6) includes support for encrypting data and authenticating headers at the Internet level, making these operations totally transparent to applications. Today, many firewall vendors include support for encryption with their products, as noted in the accompanying sidebar.

The firewall marketplace is as ripe with hype as anything else surrounding the Internet. While the Internet has become as essential to doing business as telephones, maintaining effective controls requires the right firewall. Shop carefully for the perfect shield for your organization, and you'll avoid sneak attacks from the hackers, Klingons and Cardassians who lurk in the great abyss. IT



Most firewalls today are based on application gateways running on dual-homed hosts. While less flexible than packet filters, the dual-homed host hides the internal network—only the external router, the Web server and the firewall itself are open to direct attack. The failure mode is more secure—if the firewall software is disabled, no traffic passes through. The gate remains closed.

Rik Farrow *consults, teaches and writes about Unix and Internet security while living in the high desert. He can be reached at rik@spirit.com.*