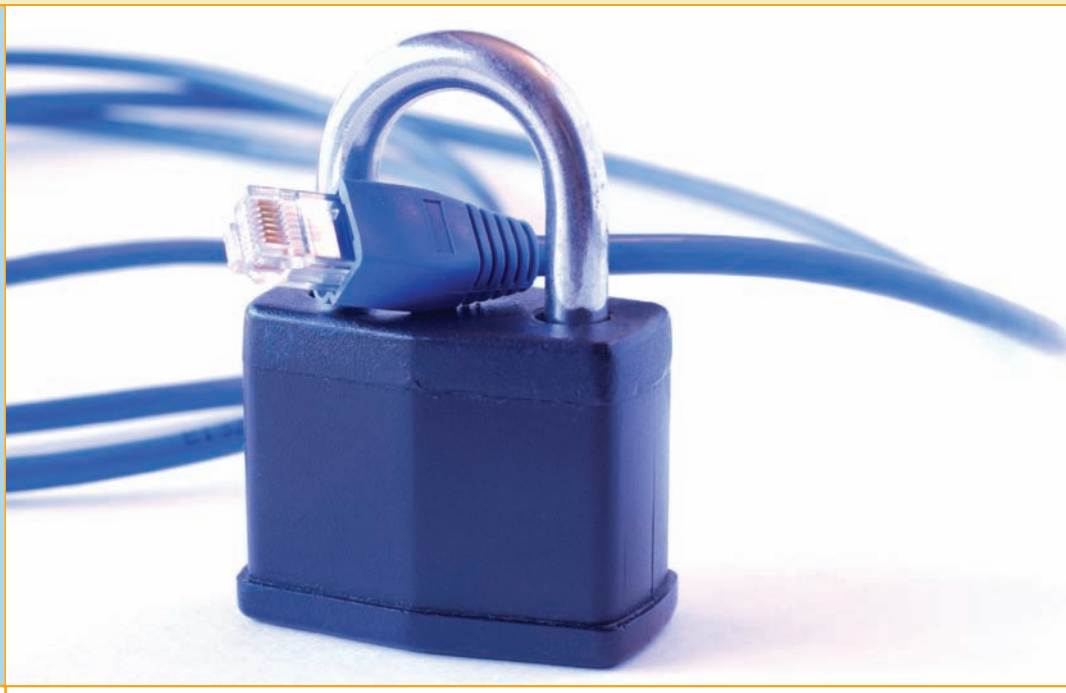
chapter 17

Protecting Your Network

"The superior man, when resting in safety, does not forget that danger may come."

—Confucius



In this chapter, you will learn how to

- **Discuss the common security threats in network computing**
- **Describe methods for securing user accounts**
- **Explain how firewalls, NAT, port filtering, and packet filtering protect a network from threats**

The very nature of networking makes networks vulnerable to a dizzying array of threats. By definition, a network must allow multiple users to access serving systems, but at the same time we must protect the network from harm. Who are the people creating this threat?

The news may be full of tales about **hackers** and other malicious people with nothing better to do than lurk around the Internet and trash the peace-loving systems of good folks like us, but in reality hackers are only one of many serious network threats. You will learn how to protect your networks from hackers, but first I want you to appreciate that the average network faces plenty more threats from the folks who are authorized to use it than those who are not authorized. Users with good intentions are far more likely to cause you trouble than any hacker. Additionally, don't think all network threats are people. Let's not forget natural disasters like floods and hurricanes. Even third parties can unintentionally wreak havoc—what will you do if your building suddenly lacks electricity? So a **network threat** can be any number of things that share one essential feature: the potential to damage network data, machines, or users. The first order of business, therefore, is to stop and think about the types of threats that face the average network. As we define the threats, we can discuss the many tools and methods used to protect our precious networks from intentional harm.

Be aware that in some circles, the term "hacker" describes folks who love the challenge of overcoming obstacles and perceived limitations—and that's a positive thing! At least for this chapter we will define a hacker as an unauthorized person who is intentionally trying to access resources on your network.

Test Specific

Common Threats

The threats to your network are real and widespread. Here's a list of some of the more common potential threats to your network. The sections that follow give details on those threats and explain how to deal with them.

- System crashes and other hardware failures
- Administrative access control weaknesses
- Malware, such as viruses and worms
- Social engineering
- Denial of Service attacks
- Physical intrusion
- Rogue access points

System Crash/Hardware Failure

Like any technology, computers can and will fail—usually when you can least afford for it to happen. Hard drives crash, servers lock up, the power fails—it's all part of the joy of working in the networking business. We need to create redundancy in areas prone to failure (like installing backup power in case of electrical failure) and performing those all-important data backups. Beyond that, the idea is to deploy redundant hardware to provide **fault tolerance**. Take advantage of technologies like RAID (Redundant Array of Inexpensive Disks) to spread data across multiple drives. Buy a server case with multiple power supplies or add a second NIC.

See Chapter 18, "Network Management," for more information on RAID.

The CompTIA Network+ exam does not test you on the details of file system access controls. In other words, don't bother memorizing details like NTFS permissions, but do appreciate that you have fine-grained controls available.

Administering your super accounts is only part of what's called *user account control*. See "Controlling User Accounts" later in this chapter for more details.

Administrative Access Control

All operating systems and many TCP applications come with some form of access control list (ACL) that defines what users can do with the server's shared resources. An access control might be a file server giving a user read-only privileges to a particular folder, or an FTP server only allowing certain logins to use certain folders. Every operating system—and many Internet applications—are packed with administrative tools and functionality. We need these tools to get all kinds of work done, but by the same token we need to work hard to keep these capabilities out of the reach of those who don't need them.

Make sure you know the "super" accounts native to Windows (administrator) and Linux and Macintosh OS X (root). You must carefully control these accounts. Clearly, giving regular users administrator/root access is a bad idea, but far more subtle problems can arise. I once gave a user Manage Documents permission for a busy laser printer in a Windows network. She quickly realized she could pause other users' print jobs and send her print jobs to the beginning of the print queue—nice for her but not so nice for her co-workers. Protecting administrative programs and functions from access and abuse by users is a real challenge, and one that requires an extensive knowledge of the operating system and of users' motivations.

Malware

The term **malware** defines any program or code (macro, script, and so on) that's designed to do something on a system or network that you don't want to have happen. Malware comes in quite a variety of guises, such as viruses, worms, macros, Trojans, rootkits, and adware and spyware. Let's examine all these malware flavors and then finish with how to deal with them.

Virus

A **virus** is a program that has two jobs: to replicate and to activate. *Replication* means it makes copies of itself, often as code stored in boot sectors or as extra code added to the end of executable programs. *Activation* is when a virus does something like erase the boot sector of a drive. A virus only replicates to other drives, such as thumb drives or optical media. It does not replicate across networks.

Worm

A **worm** is identical in function to a virus except that it replicates exclusively through networks. A worm, unlike a virus, doesn't have to wait for someone to use a removable drive to replicate. If the infected computer is on a network, a worm will immediately start sending copies of itself to any other computers on the network it can locate.

Macro

A **macro** is any type of virus that exploits application macros to replicate and activate. Macros exist in any application that has a built-in macro language, such as Microsoft Excel, that users can program to handle repetitive tasks (among other things).

Trojan

A **Trojan** is a piece of malware that looks or pretends to do one thing while at the same time doing something evil. The more "popular" Trojans turn an infected computer into a server and then open TCP/IP ports so that a remote user can control the infected computer. They can be used to capture keystrokes, passwords, files, credit card information, and more. This type of Trojan is called a *remote administration tool* (*RAT*), though you don't need to know that for the CompTIA Network+ exam. Trojans do not replicate.

Rootkit

For a virus or Trojan to succeed it needs to come up with some method to hide itself. As awareness of malware has grown, anti-malware programs make it harder to find new locations on a computer to hide. A **rootkit** is a Trojan that takes advantage of very low-level operating system functions to hide itself from all but the most aggressive of anti-malware tools.

The most infamous rootkit appeared a few years ago as an antipiracy attempt by Sony on its music CDs. Unfortunately for the media giant, the rootkit software installed when you played a music CD and opened a backdoor to an infected computer that could be used for malicious intent.

Adware/Spyware

There are two types of programs that are similar to malware in that they try to hide themselves to an extant. **Adware** is a program that monitors the types of Web site you frequent and uses that information to generate targeted advertisements, usually pop-up windows. Adware isn't by definition evil, but many adware makers use sneaky methods to get you to use adware, such as using deceptive-looking Web pages ("Your computer is infected with a virus—click here to scan NOW!"). As a result, adware is often considered malware.

Spyware is a function of any program that sends information about your system or your actions over the Internet. The type of information sent depends on the program. An adware program will include your browsing history. A more aggressive malware may send keystrokes or all of the contacts in your e-mail.

Dealing with Malware

We deal with malware in three ways: anti-malware programs, training, and procedures. At the very least, every computer should run an anti-malware program. If possible, add an appliance that runs anti-malware programs against incoming data from your network. Many such appliances exist but they are most common in proxy servers. Also remember that an anti-malware program is only as good as its updates—keep everyone's definition file up to date! Users must be trained to look for suspicious code and understand that they must not run these programs. Last, your organization should have procedures in place so that everyone knows what to do if they encounter malware.

One of the most important malware mitigation procedures is to keep systems under your control patched and up to date. Microsoft does a very good job putting out bug fixes and patches as soon as problems occur. If your systems aren't set up to update automatically, then schedule manual updates regularly.

Try This!

Scoring Excellent Anti-Malware Programs

You can download many excellent anti-malware programs for free, either for extended trial periods or for indefinite use. Since you need these programs to keep your systems happy, try this! Download one or more anti-malware programs, such as the following:

- **Lavasoft Ad-Aware (www.lavasoft.com)** Ad-Aware is an excellent anti-spyware program. Ad-Aware will root out all sorts of files and programs that can cause your computer to run slowly (or worse).
- **Spybot Search&Destroy (www.safer-networking.org)** Spybot Search&Destroy from Safer Networking Ltd. is another superb anti-spyware program. Many folks use both Ad-Aware and Spybot—though sometimes the two programs detect each other as spyware!
- **AVG Anti-Virus (http://free.avg.com)** AVG offers a free version of their anti-virus software for non-commercial use. Updated regularly to add the latest virus signatures, the software will keep your system clean and bug free.

Social Engineering

The vast majority of attacks against your network come under the heading of **social engineering**—the process of using or manipulating people inside the networking environment to gain access to that network from the outside. The term "social engineering" covers the many ways humans can use other humans to gain unauthorized information. This unauthorized information may be a network login, a credit card number, company customer data—almost anything you might imagine that one person or organization may not want a person outside of that organization to access.

It's common for these attacks to be used together, so if you discover one of them being used against your organization, it's a good idea to look for others.

Social engineering attacks aren't hacking—at least in the classic sense of the word—although the goals are the same. Social engineering is where people attack an organization through the people in the organization or physically access the organization to get the information they need.

The most classic form of social engineering is the telephone scam where someone calls a person and tries to get them to give them a user name/password combination. On the same vein, someone may physically enter your building under the guise of someone who might have legitimate reason for being there, such as cleaning personnel, repair technicians, or messengers. They then snoop around desks, looking for whatever they've come to find (one of many good reasons not to put passwords on your desk or monitor). They might talk with people inside the organization, gathering names, office numbers, or department names—little things in and of themselves, but powerful tools when combined later with other social engineering attacks.

These old-school social engineering tactics are taking a backseat to a far more nefarious form of social engineering: phishing.

Phishing

In a **phishing** attack, the attacker poses as some sort of trusted site, like an online version of your bank or credit card company, and solicits you to update your financial information, such as a credit card number. You might get an e-mail message, for example, that purports to be from PayPal telling you that your account needs to be updated and provides a link that looks like it goes to http://billing.paypal.com. Clicking the link http://billing.paypall.com (note the extra "l" in the name), you might end up at a site that resembles the PayPal billing site, but is actually http://www.merchntaccount.com, a phishing site.

Denial of Service

Denial of Service (DoS) attacks are the work of hackers whose only interest is in bringing a network to its knees. This is accomplished by flooding the network with so many requests that it becomes overwhelmed and ceases functioning. These attacks are most commonly performed on Web and e-mail servers, but virtually any part of a network can be attacked via some DoS method.

The secret to a successful DoS attack is to send as many packets as possible against the victim. Not only do you want to send a lot of packets, you want the packets to contain some kind of request that the victim must process as long as possible to force the victim to deal with each attacking packet for as long as possible. There's a number of ways to get a good DoS going, but the CompTIA Network+ objectives expressly mention a **smurf** attack. A smurf attack is a form of DoS that sends broadcast PINGs to the victim. Not only that, the source IP of the PINGs is changed from the real system sending the packet to another (often, nonexistent) machine. Smurf attacks are no longer a menace because almost all network devices now know not to forward broadcast PINGs.

A smurf attack is a form of DoS that sends broadcast PINGs to the victim.

Far more menacing than a simple DoS attack are **Distributed Denial of Service (DDoS) attacks**. A DDoS uses multiple (as in hundreds up to hundreds of thousands) of computers under the control of a single operator to send a devastating attack. DDoS operators don't own these computers, but instead use malware to take control of computers. A single computer under the control of an operator is called a **zombie**. A group of computers under the control of one operator is called a **botnet**.

Zombified computers aren't obvious. DDoS operators often wait weeks or months after a computer's been infected to take control of it.

To take control of your network's computers, someone has to install malware on the computer. Again, anti-malware, training, and procedures will keep you safe from zombification (but feel free to make some joke about eating human brains).

Physical Intrusion

You can't consider a network secure unless you provide some physical protection to your network. I separate physical protection into two different areas: protection of servers and protection of clients.

Server protection is easy. Lock up your servers to prevent physical access by any unauthorized person. Large organizations have special server rooms, complete with card-key locks and tracking of anyone who enters or

Tech Tip

Lock Them Down

A Windows PC should be locked down when not actively used. The simple thing to teach your users to do is to press the WINDOWS KEY-L *combination when they get up from their desks. The effects from the key combination vary according to both the version of Windows and whether a system is a member of a workgroup or domain, but all will require the user to log in to access his or her account (assuming the account is password protected in the first place, of course!).*

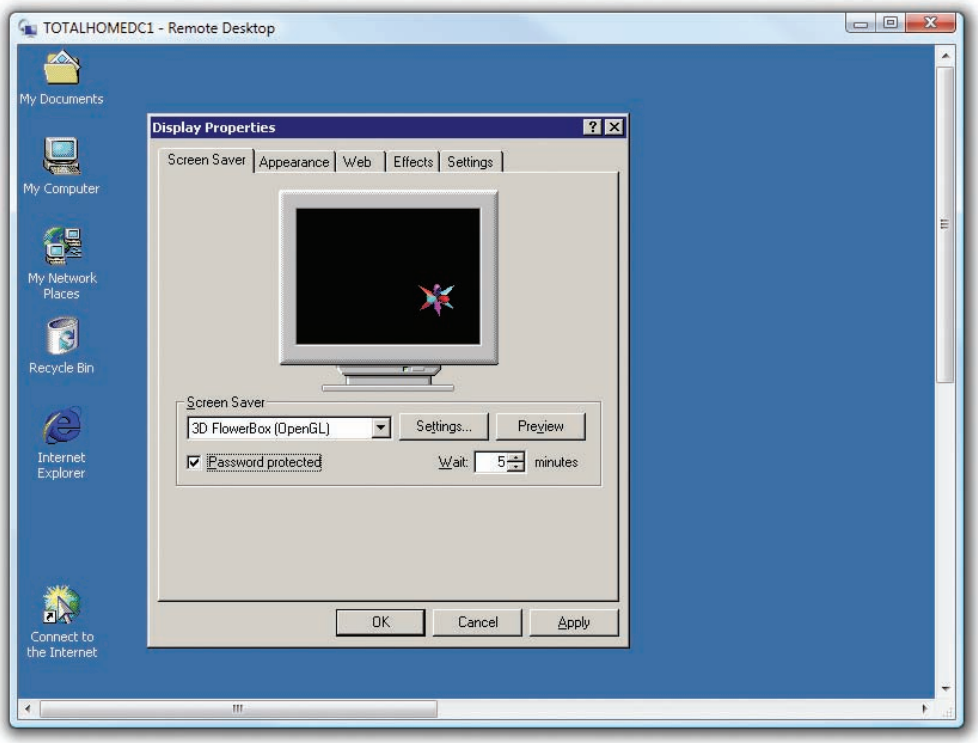
exits. Smaller organizations will at least have a locked closet. While you're locking up your servers, don't forget about any network switches! Hackers can access networks by plugging into a switch, so don't leave any switches available to them.

Physical server protection doesn't stop with a locked door. One of the most common mistakes made by techs is walking away from a server while still logged in. Always log off your server when it's not in use! As a backup, add a password-protected screensaver (Figure 17.1).

It's difficult to lock up all of your client systems, but you should have your users performing some physical security. First, all users should use screensaver passwords. Hackers will take advantage of unattended systems to get access to networks. Second, make users aware of the potential for dumpster diving and make paper shredders available. Last, tell users to mind their work areas. It's amazing how many users leave passwords available. I can go into any office, open a few desk drawers, and will invariably find little yellow sticky notes with user names and passwords. If users must write down passwords, tell them to put them in locked drawers!

Rogue Access Points

A **rogue access point** is an unauthorized wireless access point (WAP) installed in a computer network. Rogue access points are a huge problem today. It's easy to purchase an inexpensive WAP and just plug it into a network. To make the issue even worse, almost all WAPs are designed to



• **Figure 17.1** Applying a password-protected screensaver

work using the preinstalled configuration, giving bad guys easy access to your network from a location physically outside your network.

The biggest reason rogue access points exist is that members of an organization install them for convenience. Users like their own wireless networks and, due to lack of training, don't appreciate the danger they pose. Bad guys getting into your physical location and installing rogue access points is less common.

Locating rogue access points is a challenge, especially if the person installing the rogue access point is clever enough to turn off SSID broadcasting. There are wireless sniffing programs designed to find any wireless network but they must be run often.

Securing User Accounts

Even the smallest network will have a number of user accounts and groups scattered about with different levels of permissions. Every time you give a user access to a resource, you create potential loopholes that can leave your network vulnerable to unauthorized accesses, data destruction, and other administrative nightmares. We can categorize all of these potential dangers as **internal threats**. To protect your network from these threats, you need to implement the right controls over passwords, user accounts, permissions, and policies. Let's start with probably the most abused of all these areas: passwords.

Passwords

Passwords are the ultimate key to protecting your network. Anyone with access to a user account with a valid password will get into any system. Even if the user account only has limited permissions, you still have a security breach. Remember: for a hacker, just getting into the system is half the battle.

Protect your passwords. Never give out passwords over the phone. If a user loses a password, an administrator should reset the password to a complex combination of letters and numbers, and then allow the user to change the password to something they want. All of the stronger network operating systems have this capability. Windows Server, for example, provides a setting called **User must change password at next logon**, as shown in Figure 17.2.

Make your users choose good passwords. I once attended a network security seminar, and the speaker had everyone stand up. She then began to ask questions about our passwords—if we responded positively to the question we were to sit down. She began to ask questions like "Do you use the name of your spouse as a password?" and "Do you use your pet's name?"

By the time she was done asking about 15 questions, only 6 people out of some 300 were still standing! The reality is that most of us choose passwords that are amazingly easy to hack. Make sure you use strong passwords: at least eight characters in

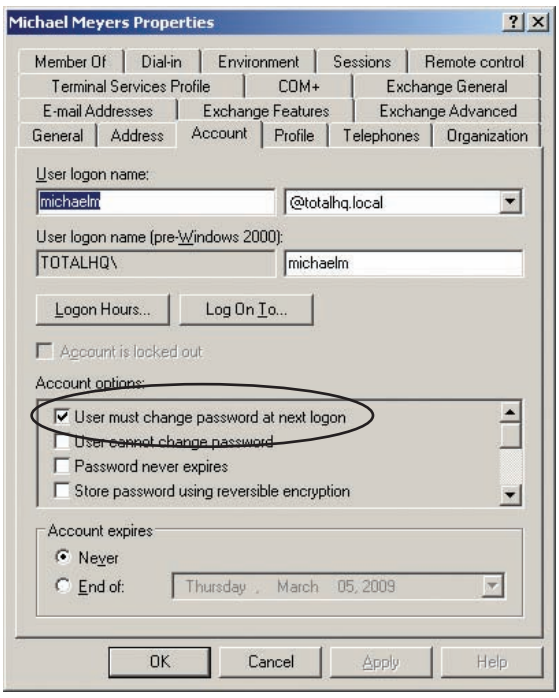


Figure 17.2 Windows Server option for requiring a user to change a password

Tech Tip

More Than Letters and Numbers

Using nonalphanumeric characters makes any password much more difficult to crack, for two reasons. First, adding nonalphanumeric characters forces the hacker to consider many more possible characters than just letters and numbers. Second, most password crackers use combinations of common words and numbers to try to hack a password. Because nonalphanumeric characters don't fit into common words or numbers, including a character such as an exclamation point will defeat these common-word hacks. Not all serving systems let you use characters such as @, $, %, or \, however, so you need to experiment to see if a particular server will accept them.

length (more than eight characters is better), including letters, numbers, and punctuation symbols.

Once you've forced your users to choose strong passwords, you should make them change passwords at regular intervals. While this concept sounds good on paper, and for the CompTIA Network+ exam you should remember that regular password changing is a good idea, in the real world it is a hard policy to maintain. For starters, users tend to forget passwords when they change a lot. One way to remember passwords if your organization forces you to change them is to use a numbering system. I worked at a company that required me to change my password at the beginning of each month, so I did something simple. I took a root password—let's say it was "m3y3rs5"—and simply added a number to the end representing the current month. So when June rolled around, for example, I would change my password to "m3y3rs56." It worked pretty well!

No matter how well your password implementation goes, using passwords always creates administrative problems. First, users forget passwords and someone (usually you) has to access their account and reset their passwords. Second, users will write passwords down, giving hackers an easy way into the network if those bits of paper fall into the wrong hands. If you've got the cash, there are two alternatives to passwords: smart devices and biometrics.

Smart devices are credit cards, USB keys, or other small devices that you insert into your PC in lieu of entering a password. They work extremely well and are incredibly difficult to bypass. The downside is that they might be lost or stolen.

If you want to go seriously space-age, then biometrics are the way to go. **Biometric devices** scan fingerprints, retinas, or even the sound of the user's voice to provide a fool-proof replacement for both passwords and smart devices. Biometrics have been around for quite a while, but were relegated to extremely high-security networks due to their high cost (thousand of dollars per device). That price has dropped substantially, making biometrics worthy of consideration for some networks.

Try This!

Authentication Factors

You can categorize ways to authenticate into three broad areas: ownership factors, knowledge factors, and inherent factors. An ownership factor is something the user has, like an ID card or security token. A knowledge factor is something the user knows, like a password or personal identification number (PIN). An inherent factor is something that is part of the user, like a fingerprint or retinal pattern.

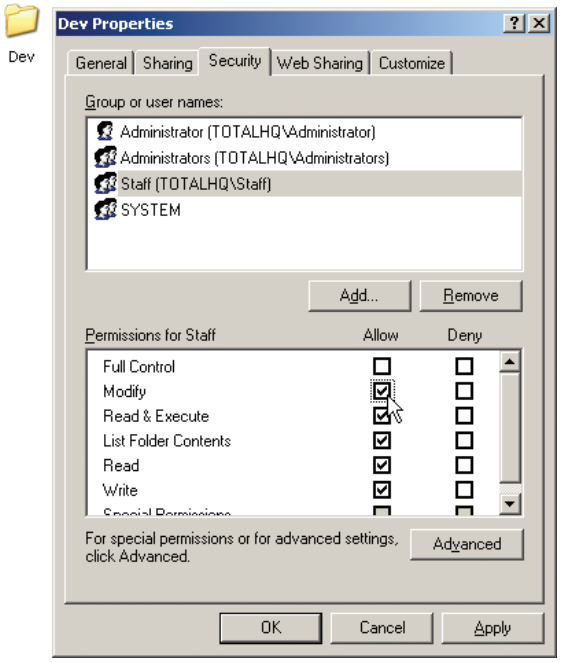
You can use one or more of these factors to authenticate a user. In fact, *two-factor authentication* is a fairly standard practice in secure facilities, like some government offices. Clearly, passwords are not the only way anymore, so try this!

Either head out to your local computer store or access one of the big ones on the Internet (like Amazon) and see what variety of authentication factors you can find. Make a list that contains at least one for each of the three authentication factors and then compare that list with lists compiled by your classmates. What would work for your network?

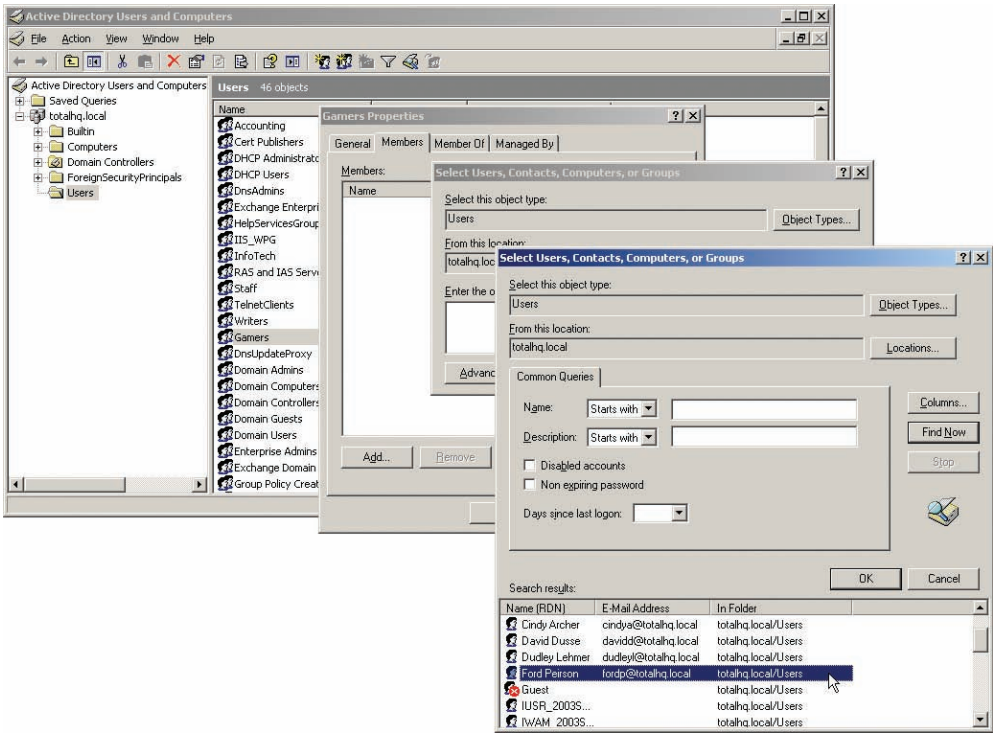
Controlling User Accounts

A user account is just information: nothing more than a combination of a user name and password. Like any important information, it's critical to control who has a user account and to track what these accounts can do. Access to user accounts should be restricted to the assigned individuals (no sharing, no stealing), and those accounts should have permission to access only the resources they need, no more. This control over what a legitimate account can do is called the *least privilege* approach to network security and is by far the most common approach used in networks.

Tight control of user accounts is critical to preventing unauthorized access. Disabling unused accounts is an important part of this strategy, but good user account control goes far deeper than that. One of your best tools for user account control is groups. Instead of giving permissions to individual user accounts, give them to groups; this makes keeping track of the permissions assigned to individual user accounts much easier. Figure 17.3 shows an example of giving permissions to a group for a folder in Windows Server. Once a group is created and its permissions set, you can then add user accounts to that group as needed. Any user account that becomes a member of a group automatically gets the permissions assigned to that group. Figure 17.4 shows an example of adding a user to a newly created group in the same Windows Server system.



• **Figure 17.3** Giving a group permissions for a folder in Windows



• **Figure 17.4** Adding a user to a newly created group

Groups are a great way to get increased complexity without increasing the administrative burden on network administrators, because all network operating systems combine permissions. When a user is a member of more than one group, which permissions does he have with respect to any particular resource? In all network operating systems, the permissions of the groups are *combined*, and the result is what we call the **effective permissions** the user has to access the resource. Let's use an example from Windows Server. If Timmy is a member of the Sales group, which has List Folder Contents permission to a folder, and he is also a member of the Managers group, which has Read and Execute permissions to the same folder, Timmy will have List Folder Contents *and* Read and Execute permissions to that folder.

Watch out for *default* user accounts and groups—they can become secret backdoors to your network! All network operating systems have a default Everyone group and it can easily be used to sneak into shared resources. This Everyone group, as its name implies, literally includes anyone who connects to that resource. Some versions of Windows give full control to the Everyone group by default. All of the default groups—Everyone, Guest, Users—define broad groups of users. Never use them unless you intend to permit all those folks to access a resource. If you use one of the default groups, remember to configure it with the proper permissions to prevent users from doing things you don't want them to do with a shared resource!

All of these groups only do one thing for you: they enable you to keep track of your user accounts. That way you know resources are only available for users who need those resources, and users only access the resources you want them to use.

Before we move on, let me add one more tool to your kit: diligence. Managing user accounts is a thankless and difficult task, but one that you must stay on top of if you want to keep your network secure. Most organizations integrate the creation, disabling/enabling, and deletion of user accounts with the work of their human resources folks. Whenever a person joins, quits, or moves, the network admin is always one of the first to know!

The administration of permissions can become incredibly complex even with judicious use of groups. You now know what happens when a user account has multiple sets of permissions to the same resource, but what happens if the user has one set of permissions to a folder, and a different set of permissions to one of its subfolders? This brings up a phenomenon called **inheritance**. We won't get into the many ways different network operating systems handle inherited permissions. Lucky for you, the CompTIA Network+ exam doesn't test you on all the nuances of combined or inherited permissions—just be aware that they exist. Those who go on to get more advanced certifications, on the other hand, must become extremely familiar with the many complex permutations of permissions.

Firewalls

I always fear the moment when technical terms move beyond the technical people and start to find use in the nontechnical world. The moment any technical term becomes part of the common vernacular, you can bet that its true meaning will become obscured, because without a technical background people are reduced to simplistic descriptions of what is invariably a

far more complex idea. I submit the term *firewall* as a perfect example of this phenomenon. Most people with some level of computer knowledge think of a firewall as some sort of thing-a-ma-bob that protects an internal network from unauthorized access to and from the Internet at large. That type of definition might work for your VP as you explain why you need to get a firewall, but as techs, we need a deeper understanding.

Firewalls protect networks from **external threats**—potential attacks from outside your network—by using a number of methods, such as hiding IP addresses using NAT, selectively blocking TCP/UDP ports, or even filtering traffic based on MAC addresses. From there, things get much more complex, so for now let's define a firewall as a device that filters IP traffic to protect networks and computers. But a firewall doesn't have to be a dedicated device. There are two very different places where you might run into a firewall. The first place is a device at the edge of your network. Given that there's already a router at the edge of your network, you'd be hard pressed to find a router today that does not also act as a firewall. Since the firewall is in a box on the network, we call these *network-based* firewalls (also called hardware firewalls). The second place is software installed on your computer that does the same job but only firewalls packets coming in and out of your system. We call these *host-based* firewalls (also called software firewalls). In a perfect world, your network has a network-based firewall at the edge of your network and all of your systems run a host-based firewall.

Hiding the IPs

The first and most common technique for protecting a network is to hide the real IP addresses of the internal network systems from the Internet. If a hacker gets a real IP address, he can then begin to probe that system, looking for vulnerabilities. If you can prevent a hacker from getting an IP address to probe, you've stopped most hacking techniques cold. You already know how to hide IP addresses using **Network Address Translation (NAT)**. That's why most routers have built-in NAT capability. Not only does NAT reduce the need for true IANA-supplied public IP addresses, but it also does a great job protecting networks from hackers, because it is difficult to access a network using private IP addresses hidden behind a NAT-enabled router.

Many sources challenge the idea that NAT is a firewall feature. Granted, NAT wasn't originally designed to act as a firewall, but it sure does protect your network.

Cross Check

NATs Away!

You learned about the many flavors of NAT way back in Chapter 8, "The Wonderful World of Routing," so check your memory. How does overloaded NAT work? What's another name for Port Address Translation (PAT)? What are some of the names represented by the acronym SNAT and how do those technologies work?

Port Filtering

The second most common firewall tool is **port filtering**, also called **port blocking**. Hackers often try less commonly used port numbers to get into a network. Port filtering simply means preventing the passage of any TCP or UDP packets through any ports other than the ones prescribed by the system administrator. Port filtering is effective, but it requires some serious

configuration to work properly. The question is always, "Which ports do I allow into the network?"

When you open your browser and access a Web page, your Web browser sends out packets to the Web server with the destination port of 80. Web servers require this and it's how TCP/IP works.

No one has problems with the well-known ports like 80 (HTTP), 20/21 (FTP), 25 (SMTP), and 110 (POP3), but there are a large number of lesser-known ports that networks often want opened.

I recently installed port filtering on my personal firewall and everything worked great—until I decided to play the popular game World of Warcraft on the Internet. (Note to WoW nerds: Blackwater Raiders server, I'm "Pelape" or "Pelope.") I simply could not connect to the Internet servers, until I discovered that World of Warcraft requires TCP port 3724 open to work over the Internet. After reconfiguring my port filter (I reopened port 3724) I was able to play WoW, but when I tried to help one of my friends using Microsoft Remote Desktop, I couldn't access his system! Want to guess where the problem lay? Yup, I needed to open port 3389. How did I figure these out? I didn't know which ports to open, but I suspected that my problem was in the port arena so I fired up my Web browser (thank goodness that worked!) and went to the World of Warcraft and Microsoft Web sites, which told me which ports I needed to open. This constant opening and closing of ports is one of the prices you pay for the protection of port filtering, but it sure stops hackers if they can't use strange ports to gain access.

Most routers that provide port blocking manifest it in one of two ways. The first way is to have port filtering close *all* ports until you open them explicitly. The other port filtering method is to leave all ports open unless you explicitly close them. The gotcha here is that most types of IP sessions require *dynamic port* usage. For example, when my system makes a query for a Web page on HTTP port 80, the Web server and my system establish a session using a *different* port to send the Web pages to my system. Figure 17.5 shows the results of running `netstat -n` switch while I have a number of Web pages open—note the TCP ports used for the incoming Web pages (the Local Address column). Dynamic ports can cause some problems for older (much older) port filtering systems, but almost all of today's port filtering systems are aware of this issue and handle it automatically.

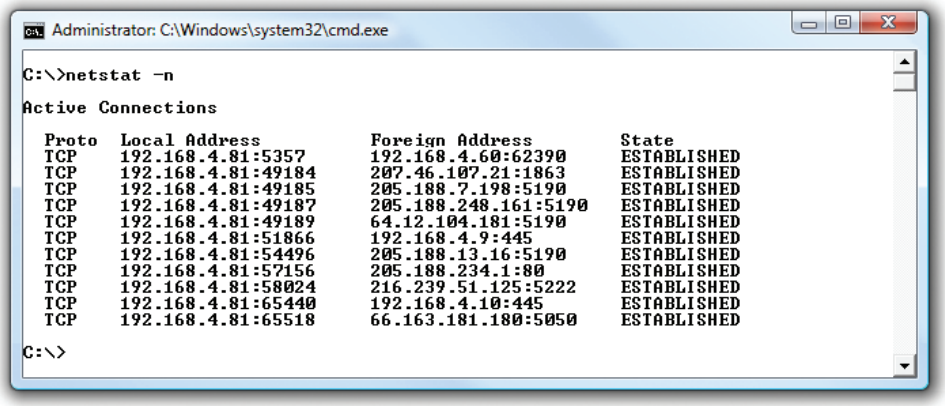
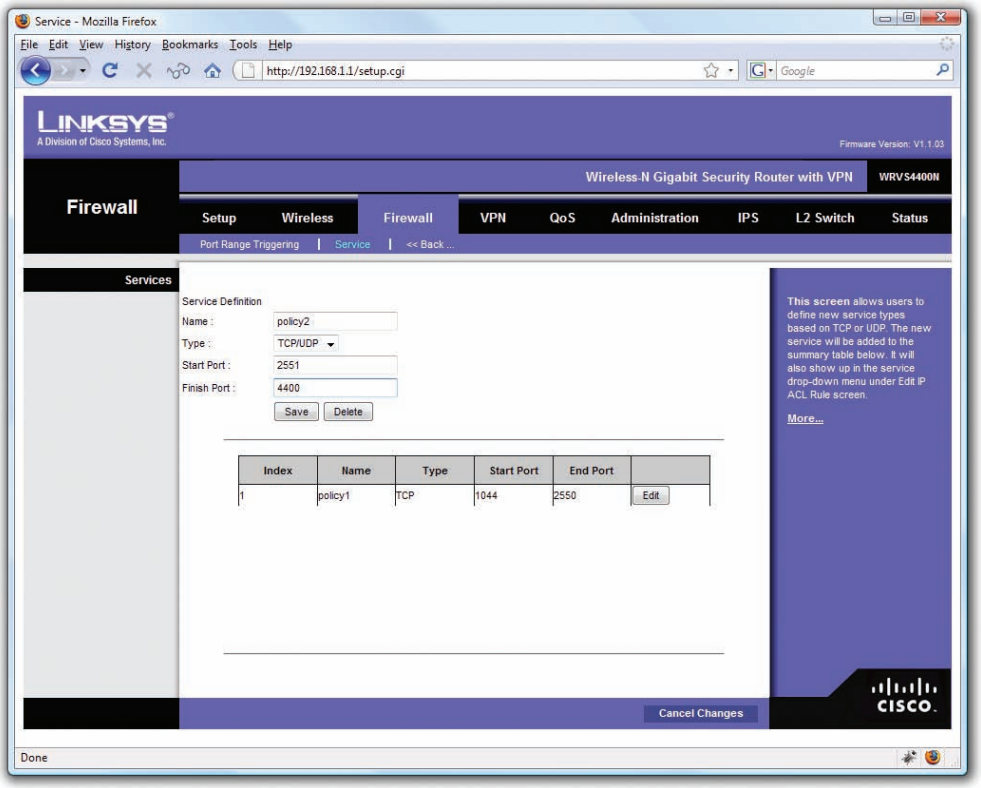


Figure 17.5 The `netstat -n` command showing HTTP connections

Port filters have many different interfaces. On my little gateway router, the port filtering uses the pretty, Web-based interface shown in Figure 17.6. Linux systems use either IPTABLES or NETFILTER for their firewall work. Like most Linux tools, these programs are rather dull to look at directly and require substantial skill manipulating text files to



• **Figure 17.6** Web-based port filtering interface

do your filtering chores. Most Linux distributions come with handy graphical tools, however, to make the job much easier. Figure 17.7 shows the firewall configuration screen from the popular YaST utility, found on the SUSE Linux distribution.

So, can one router have both NAT and port filtering? You bet it can! Most gateway routers come with both—you just need to take the time to configure them and make them work!

The CompTIA Network+ exam expects you to know that NAT, proxy serving, and port filtering are typical firewall functions!

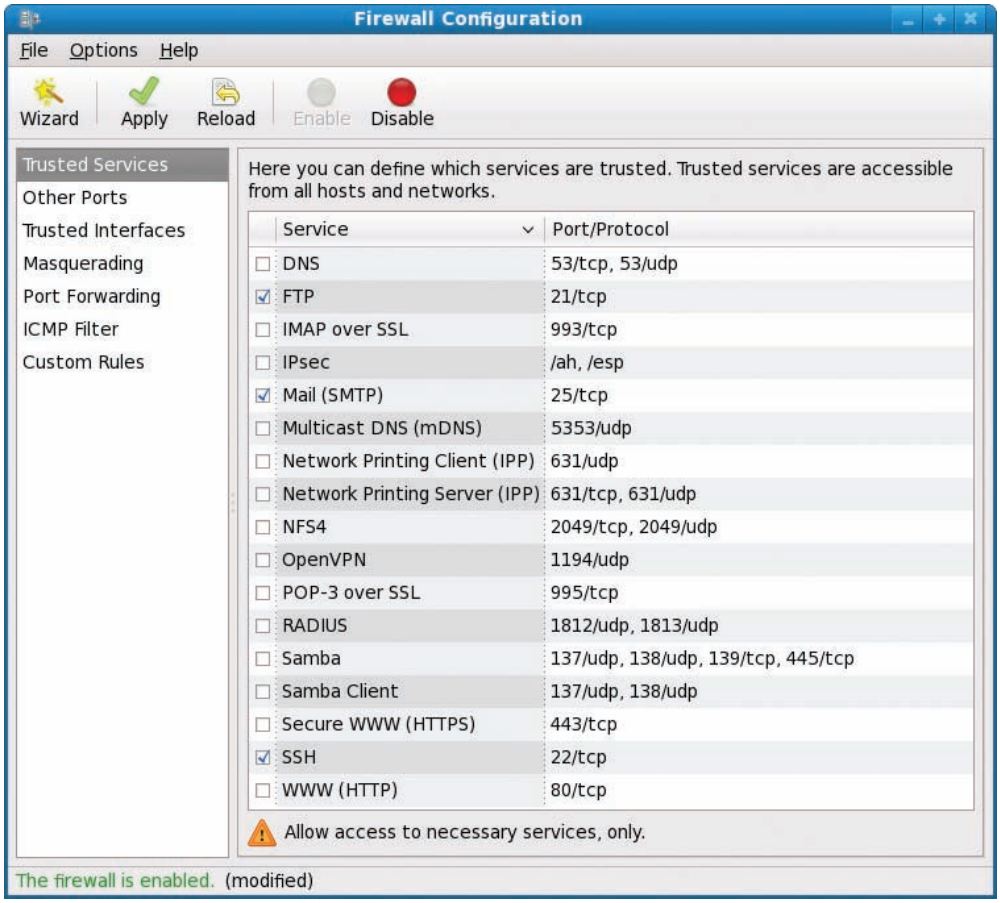
Packet Filtering

Port filtering deals only with port numbers; it completely disregards IP addresses. If an IP packet comes in with a filtered port number, the packet is blocked, regardless of the IP address. **Packet filtering** or **IP filtering** works in the same way, except it blocks packets based on IP addresses. *Packet filters*,

Cross Check

Proxy Servers

You learned about proxy servers back in Chapter 12, "Advanced Network Devices," so check your memory now. How does a proxy server work? At what layer of the OSI seven-layer model do proxy servers function?

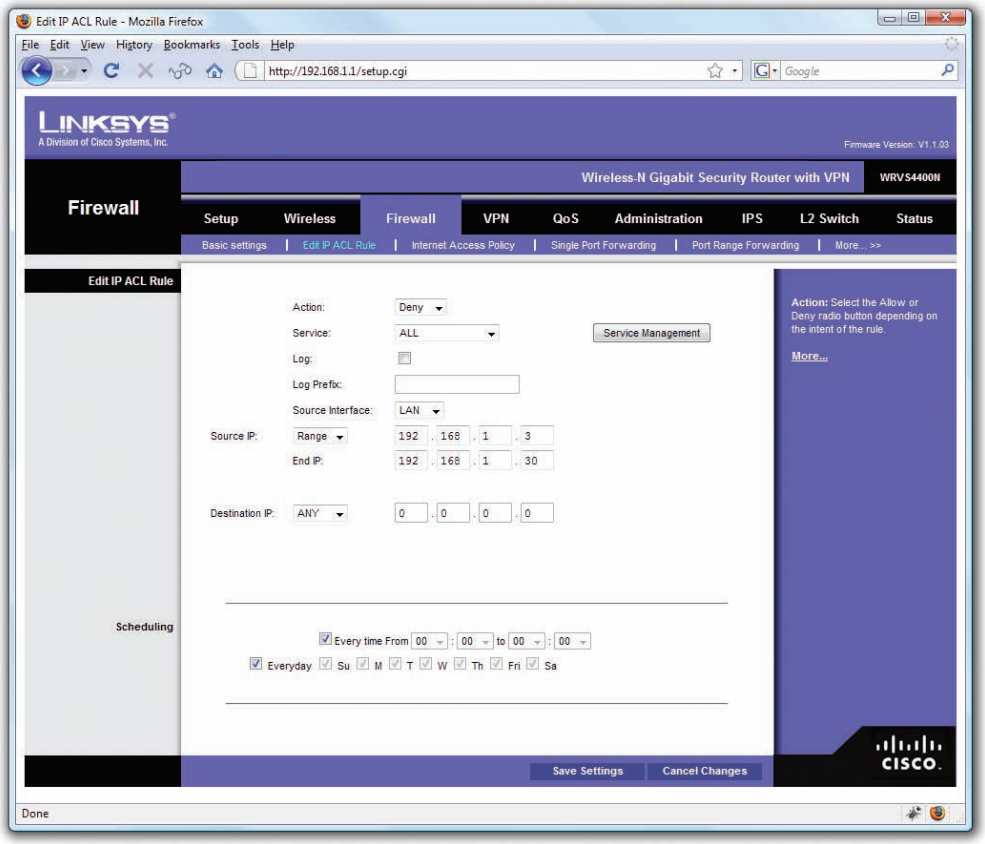


• **Figure 17.7** YaST configuration program

also known as *IP filters*, will block any incoming or outgoing packet from a particular IP address or range of IP addresses. Packet filters are far better at blocking outgoing IP addresses, because the network administrator knows and can specify the IP addresses of the internal systems. Blocking outgoing packets is a good way to prevent users on certain systems from accessing the Internet. Figure 17.8 shows a configuration page from a router designed to block different ranges of IP addresses and port numbers.

This type of filtering is called **stateless filtering** because the device that does the filtering just checks the packet for IP addresses and port numbers and blocks or allows accordingly. Each packet is judged as an individual entity to determine whether it should be allowed into the network. Stateless filtering works at Layer 3 of the OSI seven-layer model. Stateless filtering is inexpensive and easy to implement, but has one issue: once you've opened a particular path into your network, that path is open. Someone spoofing IP information could get in.

A more secure method of filtering is to use devices that do **stateful filtering**, where all packets are examined as a stream. Stateful devices can do more than allow or block; they can track when a stream is disrupted or packets get corrupted and act accordingly. The best of the stateful filtering devices are application proxies, working at Layer 7 of the OSI seven-layer



• **Figure 17.8** Blocking IP addresses

model. The only real problems with application proxies are that they tend to be slower than stateless filters and more expensive.

MAC Filtering

Similar to packet filtering, some firewall devices can allow or deny access to the network according to the MAC address of the client, what's called **MAC filtering**. Because every network device has a unique 48-bit MAC address, this should make for a very secure network. It's often one of the implemented security measures in wireless networks, for example, because it's quick to set up.

Many programs enable you to spoof or mimic a MAC address, though, so MAC filtering is not a strong deterrent for a determined hacker.

Personal Firewalls

Back in the days of dial-up connections, the concept of protection from external threats wasn't very interesting. The concept of dial-up alone was more than enough protection for most users. First, systems using dial-up connections were by definition only periodically on the Internet, making them tough for hackers to detect. Second, all dial-up connections use DHCP-assigned IP addresses, so even if a hacker could access a dial-up user during one session,

that dial-up user would almost certainly have a different IP address the next time they accessed the Internet. As long as they have installed a good antivirus program, dial-up users have nothing to fear from hackers.

The onset of high-speed, always-connected Internet links has changed the security picture completely. The user who dumps his or her dial-up connection for ADSL or a cable modem immediately becomes a prime target for hackers. Even though most ADSL and cable modems use DHCP links, the lease time for these addresses is more than long enough to give even the casual hacker all the time they need to poke around in the systems.

One of the first items on the agenda of Windows users with high-bandwidth connections is to turn off File and Print Sharing. Because NetBIOS can run over IP, sharing a folder or printer makes it available to anyone on the Internet unless your ISP helps you out by filtering NetBIOS traffic. Some hacker groups run port scanner programs looking for systems with File and Print Sharing enabled and post these IP addresses to public sites (no, I will not tell you where to find them!). When I first got my cable modem many years ago, I absentmindedly clicked the My Network Places icon on my Desktop and discovered that four of my fellow cable users had their systems shared, and two of them were sharing printers! Being a good neighbor and not a hacker, I made sure they changed their erroneous ways!

Although you can (and should) buy a hardware firewall to place between your system and the Internet, at the very least a single user should employ a personal software firewall program. Every operating system comes with some form of built-in personal firewall. Every copy of Windows comes with Windows Firewall (which we will discuss in detail in a moment). There are also third-party software firewalls like ZoneAlarm Pro (Figure 17.9). These personal firewall programs are quite powerful, and

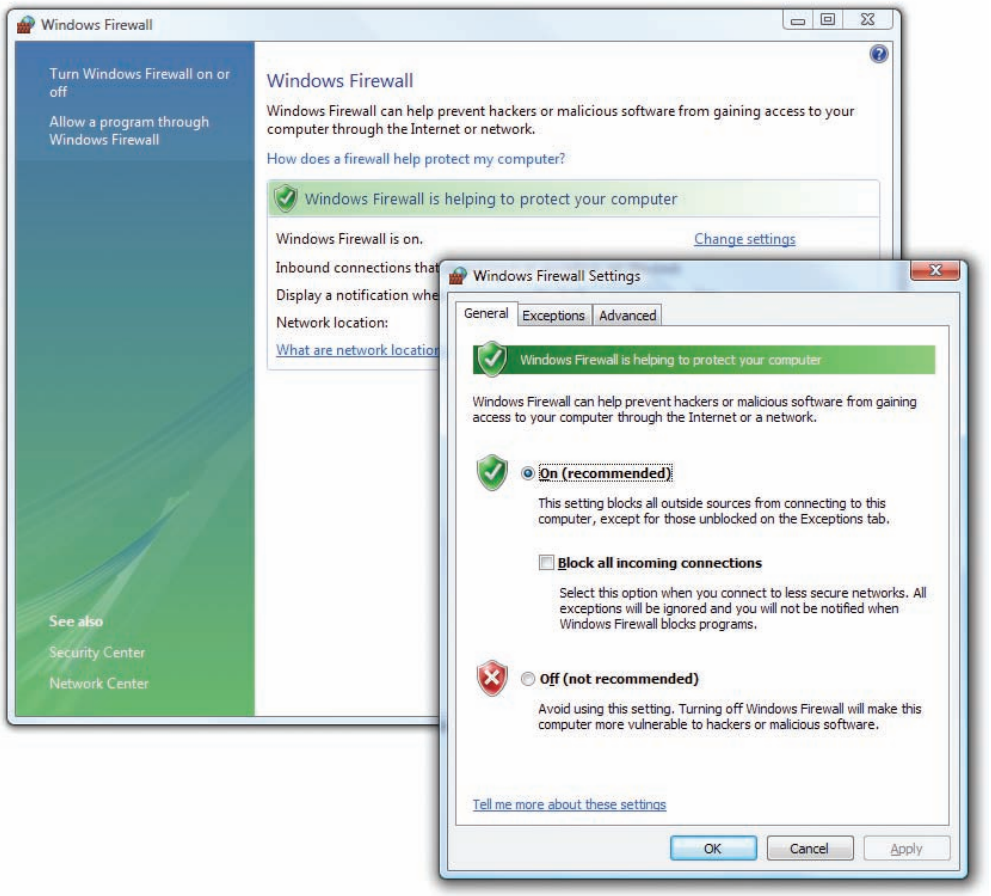
• **Figure 17.9** ZoneAlarm Pro

have the added benefit of being easy to use. These days, there's no excuse for an individual Internet user not to use a personal firewall.

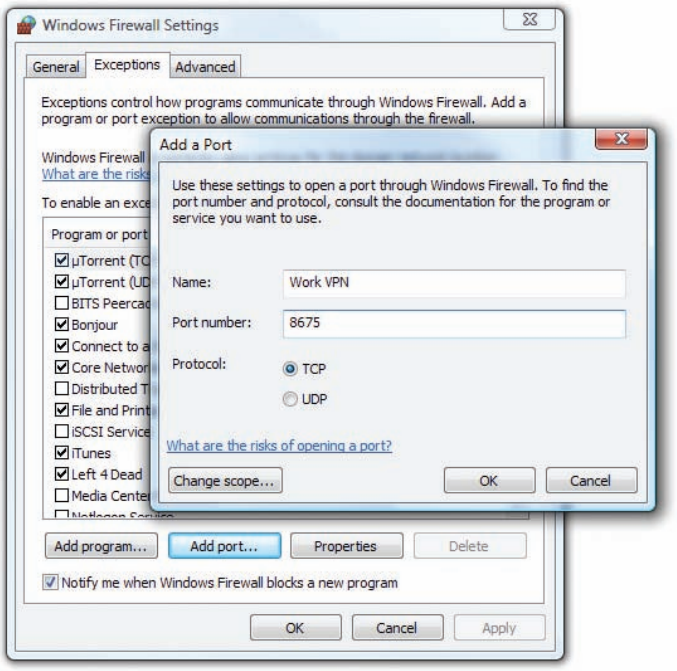
Every version of Windows comes with the handy Internet Connection Sharing (ICS) but ICS alone doesn't provide any level of support other than NAT. Starting with Windows XP, Microsoft included Internet Connection Firewall (ICF), renamed in Windows XP Service Pack 2 as **Windows Firewall**. Windows Firewall works with ICS to provide basic firewall protection for your network. Windows Firewall is often used without ICS to provide protection for single machines connected to the Internet. Figure 17.10 shows the screen where you'd turn on Windows Firewall in Windows Vista.

By default Windows Firewall blocks all incoming IP packets that attempt to initiate a session. This is great for networks that only use the Internet to browse the Web or grab e-mail, but will cause problems in circumstances where you want to provide any type of Internet server on your network. You can manually open ports through the firewall (Figure 17.11).

Products such as ZoneAlarm and Windows Firewall do a fine job protecting a single machine or a small network. But software firewalls run on your system, taking CPU processing away from your system. On an individual system this firewall overhead doesn't strain your system, but once



• **Figure 17.10** Enabling Windows Firewall



• **Figure 17.11** Opening TCP/IP ports in Windows Firewall

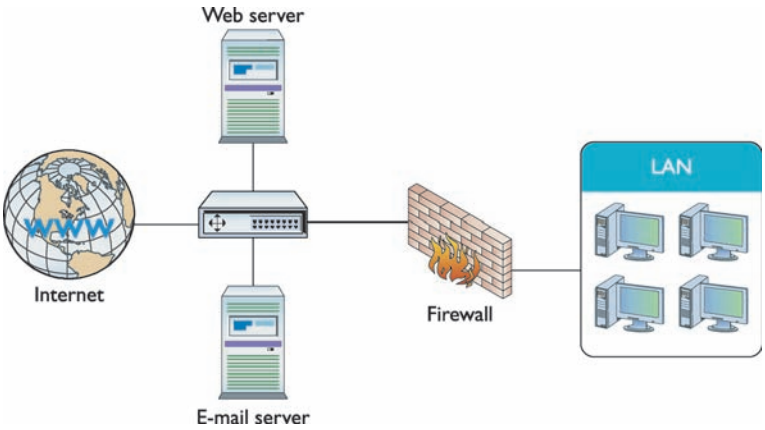
you start to add more than three or four systems, or if you need to add advanced functions like a VPN, you'll need a more robust solution. That's where small office and home office (SOHO) connections come into play.

Network Zones

Look for the CompTIA Network+ exam to refer to network setups where the firewall resides in a dedicated box as a *network-based firewall*. The exam calls firewall programs installed on your computer, such as Windows Firewall, *host-based firewalls*.

Large networks need heavy-duty protection that not only protects from external threats, but does so without undue restriction on the overall throughput of the network. To do this, large networks will often use dedicated firewall boxes, which usually sit between the gateway router and the protected network. These firewalls are designed to filter IP traffic (including NAT and proxy functions), as well as to provide high-end tools to track and stop incoming threats. Some of the firewall systems even contain a rather interesting feature called a honey pot. A **honey pot** is a device (or a set of functions within a firewall) that creates a fake network, which seems attackable to a hacker. Instead of trying to access the real network, hackers are attracted to the honey pot, which does nothing more than record their actions and keep them away from the true network.

Once you start to add publicly accessible servers to your network, like Web and e-mail servers, you're going to have to step up to a more serious network protection configuration. Because Web and e-mail servers must have exposure to the Internet, you will need to create what's called a **demilitarized zone (DMZ)**, a lightly protected network positioned between your firewall and the Internet. There are a number of ways to configure a DMZ. Figure 17.12 shows one classic example using and external and an internal router.



• **Figure 17.12** A DMZ configuration

The private, protected network is called an **intranet**. Compare this term to the term extranet you learned in Chapter 14, "Remote Connection Basics," and make sure you understand the difference!

Securing Remote Access

The mad proliferation of high-speed Internet connections to most households in the United States has enabled a lot of workers to work partly from home. Although this provides one cost-effective solution to the rising price of gasoline and of physical commuting, from a network security standpoint it opens up a potential can of worms. Network techs and administrators must strike a fine balance between making resources readily available over the Internet and making certain that only authorized users get access to those resources.

Chapter 17 Review

Chapter Summary

After reading this chapter and completing the exercises, you should be able to do the following.

Discuss the common security threats in network computing

- Network threats include system crashes, hardware failure, administrative access control, malware, social engineering, denial of service attacks, physical intrusion, and rogue access points.
- Hard drives crash, servers lock up, and power goes out. It is important to create redundancy as a proactive approach to dealing with these potential hazards before they occur.
- RAID technology provides fault tolerance for your data stored on hard drives.
- The administrative account on Windows is "administrator." On Linux and Macintosh OS X, it's "root."
- Malware describes any program or code that's designed to do something that you don't want to happen. There are many types of malware, including viruses, worms, macros, Trojans, and rootkits.
- A virus replicates, or makes copies of itself, but only across hard drives, not across networks. It also activates, or does something destructive like erasing files.
- A worm is identical to a virus except a worm replicates exclusively across networks.
- A macro is any type of virus that exploits application macros to replicate and activate.
- A Trojan is malware that looks or pretends to do one thing while at the same time doing something unwanted. Trojans can be used to turn an infected computer into a server and capture keystrokes, passwords, or files. Trojans, unlike viruses, do not replicate.
- Rootkits are Trojans that hide themselves so that many anti-malware tools can't find them.
- Malware can be avoided much of the time through user training. If malware infections do occur, they can often be removed with anti-malware software. However, this software must be kept up to date because new malware threats are discovered often.
- Social engineering accounts for the vast majority of network attacks. This includes using or manipulating people inside the networking environment in order to gain unauthorized access.
- Phishing attacks are becoming more common than old-school social engineering. In a phishing scam, an attacker tries to trick users into revealing information by posing as a financial, medical, or other institution or individual in need of help.
- Phishing attacks can manifest as e-mails, bogus Web sites, or even physical telephone calls.
- Flooder hackers perform Denial of Service (DoS) attacks to overwhelm your Web and e-mail servers with so many requests they're forced to cease functioning. DoS attacks include the smurf attack, which repeatedly PINGs an IP address.
- Distributed Denial of Service (DDoS) attacks are far more menacing than DoS attacks. DDoS attacks use multiple (hundreds) of infected computers (zombies) to perform the attack. A group of zombies under the control of a single operator forms a botnet.
- Servers should be physically protected by locking them in a room, or at the very least, a locked closet. The same holds true for network switches. A hacker can access your network by simply plugging a laptop into an unsecured switch.
- Never walk away from a server without logging off or locking the screen. A password-protected screensaver is also a good idea.
- Papers should be shredded to protect against successful dumpster diving. If you must write your password on a piece of paper, store it in a locked drawer.
- A rogue access point is an unauthorized wireless access point. These are very common in private homes because wireless routers purchased by novices are often configured to work out of the box with no security, allowing neighbors or anyone parked outside to access the network.

Describe methods for securing user accounts

- Internal threats from employees and users are more successfully subdued through policy implementation than through technology.
- Strong passwords are the ultimate key to protecting your network. A strong password includes upper- and lowercase letters, numbers, and nonalphanumeric characters and is at least eight characters long.
- In a perfect world, the best practice is to change your passwords regularly. However, this practice is difficult to maintain in the real world.
- A smart device, such as a credit card or USB device, can be inserted into a PC in lieu of entering a password. Similarly, biometric devices can be used to scan fingerprints, retinas, or even voice prints to authenticate a user without physically typing a password.
- Unused user accounts should be disabled, such as default accounts like Guest.
- Permissions should not be given to individual user accounts, but rather to groups; then, individual user accounts can be placed in these groups.
- It is possible for a user to be a member of several groups, with each group assigned different permissions. The permissions are combined to create the effective permissions.
- Default groups, such as Everyone, Guest, and Users, should be avoided unless you intend to permit all members of these groups to access a resource.
- When a user has conflicting permissions on a folder and subfolders, inheritance determines the effective permissions.

Explain how firewalls, NAT, port filtering, and packet filtering protect a network from threats

- Firewalls are either hardware or software that use a variety of methods to protect a network from threats. A common way is hiding IP addresses with internal address ranges, like the 192.168.x.y or 10.x.y.z ranges.
- A network-based firewall is integrated into a router, so it is also called a hardware firewall. A host-based firewall is software installed in individual computers. A secure network uses both.
- Network Address Translation hides the real IP addresses of an internal network from the Internet.
- Port filtering (or port blocking) restricts traffic based on port numbers, like allowing port 80 for Web pages (HTTP), but restricting port 23 to block Telnet traffic and hacking attempts.
- Packet filtering (IP filtering) filters signals based on data packets to allow only certain types of packets to flow to and from your network.
- Stateless filtering checks the packet for the IP addresses and port numbers and blocks or allows accordingly. Stateful filtering, which is more secure, examines all packets as a stream and can track when a stream is disrupted or when packets get corrupted.
- MAC filtering filters packets based on MAC addresses rather than IP addresses. MAC addresses can easily be spoofed, however, so this is not secure protection from a determined hacker.
- Dial-up users make poor hacking targets due to the nature of dial-up connections. They are not always connected to the Internet, making them hard to find. And they use DHCP-assigned IP addresses, which change every time they connect to the Internet. Always-on connections, such as cable or DSL, make for easy targets, so they should be protected.
- A personal firewall, such as ZoneAlarm Pro, is powerful enough to protect home computers and often does a better job than the firewall that comes built into Windows.
- A honey pot is a device or set of tools within a firewall that creates a fake network. The fake network directs hacking attacks away from the actual network.
- Larger networks having multiple servers should establish a demilitarized zone (DMZ), which is a network segment on the outer edge of your corporate network between your firewall and the Internet. The DMZ adds a layer of protection around your corporate network and can protect both incoming and outgoing transmissions.

Key Terms

adware *(461)*
biometric device *(466)*
botnet *(463)*
demilitarized zone (DMZ) *(476)*
Denial of Service (DoS) attack *(463)*
Distributed Denial of Service (DDoS) attack *(463)*
effective permissions *(468)*
external threats *(469)*
fault tolerance *(459)*
firewall *(469)*
hacker *(459)*
honey pot *(476)*
inheritance *(468)*
intranet *(477)*
internal threats *(465)*
IP filtering *(471)*
MAC filtering *(473)*
macro *(460)*
malware *(460)*
Network Address Translation (NAT) *(469)*
network threat *(459)*
packet filtering *(471)*
passwords *(465)*
phishing *(463)*
port blocking *(469)*
port filtering *(469)*
rogue access point *(464)*
rootkit *(461)*
smart device *(466)*
smurf *(463)*
social engineering *(462)*
spyware *(461)*
stateful filtering *(472)*
stateless filtering *(472)*
Trojan *(461)*
virus *(460)*
Windows Firewall *(475)*
worm *(460)*
zombie *(463)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all the terms will be used.

1. Bogus e-mails trying to trick you into revealing information constitute _____ attacks.
2. _____ is when you separate and either allow or deny access based only on the packet type being sent.
3. A(n) _____ is either hardware or software that protects a network from threats by using a variety of methods.
4. When your network blocks out traffic based on port number, you are using _____.
5. The Microsoft Windows XP (Service Pack 2 and later) operating system includes a built-in feature called _____ to protect from network threats.
6. The infamous "smurf attack" is a classic _____.
7. Many IT professionals are surprised when they first learn that the majority of network threats are _____.
8. The _____ is when a network administrator has set up a perimeter defense using two routers on the outer edge of your corporate network between your firewall and the Internet.
9. _____ hides your private network's IP addresses from the Internet.
10. A(n) _____ makes copies of itself across hard drives, but not across a network.

Multiple-Choice Quiz

1. Where do most network threats come from?
   - **A.** Internal users
   - **B.** External users
   - **C.** Both internal and external users
   - **D.** Network technicians
2. What aspect of protecting your network involves theft of equipment?
   - **A.** Packet filtering
   - **B.** Physical security
   - **C.** Policies
   - **D.** Port filtering
3. Which of the following items make up the strongest complex passwords? (Select all that apply.)
   - **A.** Lowercase letters
   - **B.** Uppercase letters
   - **C.** Numbers
   - **D.** Special characters
4. What is another name for port filtering?
   - **A.** Port blocking
   - **B.** Port filing
   - **C.** Port folders
   - **D.** Port segments
5. What is the term used to describe when folder permissions flow downward into subfolders?
   - **A.** Flowing
   - **B.** Inheritance
   - **C.** Permissions
   - **D.** Propagation
6. How should user accounts be established? (Select two.)
   - **A.** Open to all company individuals
   - **B.** Only given to specified individuals
   - **C.** Allowed access to needed resources
   - **D.** Allowed access to all resources
7. Where would a DMZ more commonly be found?
   - **A.** On a single PC
   - **B.** On a server
   - **C.** On a SOHO
   - **D.** On a larger network
8. Just after opening a Microsoft Excel spreadsheet, Rowan notices that some of his filenames have changed and that his network connection no longer works. What type of malware has infected his computer?
   - **A.** Worm
   - **B.** Macro
   - **C.** Trojan
   - **D.** Rootkit
9. What problem does a rogue access point introduce?
   - **A.** Unauthorized physical access to a server
   - **B.** Unauthorized access to a wired network
   - **C.** Unauthorized access to a wireless network
   - **D.** Unauthorized physical access to a router or gateway
10. What is the difference between a virus and a worm?
    - **A.** A virus is only distributed via e-mail. A worm is only distributed via infected Web servers.
    - **B.** A worm is only distributed via e-mail. A virus is only distributed via infected Web servers.
    - **C.** A virus replicates across networks. A worm does not.
    - **D.** A worm replicates across networks. A virus does not.
11. Which statements about passwords are true? (Select two.)
    - **A.** You should change your password regularly.
    - **B.** You should use familiar terms, like your pet's name or your birthday, as your password because it will be easy for you to remember.

C. It is okay to write your password on a piece of paper in case you forget it, as long as keep the paper in a locked drawer.

D. You may not use spaces in a password.

12. Which statement is true?

A. A DoS uses a zombie while a DDoS uses a botnet to attack a single system.

B. A DoS uses a botnet while a DDoS uses a zombie to attack a single system.

C. A DoS attacks a single system while a DDoS attacks multiple systems.

D. A DoS attacks systems on the Internet while a DDoS attacks system in a DMZ.

13. What is a honey pot?

A. It acts as a fake network, luring potential hackers away from the actual network.

B. It is a security measure that slows unauthorized network access to a crawl (as if running in honey), making your network undesirable to hackers.

C. It is what hackers call an easily hacked network.

D. It is a specialized padlock manufactured for the sole purpose of securing computer systems.

14. You receive an e-mail from your credit card company informing you that your card number has been stolen. You click a link in the e-mail and are taken to what looks like your credit card company's Web site, where you are asked to enter your credit card number to determine if it is among those that were recently stolen. What should you do?

A. Enter your credit card number immediately to determine if it is among those stolen as this is the only way to protect against unauthorized charges to your account.

B. Call the toll-free number listed on the Web site to verify it is legitimate before entering your card number.

C. Call the toll-free number listed on the Web site and read your card number over the phone to the customer service representative.

D. Close your browser without entering your card number as it is likely a phishing scam, then call the toll-free number listed on the back of your actual credit card to verify that is the case.

15. Which are examples of a software firewall? (Select two.)

A. The firewall software built into a router

B. Host-based firewalls

C. Network-based firewalls

D. ZoneAlarm Pro

Essay Quiz

1. Many people have said that you don't know something unless you can describe it simply to others. Write down a brief definition of social engineering. Include some examples.
2. Research three software firewall solutions. Compare and contrast the solutions that you find based on cost, reputation (research product reviews), and support provided.
3. Some of the older military veterans in your networking class are surprised to see the term "DMZ" being used. Write a short paragraph defining a DMZ and its uses.

Lab Projects

• Lab Project 17.1

In this lab project you will continue to quench your thirst for knowledge of hacking. Use the Internet to research three hacking tools or techniques. Do not try these techniques on your classroom lab network, but research them as time permits. Document your findings, and be prepared to show off your knowledge with others in your class. Have fun learning even more about hacking!

• Lab Project 17.2

You have been tasked with finding out the cost of a variety of firewalls and other software. Create a spreadsheet similar to the following one. Use the Internet to research prices and Web site locations for each of the following items, as well as current variations/versions of this and other software. Note: some items may be freeware/shareware, or included with an operating system.

SOFTWARE	WEB SITE	COST
AVG Anti-Virus		$
CA Anti-Spyware		
Cerberus FTP Server		$
Lavasoft Ad-Aware		$
McAfee VirusScan		$
Microsoft ISA Server		$
Norton AntiVirus		$
Norton Internet Security		$
Spybot Search&Destroy		$
Trend Micro HouseCall		$
Windows Firewall		
ZoneAlarm		$
		$