# Chapter 6

# Secure Network Management

## Solutions in this Chapter:

- Network Management and Security Principles
- Management Networks
- IPSec and VPNs
- Network Management Tools and Uses

## Related Chapters:

- Chapter 1 Understanding Your Perimeter
- Chapter 2 Assessing Your Current Network
- Chapter 7 Network Switching
- Chapter 10 Perimeter Network Design
- Chapter 11 Internal Network Design

# Introduction

Throughout the preceding chapters, we described what an "internal" network segment really is, presented methods on how to assess the security of your network, document the network topology and aggregation points, presented information on the major firewall technologies and their associated products, how to attack those products using contemporary exploits, and we even talked about different ways to route information back and forth between our internal and external segments through your firewall. It won't be until the following chapters where we'll be presenting the wonders of network switching, internal segmentation, Intrusion Detection and Prevention Systems, and an in-depth look at applying the principles of this book in the Chapter 11. So, why would we stick the boring topic of network management right smack in the middle of all this excitement?

The answer is simple: before we dive head first, we need to make sure the lifeguard is on duty. Now is the time to discuss management of the network, *before* you spend a bunch of time designing an unmanageable beast of a network. Most people will tell you that network management is a boring task relegated to caffeine-addicted network operations center (NOC) drones who just wait for the big red button to light up—not true! The true bragging rights of the network engineer come from being able to measure your successes in bar graphs and pie charts, suitable for board-room meetings. What we discuss in this chapter will allow you to quantify all the late hours that you spend in the wiring closets and data centers, and prove to the budget steering committee that it really *was* worth the extra $100k to outfit all floors with managed switches instead of dumb hubs (see Chapter 7 for more information on managed switches—but not before you finish this chapter!).

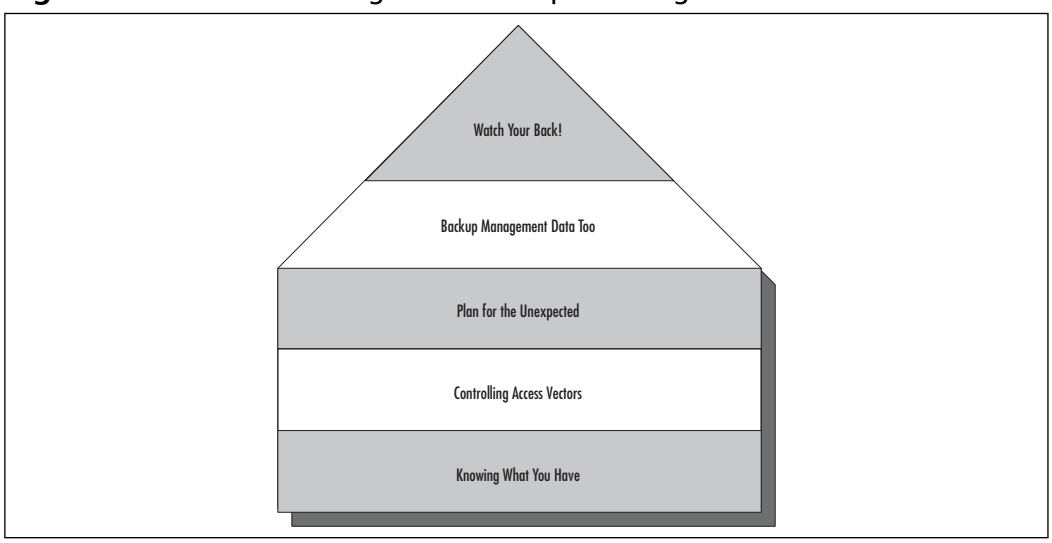
In the next section, we present five basic network management principles that will guide us through setting up our "Mission Control" center (space helmet optional). As a glimpse into the segmentation discussion in Chapter 11, we are going to discuss the concept of a management network and how to best keep things segregated on that network. No management network is complete without some form of transport layer encryption (this is the one network that will have far-reaching control over your entire infrastructure, so you're going to be highly motivated to keep prying eyes away). We will present IPSec and other VPN technologies as a way of maintaining the integrity and confidentiality of your management tools. Then, we will see those five network management prin-

ciples applied in a sampling of popular tools, running the full gamut from free open-source tools, to high-end five-figure enterprise management suites of applications. At the end of the day, you'll have a room full of blinking lights that would bring a tear to any NASA scientist's heart.

# Network Management and Security Principles

Like any good chapter with the word *management* in the title (be it Business, Sewage Treatment, or Network Management), you have come to expect the body of knowledge boiled down into a handy wallet-sized version that can serve to guide us throughout the rest of the chapter. Well, we certainly don't like to disappoint, so we have summarized all you'll ever need to know about network management into five very broad security principles that we will refer back to throughout the rest of this chapter. In addition, if you are one of the first 1000 readers to turn the page, we will even throw in a diagram at no extra charge

**Figure 6.1** Network Management Principle Pentagon




As you can see from Figure 6.1, after you have a solid foundation with Knowing What You Have, Controlling Access Vectors, and Planning for the Unexpected, you are ready to build on that with intelligent backups of your most critical management data. The pinnacle of our diagram is Watching Your

Back, where we introduce prudent security measures that can dramatically decrease your exposure to electronic eavesdropping, and with any luck turn you into an appropriately fearful, paranoid security engineer who encrypts everything, including your business cards.

Notes from the Underground…

### Specially Coded Business Cards

While it might seem insane to encrypt your business cards that you hand out to people, there is something to be said for *encoding* them. We're not going to confess to any of our tricks, but let's just say that some people have different versions of business cards printed at work, all with different extension numbers for our telephone, as well as slight variations in e-mail addresses (sandres@securitysageguide.com versus stevea@securitysageguide.com versus steve.andres@securitysageguide.com).

Need to drop off a business card to receive a cool T-shirt at a booth (and how many of us have done that at one too many RSA Conferences?), but don't want to get listed on a telemarketer's call sheet? No problem; give them the card with the phone extension that goes directly to voicemail, and the e-mail address that goes directly to the spam folder. Have an important business contact that you just ran into at Black Hat? Give him the one with the "priority" e-mail and the extension number that forwards directly to your cell phone.

## Knowing What You Have

As shown in our Principles Pentagon, any good network management strategy begins with an inventory to get a handle on what you have in your environment. Most of the tools that we discuss later in this chapter either have a network discovery wizard built in, or insist that you provide them with an inventory of your networking devices as part of their initial setup. If you've been reading along with us, we covered the importance of network asset inventory back in Chapter 2. We also covered a number of great tools to make this (sometimes dreaded) task a lot more manageable (pun intended).

The importance of an asset inventory cannot be overstated. Without a detailed list, you will not know where to spend most of your dollars and most of your time. If you have relatively few Windows machines, there hardly seems to be a reason to invest money in a Microsoft SMS solution. By the same token, if you have very few UNIX servers, using a management system based on *rshell* and *rexec* commands would be impractical at best.

# Controlling Access Vectors

Once you have a snazzy-looking network map and a detailed asset inventory in front of you, it becomes a lot easier to see all of the access vectors to your information resources. An access vector is any conduit or method with which an unauthorized or authorized user can view, manipulate, or erase sensitive data. The most common access vectors are summarized in Table 6.1.

**Table 6.1** Common Access Vectors

| Name | Method/Conduit |
|---|---|
| Console | Direct access to the file server's keyboard, or the firewall/router's serial configuration port. |
| Shoulder-Surf | Peering over one's shoulder to watch keystrokes. |
| Local Subnet | Computers within same collision domain might eavesdrop or attack. |
| Local Network | Computers within the same network might be able to attack information resource. |
| Wireless | Often overlooked, this includes both authorized and hostile wireless connections. |
| Dial-Up Modem | Legacy dial-up modem pools can be a dangerous vector if not managed correctly. |
| VPN | Virtual private network (VPN) connections that come through the firewall should watched. |
| Internet | Anything that your firewall does not block can become an access vector. |
| Malicious Outbound | Don't forget that sensitive data transmissions can originate inside and be destined for malicious hosts beyond your firewall. |

While you certainly can't annotate every variation of an access vector on your network map, it can be beneficial to call special attention to VPN, dial-up,

and wireless connections, since those are so easily ignored during security planning. Contemporary wisdom brings us to conclude that everything in the big cloud labeled "Internet" is bad (or potentially hostile), and everything on this side of the firewall is good. However, that's not always the case. While every network is different and you must craft your own strategy using the constraints placed before you, we will attempt to provide some guidance on minimizing your risk exposure for these attack vectors. This isn't a "How To" chapter; it is about guidance and principles and tips to get you started.

## Console

While it is undoubtedly the most damaging access vector, *console* access is also the easiest to mitigate. This access vector can, by definition, only be used if there is direct, physical access to the hardware in question (router, firewall, file server, database, etc.). If the attacker can actually walk right up to the device and touch it, then you know you're in trouble. The best password policy in the world won't stop the attacker from popping open the case and walking out the door with your hard drives. With your data safely at home, she can spend days or weeks with password-cracking programs to try to get at your data. In reality, there are backdoor methods to avoid password protections altogether that take less than an hour. Or, the attacker could not even care about the data for herself, but instead just use it to extort money from the victim (perhaps resulting in a public relations backlash should this incident be reported to the mainstream media).

Make absolutely sure that you have appropriate physical access controls in place wherever there is in information storage device. This includes not only your nicely chilled "showcase" NOC with the smoked glass windows and the multimillion-dollar fire suppression system, but also each and every one of your wiring closest and server rooms. Now, notice that we said *appropriate* physical access controls; while you might need a state-of-the-art proximity card system for your NOC, your wiring closets might be okay with just a good, solid deadbolt lock. The point is to have something—anything—to prevent a casual tinkerer or a determined attacker from laying their hands on your information. If all he has to do is reach under the receptionist's desk to find your HR database—and don't tell me you haven't heard of *that* urban legend—you have not exercised proper controls. If the attacker has to saw through a deadbolt (and thus making quite a ruckus) to get to your hubs and switches, you have succeeded.

**NOTE**

More information about physical access controls can be found toward the end of Chapter 2, as well as the Network Management Tools section later in this chapter.

## Shoulder-Surf

We've all seen the "shoulder-surfer" in action. The login prompt comes up on the screen, and the coworker next to you leans in uncomfortably close so that he can watch your keystrokes as you type them, hoping to capture your password. The usual mitigation technique for this is to either type ridiculously fast, such that your coworker can't keep up, or give him a menacing stare and tell him to back off. Both are troublesome. We even know some people who will make mistakes on purpose in their passwords and use the backspace key frequently while typing, so that the potential shoulder-surfer gets confused in the process.

We're going to stop short of embarrassing ourselves by telling you about cultural etiquette and proper personal space issues; anyone who has seen either of us eating lunch can tell you that etiquette is something we do not list on our résumés. However, besides the obvious mitigation step of having others turn their heads, another (more techie) method is to employ two-factor authentication. In this strategy, the user only has a short PIN to enter, and the rest of the "password" is made up of a short-lived numerical sequence (the "token code") that appears on a key fob, credit card-sized device, or Palm Pilot applet. If the annoying individual next to you leans in for a peek, chances are he will spy your token code and not your PIN, since it is more easily read. The look on his face when he realizes that the number is only valid for the next 59 seconds is quite priceless!

Notes from the Underground…

## Take My Token… Please!

I'm definitely anything but tactful when it comes to personal-space issues. I'll either ask someone to move out of the way and turn their head, or I will just move them out of my way and turn their head. That being said, I must confess that I did lose my patience with a particular shoulder-surfer back when I was working for the University of California. We will call him "Tim" (since that was his name). UCLA had invested heavily in the SecurID two-factor authentication system for their centralized billing and campus authentication project, and all staff members were issued big 3- x 5-inch token cards and instructed to never put them in their wallet (although they were wallet sized). Eager to learn about all the access privileges that he did not possess on the IBM ES9000 Supercomputer that ran the Bruins' über-database, Tim would always get especially close and intimate with you as you went to log in. It became so bad that at one point, I just handed him my token and asked him to read the "password" off to me! Little did he know that I used the diversion to enter in my PIN without observation, before sliding the keyboard over to him and having him enter the token code (which would expire in a matter of seconds). Shortly after this little stunt (about 10 seconds after, with time still ticking down on the SecurID), Tim excused himself to rush to the "bathroom" and apparently made a pit stop at his desk to attempt a login using my credentials.

Not only did Tim not have my PIN (only my token code, which was invalidated as soon as I used it no matter how much time was left), he also received a call from Academic Information Services, the campus' authentication police. After a four-hour "tutorial" on the punishments associated with California Penal Code section 500 (unauthorized access to a State-owned computer system), Tim was relocated to a Circuit City nearby, where he now enjoys snooping on credit-card numbers and pestering senior citizens with extended warranty sales pitches.

If you're interested in learning more about two-factor authentication, a number of white papers at vendor Web sites are definitely worth reading. The major player in this market is RSA Security, with their SecurID tokens, but you

can also find similar token solutions from ActivCard, Authenex, CryptoCard, and Rainbow. Links to vendor Web sites are listed at the end of this chapter.

Tools & Traps…

## A SecurID by Any Other Name

Although there are a number of vendors out there sporting two-factor authentication options (a recent search on Google revealed 31,400 hits), our favorite is still the original: the SecurID token from Security Dynamics, which later purchased RSA Security and adopted the acquired name. Many newer vendors have tokens in the form of USB keys, but we prefer the rugged design and simplicity of the RSA SecurID key fob. Newer models even employ the *Rijndael* cipher, also known as the Advanced Encryption Standard (AES), newly certified from the U.S. Government.

Notes from the Underground…

## Alien Technology?

DES (the data encryption standard), which was the encryption standard for over 20 years, was replaced in 2000 by AES (Advanced Encryption Standard). AES is based upon the *Rijndael* block cipher written by Joan Daemen and Vincent Rijmen, two Flemish gentlemen from Belgium. Since the 70's, the United States had very strict regulations governing the export of crypto outside of the United States. These regulations were 'relaxed' in 1999 and quickly afterward, the encryption standard adopted by NIST and the US Government was a 'foreign' one that could not have legally moved across US borders just months before…

## Local Subnet

Machines that are located within the same *collision domain* of one another will, by definition, be able to see each other's network traffic. This is usually the case when you are using hubs; with network switches, each port becomes its own collision domain and these issues are not present. Note that at aggregation points, again by definition, all the traffic will be aggregated into one stream, which can lend itself to eavesdropping. However, the point of this access vector is the ease with which machines, within the same collision domain of the information resource, can eavesdrop on data bound for the file server, and requests being fulfilled back out to workstations.

The easiest mitigation step for this attack vector is also one that will greatly increase network performance; replace all of your hubs with manageable switches and you can (practically) cross this attack vector right off your list. See Chapter 7 for an extended discussion on collision domains, broadcast domains, hubs, switches, and beef jerky (we're not kidding).

## Local Network

The access vector that we're calling *local network* is your run-of-the-mill network-based attack, with an emphasis on ones originating within the "trusted" part of your network infrastructure. These are the ones that can surprise you at 3 A.M. on any given Sunday because you assume (perhaps incorrectly) that anyone within your organization would have no reason to maliciously pilfer information from your databases. Even the world's largest Internet service provider, America Online (AOL), fell victim to this attack vector.

Notes from the Underground…

### AOL SecurID Bypass

With your personal bias for or against AOL aside, you have to admit that they do have a pretty amazing user membership. Accordingly, their internal customer information systems must have high security. One such system (which has since been replaced) was the Customer Records Information System (CRIS), which held sensitive information on more than 23 million subscribers. The system was engineered with two-factor

Continued

authentication (using RSA SecurID tokens), but was set to implicitly trust all "on campus" connections from within the AOL headquarters.

Some former AOL employees knew the architecture of CRIS and knew that it was much too difficult to try to hack the SecurID system to access CRIS remotely. Instead, they just needed to compromise an internal machine, and redirect all requests via that workstation. Sadly for AOL Customer Service, this was not very difficult. In June 2000, through the normal coercion that happens in every spam message we all receive, a particularly non-savvy customer service representative clicked on a link that launched a malicious Web site (www.computerworld.com/security-topics/security/story/0,10801,46090,00.html). Therein, an ActiveX control was loaded and (thanks to the user clicking "YES") executed on the internal AOL computer. From there, it was quite easy for the attacker to route requests via this workstation. Since the CRIS security architects made the assumption that internal requests were always valid (and thus ignoring the *local network* attack vector), millions of subscribers were affected.

Since that time, AOL has changed their authentication methods to always use SecurID two-factor authentication regardless of internal or external connections, and has since rewritten their internal systems (calling the new system "Merlin"). Sadly, once again an AOL customer service rep was tricked into accepting (and executing) a file transfer via instant messaging in February 2003 (www.wired.com/news/infostructure/0,1377,57753,00.html). Although the new Merlin application required a username, two passwords, and a SecurID token, using elementary social engineering and spoofed e-mails from AOL Operations, attackers were able to gain access to the Merlin database of 35 million subscribers!

We don't mean to beat up on the AOL security engineers—we're sure they're kept quite busy and we would probably have just as difficult a time securing a network that big across an employee community of very differing skill levels. However, if nothing else, it makes you consider the local network attack vector in an entirely new light, as well as ponder the wisdom in allowing these customer service workstations to access the Internet at all.

And if that doesn't get you thinking, just sit back and consider that their customer database went from 23 million to 35 million in just three years! Guess all those CDs by mail really do have an effect.

## Wireless

The time might soon come when all of us feel completely safe in deploying a wireless segment of our networks. As of our publication date, that level of comfort is still not there. From a corporate security engineer's point of view, there simply isn't enough benefit to outweigh the potential security costs introduced by wireless networks. Unfortunately, sometimes other parts of the company (Sales, Marketing, Executives) have more pull in IT efforts than those in security, and the convenience of a wireless local area network (WLAN) is demanded by many these days.

If you are one of the many who have been forced to (or perhaps willingly) install a wireless network, you should definitely pay close attention to these attack vectors and note them with some ridiculously bright yellow highlighting in your network map. Some mapping tools mentioned in Chapter 2 even use a different icon for wireless access points (WAPs) to make your job of identifying them easier. After documenting all of the WAPs throughout your network, it wouldn't be a bad idea to hire an outside firm to "sweep" through your building(s) to make sure that no unauthorized WAPs have found their way on your network. With the price point of these devices going south of $50, don't be surprised to find a WAP right next to the chewing gum and tabloids in the "impulse buy" section of your supermarket.

Make sure to consider the attack vectors introduced by both unauthorized and authorized wireless workstations. The unauthorized threat is pretty obvious: someone can park across the street, point a Pringles can at your building, and get to your HR intranet—even the U.S. Secret Service is using the popular potato chip receptacle as part of their regular security sweeps (www.computerworld.com/mobiletopics/mobile/story/0,10801,74806,00.html).

What you might not consider at first is the danger posed by *authorized* wireless connections. All too often, these connections are not encrypted, or the machines themselves are subject to compromise because they lack some form of personal firewall software installed. A study performed by AirDefense (a WLAN security vendor) in April 2003 showed that 88 percent of wireless connections at a Boston trade show are unencrypted. Additionally, some WLAN workstations were configured to connect to *any* WAP available, putting your corporate workstation (and any information on it) at risk if it were to connect with a WAP run by an attacker (referred to as a "rogue access point"). Without a personal firewall and by associating with these rogue access points, an attacker could compromise the security of your sales executive's laptop using any number of common

exploits, install a Trojan program to record keystrokes, and then sit back and wait for the laptop to wander back to your access point. Even with encryption enabled, the Trojan would be able to piggyback on the authorized wireless connection, retrieve sensitive information, and transmit it back to the attacker. Make sure you are aware of both authorized and rogue access points operating within or near your building.

## Dial-Up Modem

Some of you reading this might never have heard of a "Shiva" before, but those who have will know it is synonymous with dial-up modem pools that were popular before broadband Internet access was made available to most U.S. homes. If your company does have these legacy dial-up modem pools, you should definitely run—not walk—to your nearest VPN vendor and plan a strategy to phase them out. With high-speed Internet access down to $30/month in some areas, there just isn't much sense in having a dozen phone lines (each with minimum telco charges, usage charges, and perhaps even toll-free surcharges if your company provides that) waiting to accept connections.

If you used that yellow highlighter we talked about in the previous section for the wireless segments, you should use a red marker to circle any leftover dial-up modem pools. These usually sit behind the firewall, and aren't heavily guarded. Anyone in the world with a dial tone can reach your modem pool and attempt to log in. While brute-forcing a VPN password over a few weeks will definitely be noted in the firewall logs and the IDS logs, it would be quite believable to hear that the dial-up pool either performs no logging, or that logs are almost never reviewed, since the connections are assumed to be trusted.

Tools & Traps…

### Who Is Shiva?

Many vendors exist (or existed) for dial-up networking services, but the name Shiva stands out among the rest of them. Their LANrover series of connectivity products was quite popular, and we've come across it on a number of engagements. Luckily for us on the attack and penetration team, these devices almost always have single-factor (password) authentication, which is easily brute-forced (set password = username, or try a blank password). Worse yet, the default administrator password of "shiva" is almost never changed.

The Shiva LANrover was an excellent product, don't get us wrong. It's just a technology that has come and gone, and now needs to take its place on the shelf along with eight-track tapes and laser discs.

## Virtual Private Networks

VPN connections are a difficult attack vector to visualize. Often times, your VPN device is also your border firewall. In some large installations, dedicated VPN concentrators such as the Cisco 3005 VPN Concentrator (formerly the Altiga 3005) perform all the encryption services and offload the number crunching from the main firewall. In both cases, you must consider the authentication methods used as well as the authorization to use network resources.

If your firewall is performing VPN services, you at least have one thing going for you: your firewall definitely has knowledge of the VPN traffic. If you run a separate VPN concentrator, this might not be the case. Most times, dedicated VPN concentrators are installed "next to" the corporate firewall (meaning they have one interface on the Internet and the other interface connected to the internal network), rather than being in-line with the corporate firewall. This means that while an attacker might not be able to attempt too many telnet connections to your firewall's outside interface without your IDS becoming suspicious, you might be ignoring the same type of probing on the VPN concentrator.

Once a workstation makes a connection to the VPN concentrator (or VPN services running on your firewall), what authentication methods are used? Again, more is better in this case, and we like to see two-factor strong authentication

used in conjunction with these devices. The good news is that the integration between VPN concentrators and back-end authentication systems running RADIUS (discussed later in this chapter) is quite mature. You should be able to add two-factor authentication to your VPN deployment without too much configuration hassle (there will, of course, be a hefty price tag).

After successfully authenticating to the VPN concentrator or firewall, the big question is, *just what is that remote user authorized to connect to?* It's not enough to be satisfied with authentication; you must consider the dangers involved in providing remote users with unrestricted authorization throughout your internal network. Because these remote connections are likely from machines that are outside of your control (home computers) or that your IT team only maintains infrequently (a traveling salesperson with months' old anti-virus signatures is a common occurrence), you must have a healthy amount of distrust for these machines. Most VPN installations we have seen on our customer engagements are architected such that once a user is connected, he is on the local network and is able to do anything and contact any machine he pleases.

This is quite dangerous! Imagine if your vice president's young son was able to reach the keyboard during a currently logged-in session. In the process of downloading the latest Jennifer Garner movie from an illegal warez site, his son was also able to infect that laptop and spread—via the *authorized* and *authenticated* VPN connection—to the rest of the internal network.

It is for this reason that we suggest quarantining VPN connections so that they are only allowed to connect to essential servers, and that they are given IP address assignments from a completely different DHCP pool than normal users, so you can easily identify them. In Figure 6.2, we see a suggested topology where the VPN users have a dedicated network segment for their connections, apart from normal internal workstations. Furthermore, the VPN service network is only connected to the resource network (housing directory services, e-mail, etc.). Even if someone were to compromise a VPN session or even one of your remote users' computers, she would not be able to connect to the HR database or any Accounting data stores.

**Figure 6.2** Sample Topology Showing Dedicated VPN, Resource, Management, and DMZ Service Networks

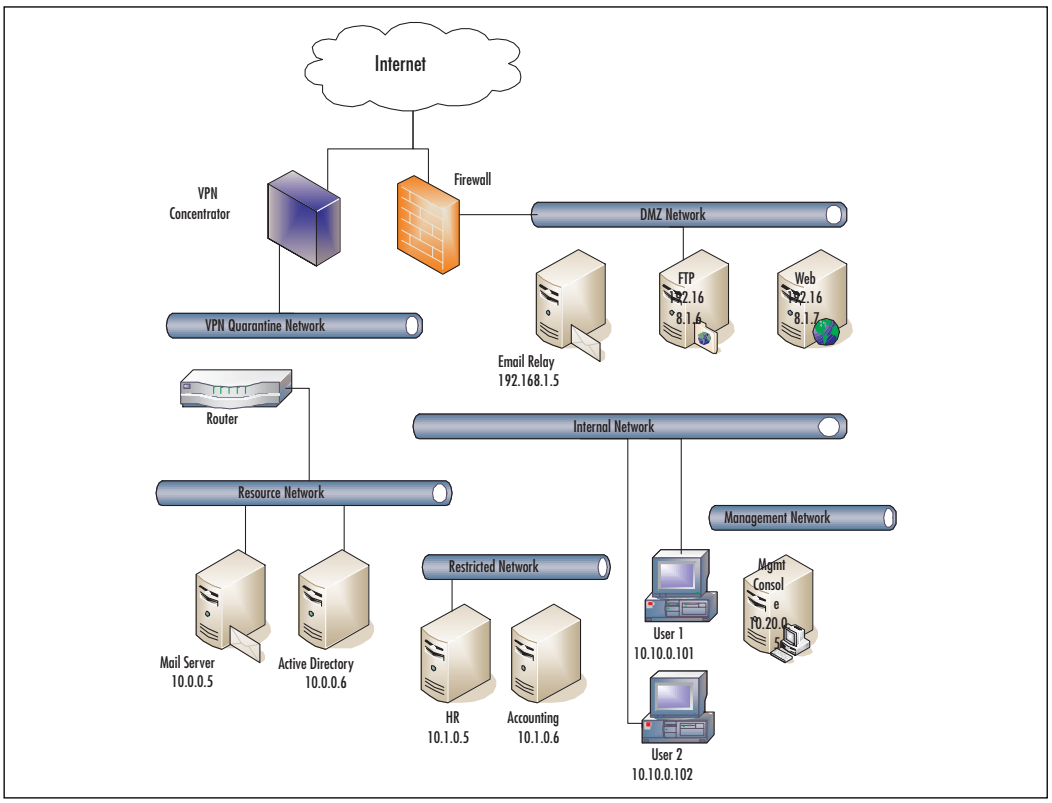



Figure 6.2 illustrates the concept of a highly segmented network, and we will showcase the benefits to a dedicated management network later in this chapter. Don't let the complexity of the diagram distract you from the concept behind it; the more you can segment your network and classify the traffic that traverses it, the easier your management task becomes.

## Internet

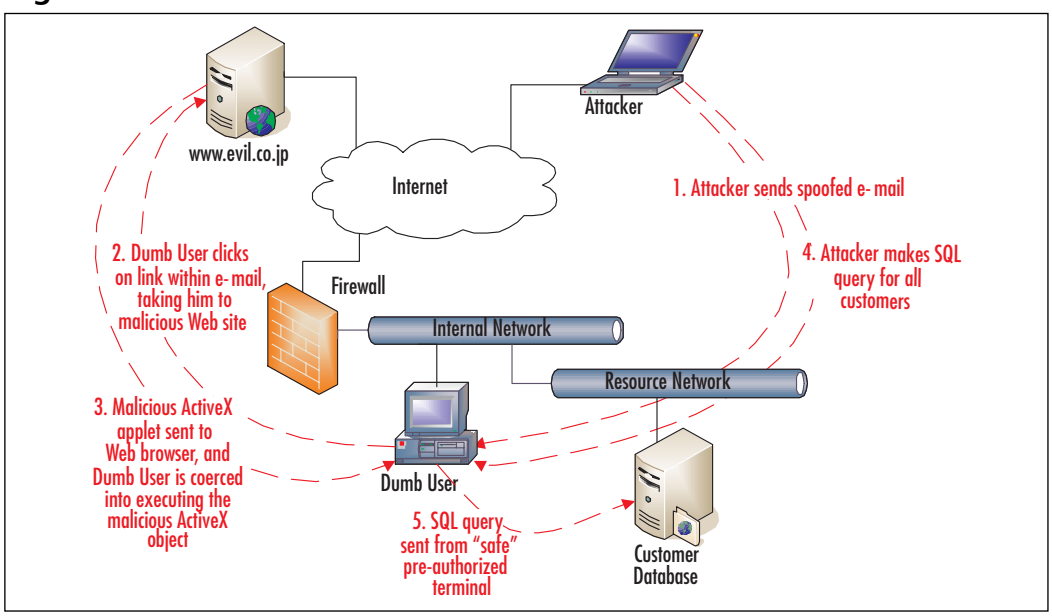
At last, we arrive at the one access vector that you knew you had all along: the big wide world of the Internet. If you are living in the 21st century and your network doesn't have some form of connection to the Internet, you probably have a good reason for it (perhaps a military network with an "air gap" defense). For the other 99 percent of us, we must treat the Internet very seriously when we consider attack vectors. By just sliding in one rather small RJ45 cable into

your firewall, you have now allowed the 6.4 billion inhabitants of Earth (or, more accurately, the small percentage of those Earthlings who have Internet access) an opportunity to invade your network. We all knew that this was an important attack vector, so there's no sense in convincing you of it now. The fear of Internet-based attacks is inherent in any modern network, and should continue to be feared and respected for many years to come.

## Malicious Outbound

A malicious outbound attack vector is one where the "attack" is usually invited (whether it should be is another story) and the damage is in the opposite direction in which most of your equipment is designed to detect. Much like the example of the AOL customer service rep that we presented earlier, it is quite easy to convince a less-savvy computer user at an organization to click on a URL within an e-mail, open an e-mail attachment, or accept a file transfer from an unknown person on instant messaging (IM). The process is illustrated succinctly in Figure 6.3.

**Figure 6.3** Malicious Outbound Connections Can Lead to Information




The attack begins with a spoofed e-mail from the organization's IT team or upper management, usually sent to a wide distribution of employees (just to make

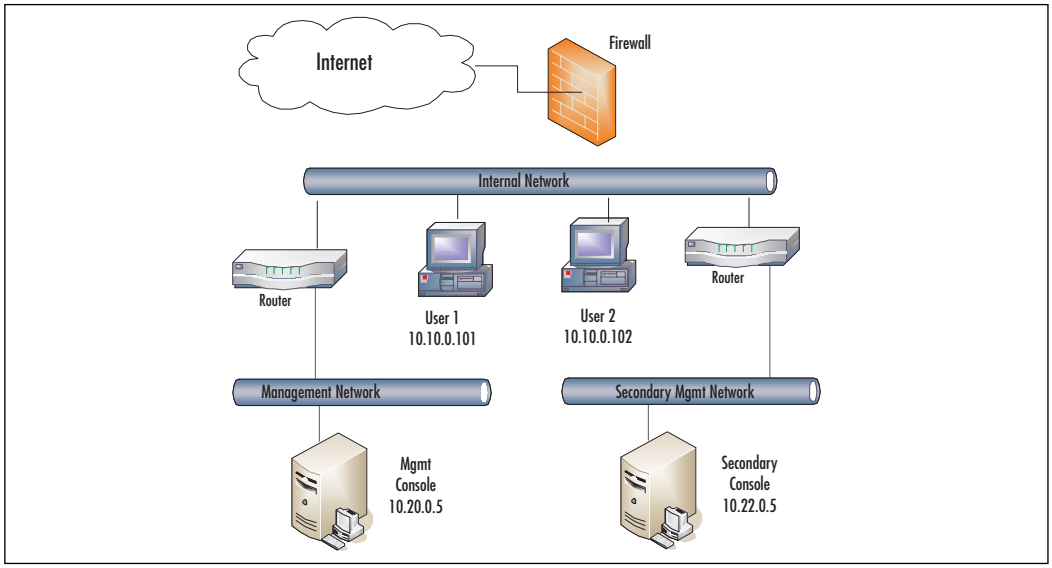
sure the attack works). The next phase involves convincing the user to click on the link, execute the attachment, or save the files sent via IM. Once this Trojan software installs itself, the attacker has remote control over the victim's machine. The attacker wastes no time, and runs a query of the customer database, but routed via the victim's computer, so that the database server believes that (and logs as such) the request is coming from the (assumed to be genuine) workstation. This, as you can imagine, can lead to a great deal of information disclosure and a huge public relations blemish should the newspapers find out about this.

So, what can be done about this and where do you use the highlighter on the topology map? You can put the highlighter away. There isn't just one conduit that might have malicious intentions; there is a potential for hundreds of attack vectors (one for each computer that sits on your internal, trusted segment). The key to mitigating this attack vector is employee education and a strongly enforced, written security policy for your network. If there is no business reason to be accepting file transfers from a stranger during business hours, make sure that this is not being done! If you have outsourced call centers to other countries, make sure they uphold the same high standards as you do at corporate headquarters. Stay vigilant!

## Plan for the Unexpected

Yes, we can hear the groans from here: nobody likes talking about disaster recovery or backup strategies, but when things go south, you don't want to tell the boss that you skipped that section of the chapter. If you're really going to invest the time and energy to create a secure network management infrastructure, you're going to want to add in redundancy wherever financial and time constraints will allow. Many of the products that we present later to manage and monitor your network can be purchased in a high-availability configuration, so that should one of the management stations fail, the other would pick up and continue to monitor your network and/or manage your network. As shown in Figure 6.4, you should attempt to place your redundant management platforms on diverse network segments, such that the demise of one upstream router does not knock out both monitoring stations.

**Figure 6.4** Redundant Management Stations on Diverse Network Segments




For more demanding monitoring needs, your organization can contract with third-party monitoring services (such as those provided by Keynote, www.keynote.com) that can check on the status of your externally facing equipment (such as Web servers, mail servers, and FTP sites) several times per minute and from different parts of the world. While your local management station might claim that your Web site is online, it might have different latency characteristics depending on your originating IP address. The real benefit here is if you are, for example, a multinational swimsuit company with Web order placement; it might be of interest to you that your site loads extremely slow from Thailand and is completely offline if you're in Australia. If you run a secure corporate network, it is much more important to know about some internal distribution-layer switch or router that failed. Third-party monitoring services will never be able to give you that level of detail because the devices are tucked away behind your border firewall.

Depending on how mission-critical your network management activities become, you might also want to invest in a secondary NOC, sometimes referred to as a "hot site" because it can be activated at a moment's notice and you can start managing your entire network from that location. If you were a nationwide insurance company with a centralized NOC that controls thousands of branch offices, you would definitely be interested in a secondary base of operations. If you are like most network administrators, with important but *not mission-critical*

network operations, you will be quite happy with some off-site data backup storage, and perhaps some drills to simulate network outages.

After the 9/11 attacks in New York, many financial customers of ours immediately began "hot site" projects, to make sure that they are ready should something of that magnitude happen again. In fact, one large financial institution is even running nationwide commercials showing off their multi-site operations center and redundant-powered data centers. Building your own "hot site" can be quite expensive, and you should probably consider going with a third party that provides these services for you.

Tools & Traps…

## Hot, Warm, or Cold?

A "hot site" is named that for the same reasons why "hot swappable" hard drives have that designation. The hard drives can be changed at a moment's notice and without rebooting. A hot site can be placed into operation in a matter of minutes, which is very comforting to the board of directors and shareholders. However, for this level of comfort, there is a great deal of cost. All information resources must be duplicated, and any database records that are updated need to be synchronized to the hot site almost instantaneously.

A "cold site" is one that has most of the infrastructure to take over network operations, but perhaps not any of the real high-ticket items (like large database servers). This is the least costly solution and works great when you just need a second base of operations online within a couple of days. This allows enough time for you to order off-site backup tapes to be delivered to the cold site, new equipment to be purchased, and network routing rules to change.

A nice middle ground to both of these options is a "warm site," which can come online within hours. As you can expect, the costs lay somewhere between the hot and cold sites, but the benefits are great. You can't just flick a switch and have all of your network operations move from New York to Iowa, but with a good deal of coordination, some courier-delivered backup tapes, and a lot of coffee, you should be able to pull off a company-saving miracle before dawn.

Continued

The costs involved in doing this yourself are rather high (unless you're of the Fortune 500 variety). Don't try to reinvent the wheel; seek the help of third-party companies that specialize in disaster recovery, such as VeriCenter (www.vericenter.com/products/disasterrecovery). They offer hot, warm, and cold sites, as well as other managed services.

In addition, the most mundane but often overlooked measure of redundancy is to make sure that any notification procedures used by your notification and network monitoring tools have multiple paths. This means that notifications shouldn't be e-mail only (what if the e-mail server is down?). Make sure that your notification options include telephone, alphanumeric pager, SMS cellular, FAX, and print-out options.

## Back Up Your Management, Too

While this is the least glamorous of the network management principles, it definitely has its place among the other four. Many times, we are aware of the sensitive nature of our customer database, our financial records, and other company-specific information stores. All of these will likely have a backup method and rotation that is far outside the scope of this book. However, what is often overlooked is the value—and indeed, the importance—of your network management systems. In case of disaster, you will certainly worry about your customers and other revenue-generating databases first. However, after the initial shock wears off, you will likely lament the loss of your network management system if you have failed to include it in your normal backup procedures.

Perhaps nightly backups are too cumbersome, but certainly monthly backups of your network management and monitoring systems are in order. The costs involved in adding your management stations to your existing backup jobs are nearly nonexistent. Even if you don't want to add the management systems to your regular backup, burning everything (system Registry settings and *init* scripts included) to a CD-R and taking it home with you certainly isn't an enormous amount of effort. This management principle is satisfied if you employ the use of hot/warm/cold sites, which practically require the backup of management systems along with the data-centric devices.

## Watch Your Back

The final suggestion, and the pinnacle of our principle pentagon (try to say that 10 times fast!), is a caution to "Watch Your Back!" At each stage in designing

your network management solution, consider a healthy dose of paranoia as your best yardstick. Your network management console will be able to monitor bandwidth as well as deactivate routes. With a flick of the mouse, you could quite easily (and hopefully accidentally) bring your network to a screeching halt. Therefore, you need to take an ounce of prevention in everything that you do regarding your management network. There's definitely a reason why we called the chapter "*Secure* Network Management."

## Authentication

The first part of a healthy paranoia is finding out whom you can trust. Put in network management terms, this means who are your authorized managers? If you're reading this chapter, certainly you probably fit into this short list, but who else should be allowed to control your network resources? Make sure to include people who can fill in for you when you are sick or away on vacation (okay, that last part was a joke; we know that you don't actually take vacation).

Once you have compiled this list, you have to determine how these people can be authenticated and how this authentication is embodied in the myriad of network management equipment available. As discussed previously, two-factor authentication is very attractive because it is hard to compromise. You not only need to know a username and a PIN, but also a temporary, ever-changing code that can only be obtained by physical possession of a key fob or calculator-sized token. The two-factor authentication server (in the case of the RSA SecurID system, the back-end is referred to as the "ACE Authentication Server") will make the determination as to whether the username + PIN + token code is genuine, but that is all it will do. Authentication is just a matter of saying you are who you say you are, but it does not allow you to do anything. That is the function of the *authorization* method you choose.

Even if you don't choose a two-factor system and decide to use password-based authentication instead, you still need a centralized server to store all this information. You're definitely not going to enjoy setting up (or removing) user accounts from all your managed devices, and you certainly don't want to use general-purpose accounts that are shared among a number of people. All managers should have their own login credentials so that audit trails and activity logs can actually have some meaning behind them, and so that we know who to point the finger at when things mysteriously stop working in the middle of the night. So, what's the best way to centralize all this information?

Most authentication vendors (be it the RSA ACE Authentication Server, or otherwise) will have a service or daemon that you can run on one of your less-used servers. This will accept the authentication requests and respond with a thumbs-up or a thumbs-down. Almost all of the solutions on the market today will support the RADIUS protocol, which allows for cross-vendor (and cross-platform) integration of billing technologies (and was originally developed for the big phone company in the early 1970s) and authentication. Using a RADIUS server (or more likely, a proprietary authentication server that speaks the RADIUS protocol), your individual network devices will be able to inter-communicate and decide on access to configuration functions. A similar, but incompatible, authentication protocol is TACACS+ (Terminal Access Controller Access Control System Plus), developed in June 1993 and documented in RFC 1492 (www.faqs.org/rfcs/rfc1492.html). TACACS+ (and its predecessor, TACACS without the +) has been all but replaced by RADIUS in most networks, with Cisco being the most notable hardware vendor that still has strong roots in TACACS+.

To use this centralized user authentication system, it's just a matter of configuring your network devices to forego their internal database of users and instead consult the local RADIUS or TACACS+ server for user logon requests. To enable TACACS+ on a Cisco 1720 router and have it consult the authentication server located at 192.2.0.22, the appropriate commands issued in configuration mode would be:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default tacacs+ enable
Router(config)# aaa authentication enable default tacacs+ enable
Router(config)# tacacs-server host 192.2.0.22
Router(config)# ip tacacs source-interface loopback0
```

This would instruct the router to contact the TACACS+ server at 192.2.0.22 for authentication duties during initial login (line two) as well as for entering privileged mode (line three, also called "enable mode"). If the TACACS+ server cannot be located, the authentication method will fall back on the standard Cisco IOS "enable" password.

RADIUS servers are available on almost all flavors of UNIX, Novell NetWare, and Microsoft Windows. You can even use some tools to integrate

directly with your Novell NDS (now called eDirectory) or Microsoft Active Directory directory services, thus eliminating the need to have separate accounts at all, and giving users the added benefit of single-sign-on (and no reason to forget their network management password).

Tools & Traps…

### And Liberty and RADIUS for All

It's not too hard to find a RADIUS server that will slip right into your existing network architecture without breaking the bank. If you are a Novell-centric organization, check out Novell BorderManager Authentication Services, which is a souped-up version of the Novell RADIUS Service for NDS announced in September 1997. Microsoft bundles a RADIUS server with its Internet Authentication Service, available in their Windows 2000 and Windows Server 2003 server products. And when in doubt, you can visit Funk Software and read up on Steel Belted RADIUS, their humorously named authentication server. They've been around since 1992 and have some very educational white papers available on their site, www.funksoftware.com.

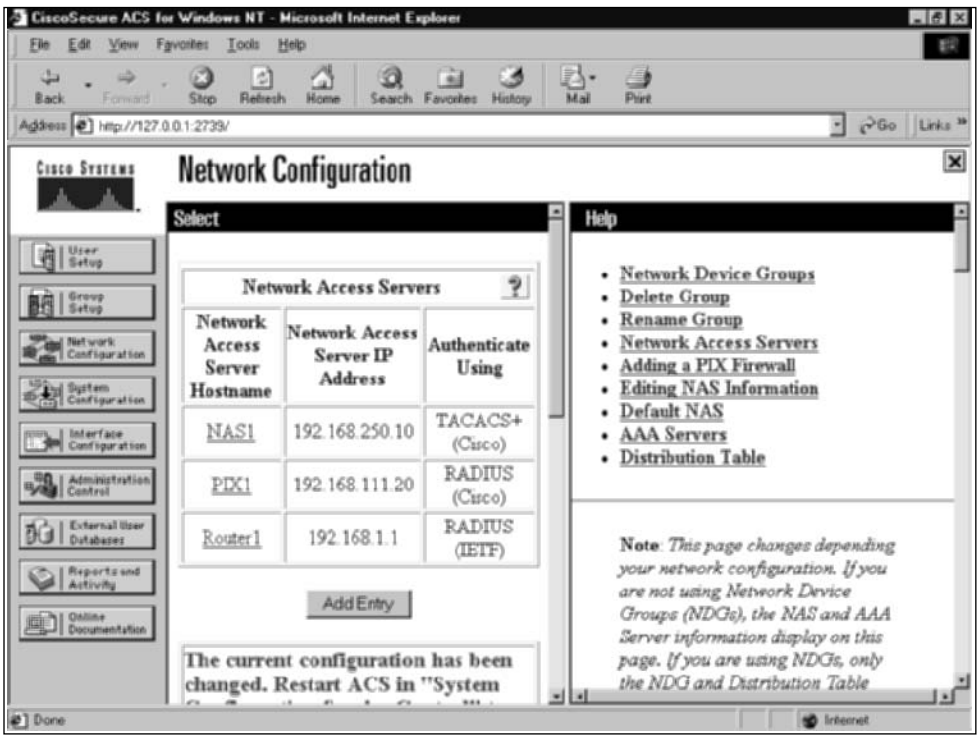
## Authorization

Once someone has established his identity to the satisfaction of your authentication server, the process of authorization begins. This is usually very simple and can be summarized succinctly: you're here, now what do you want? In most cases, such as the Cisco router configuration noted previously, the thumbs-up signal from the authentication server will just authorize the user to connect to the network device. Other times, the authentication server itself plays a bit of the authorization role, by storing certain access-level information and providing that to network devices when asked.

It is important to remember that it is the network device that is performing the authorization (in other words, allowing itself to be placed in configuration mode, etc.). The authentication server might provide hints as to the users' access levels, but it does not dictate them. The authorizing device must be willing to accept and enforce those hints. Using the Cisco Secure Access Control Server

(ACS), shown in Figure 6.5,you can set a user's privilege level 7, (for instance, 15 is the default, signifying full administrator, and 1 is the guest level of access) and thus restrict which commands he/she may issue on the router.

**Figure 6.5** Configuring Network Devices Using Secure ACS




# Encryption

The easiest piece of paranoia-avoidance to employ is also the most powerful. Encryption is so very critical to a network management strategy. We saw in Chapter 2 how easy it is to sniff packets off the network wire. What if, while you were using a network management tool to log in to a remote router, someone on your local subnet was able to intercept that password being transmitted during that telnet login session? Certainly, all the authentication and authorization schemes that you have worked so hard on will now be useless.

Nothing on your management network should be transmitted in clear text, if possible.You should never use telnet to log in to a router, firewall, or managed switch. Insist on using Secure Shell (SSH) for your management logins. If your network equipment doesn't support an encrypted management method, you

should demand this feature from your vendor. SSH should be used whenever telnet would have been used previously. Any management tasks that are performed using Simple Network Management Protocol (SNMP) should use a nondefault community string (in other words, not "public"), and you should strive to use SNMPv3, which includes encryption. If you are unable to use the newer SNMPv3, you should disable all read-write abilities within the SNMP agents, and use SNMP only for monitoring.

Even nonmanagement network traffic that traverses your management segment should be encrypted. This means that if your help desk system checks a POP mailbox for incoming tickets, you should be downloading this e-mail using POP3S (Post Office Protocol v3, via SSL/TLS) to protect your password as well as the contents of the e-mails. If your network operations team is fond of using instant messaging for quick communication with other engineers, make sure that they are using an enterprise version of these IM systems that provides for encryption, so that sensitive network configurations aren't discussed out in the open.

Tools & Traps…

## A Trillion Times Better

After seeing how easy it was (in Chapter 2) to eavesdrop on your network's data packets zooming by, you might be concerned that your IM software is also leaking valuable company information. In fact, it is, but not for the reasons you are thinking. While most folks know that e-mails can be read, inspected, or manipulated in transit, they seem to have made an assumption that IM messages are private (owing to the fact that there is no one central scary IT director to stand in their way). In reality, the network manager can easily read an IM session and perhaps capture more damaging information about the employee's love life, car troubles, and so forth.

If you must use IM products at work, you owe it to yourself to check out Cerulean Studios' Trillian product (www.ceruleanstudios.com). The intent of the software is to bring all your IM protocols together in one utility, to avoid running three sets of IM software. However, the best feature of Trillian is the ability to encrypt all AOL Instant Messenger (AIM) conversations, using what they refer to as SecureIM and 128-bit key

Continued

lengths. Using Trillian, you are free to comment to your network engineer across the country about network vulnerabilities that you have found, as well as transmit passwords (it's more secure than using the phone!).

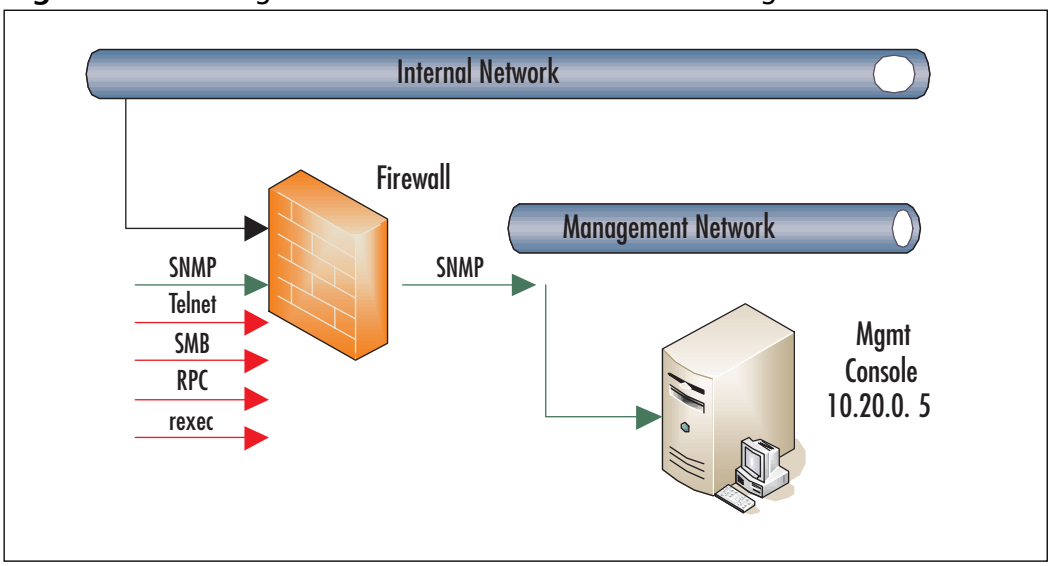
# Management Networks

In Chapter 3, "Selecting the Correct Firewall," you were introduced to the concept of a demilitarized zone (DMZ) or service network. This is where you should provision all of your servers that are going to need outside access. The reasoning is sound and simple: provide limited external access to a small segment of your network, rather than allowing potentially hostile traffic to enter the "inner sanctum" of your network fortress. In this fashion, any externally launched attacks can only be targeted toward DMZ machines, and any compromised machines in the DMZ will only be able to attack others in this screened subnet (assuming no access from the DMZ to the internal segment). Your external Web-browsing customers can still get to your content, but they can't *ping* the vice president's laptop.

The need to segment your network is paramount. If you are to provide proper management to the rest of the network, this special "control" network segment must be subject to very different rules than other segments are. As we learned in the previous section, encryption on the management network is very important. To be thorough, you would want to make sure to encrypt anything and everything on this network segment, preferably at the network transport layer. This means that you wouldn't have to worry about using telnet or other clear-text protocols because everything on that network would be encrypted. Not only will segmentation aid in defining the boundaries of this "encrypt everything" security policy, it will also greatly ease the creation of access control lists (ACLs) within routers at the edge of the management network.

The firewall (if possible) or router that you place between the internal network and the management network should be configured to only pass a discreet set of management protocols (SNMP, ICMP, etc.) to your management console(s) and only from predetermined management agents. Figure 6.6 depicts a properly filtered management network segment, blocking commonly used (and abused) file-sharing services, but allowing management data to flow to the consoles.

**Figure 6.6** Management Network with Firewall Blocking Nonessential Traffic




It is recommended to keep your management stations as dedicated consoles, and not used additionally as normal computers (for word processing, e-mail, or web-browsing activities). This also means keeping these machines off your Microsoft domain or Novell NDS tree. These machines should be pure network management and not dependant on your normal IT infrastructure. As stand-alone workstations, you can effectively close off all Microsoft SMB ports (135, 137, 139, 445) and really lock down that firewall policy to ensure security.

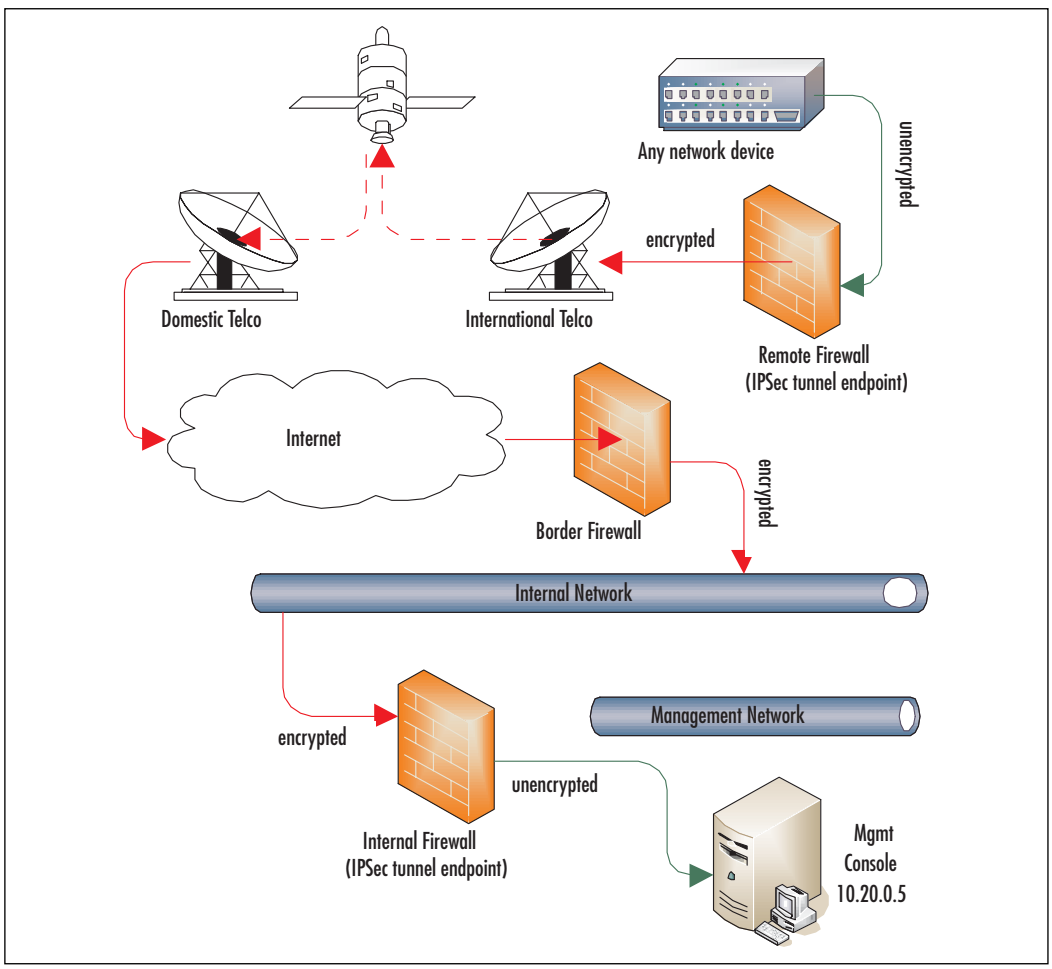
# IPSec and VPNs

The need for network-level security and encryption on your management segment is essential. The traffic on this network is sensitive by nature, so we must treat it with a different level of care than our usual internal network traffic. As mentioned in previous sections, encrypting the entire contents of this management network segment would be ideal. One way to achieve this goal is to use purpose-built commercial solutions that can divert all traffic through an encrypted tunnel, thus protecting the contents inside. Another solution, somewhat preferred due to the low costs involved, involves using the IP Security (IPSec) suite of protocols to ensure confidentiality and authenticity of network packets.

By performing its functionality at the network layer, IPSec is able to protect data transmissions without any modification to applications or clear-text proto-

cols that lie above the transport layer, and without any changes in the users' functionality. This flexibility is due to the fact that IPSec is an end-to-end encryption strategy; only the two endpoint computers need to be IPSec-aware. The routers, firewalls, and other devices that are along the path between the two do not need to understand (and preferably cannot) the IPSec traffic that is traversing through them. This allows IPSec to be run across very diverse network infrastructures—even over the Internet. You could use IPSec on your management station in California sending traffic to a DNS server in Hong Kong, and the routers and satellite signal relays between the two endpoints (including the ones that are under your control as well as the ones that belong to the ISP) would not have to be reconfigured, as shown in Figure 6.7.

**Figure 6.7** IPSec Tunnels Across Diverse Networks



# IPSec Modes and Protocols

This use for IPSec is called *transport mode*, in which two endpoints use TCP/IP and the data is secure from the originating machine all the way to the destination device. Another mode for IPSec is *tunnel mode*, in which the IPSec security is performed by the gateway devices nearest the endpoints, but not by the actual endpoints themselves. This is useful sometimes when the end devices are not intelligent enough to speak IPSec, but you still want to provide encryption services. There's no big mystery why it's called "tunnel mode"; the IPSec services on the gateway construct a virtual tunnel between itself and the other gateway, allowing client-to-client communications to flow in the tunnel away from eavesdropping.

As an added bonus, IPSec also allows for a rich set of message authentication, which means you can trust that the source machine identified in the TCP/IP headers is genuine and not spoofed. This is performed by the Authentication Header (AH) protocol, one of two protocols that implement the core IPSec encryption services. AH ensures the integrity of the header data by performing a cryptographic hash on the entire header block. On the receiving end, the same cryptographic hash is computed and compared to the one stored within the AH datagram, to detect if anything has changed in transit. If nobody has changed the headers, the message is genuine and can be trusted. Note that if you are behind a firewall performing NAT for your endpoints, the firewall will *by definition* change the source IP address (in other words, not maliciously), and that will make the AH hash fail. In that case, you would define the IPSec services in tunnel mode, terminating at your firewall (or not use AH). AH does not encrypt any data and thus does not provide confidentiality of your messages. The whole point of AH is proving that the message headers have not been tampered with.

The other major protocol is Encapsulating Security Payload (ESP), which can provide authentication and encryption services. The difference here is that the original TCP header is not authenticated (like in AH). Instead, the ESP header in transport mode is placed between the original header and the TCP header, thus protecting the data payload without fussing with the TCP header. This makes ESP especially useful for NAT-based networks, where the exterior header can and will be changed by the firewalls on either side.

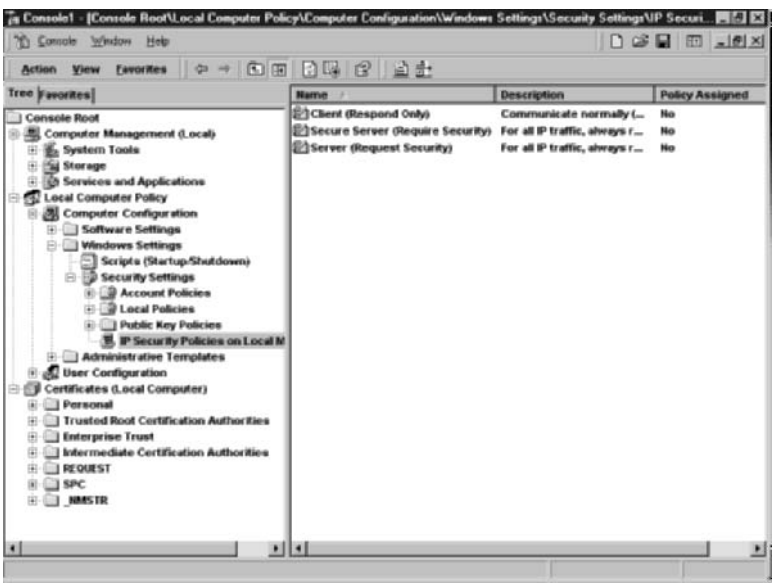
# IPSec Configuration Examples

We could spend the better part of an evening discussing the myriad ways to configure and deploy IPSec (trust us—we're a ton of fun at parties!), but we're going to concentrate on two examples that will present a good example on IPSec deployments. Consult your particular hardware vendor's documentation for more specific configuration steps.

## Windows 2000 Server

For Windows 2000 Server, an IPSec Policy Agent is built in to the operating system, making IPSec deployments quick and painless. Well, perhaps a little pain, but more of a paper cut than a knife wound. You can make light work of the IPSec configuration process by using one of the three built-in IPSec policies, or you can be really thorough and create your own. Begin by starting the Microsoft Management Console (MMC) named **Local Security Policy**, located under the **Administrative Tools** section of your Start menu. Along the left-hand side, you'll see the **IP Security Policies on Local Machine**. Once that is selected, you will see three built-in IPSec policies in the right pane of the window, as depicted in Figure 6.8.

**Figure 6.8** Windows 2000 Built-In IPSec Policies



Although you could start from scratch and roll your own policies, the three that are provided are more than enough to get you started. These predefined policies are bidirectional; if you attempt to connect to a non-IPSec machine after enabling one of these policies, the connection will fail. Make sure you troubleshoot all of your connectivity issues prior to tinkering with IPSec. Next, we will briefly examine all three policies.

- **Client (Respond Only)** This policy is used when you want your workstation to be willing to establish an IPSec connection, but only if the other machine requires it. This might come in handy if you are setting up a regular user's workstation. You could safely leave all the users at "Respond Only" and then just enable the file server to require IPSec. For our purposes in network management, we won't be using this policy extensively.
- **Secure Server (Require Security)** This policy is a lot more our style: forceful and demanding. If the other machine does not respond to the IPSec request or is too old to know what IPSec is, the connection will fail. In other words, this policy rigorously enforces encryption with the other network devices at all times. This is going to be the policy that we *want* to use, but it might not be the policy that we are *able* to use, depending on the rest of the network.
- **Server (Request Security)** The final built-in policy is (as you could have guessed) a compromise between the other two. This policy will cause the server to politely request an IPSec tunnel negotiation from the remote machine. If the negotiations fail or the other machine is not IPSec aware (such as Windows NT or Windows 95), an unsecured network session is established. This allows for greater flexibility while you're building up your secure management network and before all of your devices are IPSec capable.

## Windows Server 2003

Much of what was said in the previous section will apply for Windows Server 2003, which has virtually the same IPSec Policy Agent packaged with it. Some notable differences are that Win2003 will support the newer Triple Data Encryption Standard (3DES) by default, whereas Win2000 requires the High Encryption Pack or Service Pack 2 in order to support 3DES. Additionally, Win2000 only allows for Diffie-Hellman Group 1 and Group 2 key strengths,

which correspond to 768-bit and 1024-bit lengths, respectively. Win2003 adds the ability to use a 2048-bit key length.

**NOTE**

For more in-depth information on Microsoft Windows Server 2003, you will enjoy reading another book in the *Security Sage* series (and even if you don't enjoy books, you should buy this one anyway). *Security Sage's Guide to Attacking and Defending Windows Server 2003* by Erik Pace Birkholz, Joshua Leewarner, and Eric Schultze (ISBN: 1931836027) is an excellent resource for the busy CISO who needs more than just the basic installation and configuration information. If you have questions about the changes to the underlying OS security and how to best protect your Windows Server 2003 installations from compromise, this is the book for you.

## Cisco IOS Routers

With Cisco routers, there are no nicely predefined IPSec policies. All configuration must be done manually. However, the configuration itself is pretty straightforward, and the ability to configure and monitor absolutely everything involved with the IPSec tunnel setup, negotiation, and tear-down makes the IOS configuration tools very versatile. Although your exact configuration might vary from the example provided here, all of the steps that we will discuss will have to be performed regardless of individual IP addressing, and so forth.

The first step is to define the Internet Key Exchange (IKE) policy that the router will be using. IKE policies are the set of values that this network device is willing to use with another system. It helps to remember that this is a *list* of all the acceptable values on this router; when the remove device connects to the router, the negotiation occurs across this set of possibilities. In the following example, we set the encryption type to 3DES and the hash type to use the Secure Hash Algorithm (SHA). Then, we inform the router that the encryption will be based on a pre-shared secret (a common password that is used on both ends), and that the security association (SA) for this tunnel should last for one day (86,400 seconds):

```
router(config)# crypto isakmp policy 10
router(config-isakmp)# encryption 3des
router(config-isakmp)# hash sha
router(config-isakmp)# authentication pre-share
router(config-isakmp)# lifetime 86400
router(config-isakmp)# end
```

The next step is to actually specify that pre-shared secret that we're going to use on both endpoints of the IPSec tunnel. With these commands, you must specify the IP address of the remote router so that the correct pre-shared password can be used for encryption (here we specify passwords for two remote routers at two different branch offices):

```
router(config)# crypto isakmp identity address
router(config)# crypto isakmp key UCLAbruins address 192.2.231.12
router(config)# crypto isakmp key LAlakers address 192.2.112.3
```

So far, we've just done preparatory work. Now, the actual IPSec tunnel must be created. First, we need to define just *what* traffic should be encrypted. For our purposes, we want to encrypt everything flowing from the management network depicted in Figure 6.2 to our remote Los Angeles branch office:

```
router(config)# access-list 110 permit ip 10.20.0.0 0.0.0.255 host
192.2.231.0 0.0.0.255
```

Now we come to the final configuration step, which is very difficult to read and understand. The first group of commands is the "transform set," which defines the IPSec mode (tunnel) as well as the algorithms to be used with AH and ESP:

```
router(config)# crypto ipsec transform-set MyTransformSet ah-sha-hmac
esp-3des
router(config-ctypto-trans)# mode tunnel
router(config-ctypto-trans)# exit
```

Now that we have the encryption settings defined by the transform set, we need to make a set of attributes by linking a particular transform set with the appropriate remote network device and the address list (previously defined as ACL 110) that will trigger the IPSec tunnel to begin encryption:

```
router(config)# crypto map TheBigMapping 10 ipsec-isakmp
router(config-crypto-map)# match address 110
```

```
router(config-crypto-map)# set peer 192.2.231.12
router(config-crypto-map)# set transform-set MyTransformSet
router(config-crypto-map)# exit
```

Just when you thought you were done, there's just one more thing you have to do: assign this newly created crypto-map to one of the interfaces, hopefully the interface that will see all of the encrypted traffic:

```
router(config)# interface ethernet 0
router(config-if)# crypto map TheBigMapping
router(config-if)# exit
```

Whew, now that was a mouthful. Other network device vendors make this IPSec configuration process easier, so don't be scared away just because of the complexities involved in the Cisco IOS configuration steps. Whatever encryption solution you end up creating, make sure that you leave yourself some backdoor access to manage the IPSec settings. There is nothing more frustrating (trust us on this) than spending hours crafting a wonderful IPSec security architecture, and then locking yourself out of the remote branch office due to some silly error. Since you specified strict IPSec settings, the remote servers will not listen to you since you are unencrypted. Make sure to have an extra pair of hands near the remote machines while you are configuring the servers.

# Network Management Tools and Uses

And now, for our feature presentation: Bring out the tools! The heart of any good management network is the monitoring and management tools that you use. The mark of a good network management tool is one that has three out of the following four qualities:

- Reliability
- Ease of Use
- Flexibility/Configurability
- Reliability

And yes, we're not mistaken when we list reliability in there twice. If your management software can't be relied upon, then you might as well just not have it. The ideal solution is software where you just "set it and forget it" (much like the popular chicken rotisserie oven) and it provides you with timely alerts, easy management, and rock-solid stability.

Secondly, the ease of use for the software package that you decide on must be there. With other enterprise software deployments (like some CRM packages that we have endured), there is an extremely high learning curve, but they say that it's worth it in the end. The difference is that with network management software, there can be no learning curve. If it's going to take you 45 minutes to figure out how to get a detailed uptime report for a router that just lost its upstream connection, this software is of absolutely no value at all.

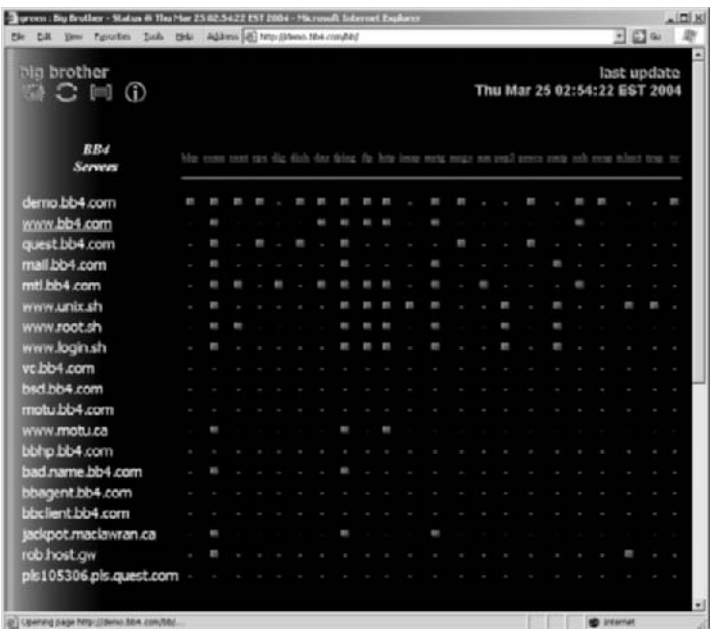
Lastly, the flexibility and configurability of your management solution should also factor into your selection. While any tool (even a DOS batch file) will work if you just want to PING a bunch of addresses, for those with more demanding needs, you're going to need a software package that will have the scalability to grow with your company. It must also have a rich feature set that is ready for tomorrow's management needs. You'll want to look "under the hood" and see if the particular software package that you're investigating stores data in a readily accessible database (MySQL, Microsoft SQL, Oracle) or if it uses a proprietary data format (or even worse—plain text flat file). Additionally, you want to note how many different methods the software package has to monitor your networks' health. While a simple ICMP PING is nice, it's hardly useful in today's locked-down networks. Make sure you can perform TCP port scanning, response time monitoring, custom HTTP query string checks, etc. If your budget allows for it, environmental monitoring would be a great thing to invest in now, and plug-in to the monitoring platform that you purchase.

## Big Brother

As with our other chapters, we like to start listing out the free or open-source tools first, so that you can try them out without getting a big budget approval process going. One of the perennial favorites in any discussion of network monitoring is Big Brother, now owned by Quest Software. Spending many years as a community-supported monitoring tool, Big Brother enjoys quite a following with over 2000 subscribers to their mailing list and over 200 custom monitoring plug-ins written by passionate users. Now, Quest Software supporting the product, a new version dubbed Big Brother Professional Edition has been released with the Professional Edition has enhanced diagnostics and a simplified installation routine. Much like other open-source software, sometimes getting the right version of the software for your particular CPU can be difficult. The Professional Edition includes a no-hassle installer, automatic configuration, and best of all, the comfort of telephone-based technical support in case you run into trouble.

While the user interface may be a bit simplistic (see Figure 6.9), it is also incredibly easy to understand. With its color-coded HTML display, it's hard to find a reason not to install Big Brother, at least at first. If you find that it fits your needs, great—continue on to chapter 7. If you still want some more features or configurability, continue onward to the following pages.

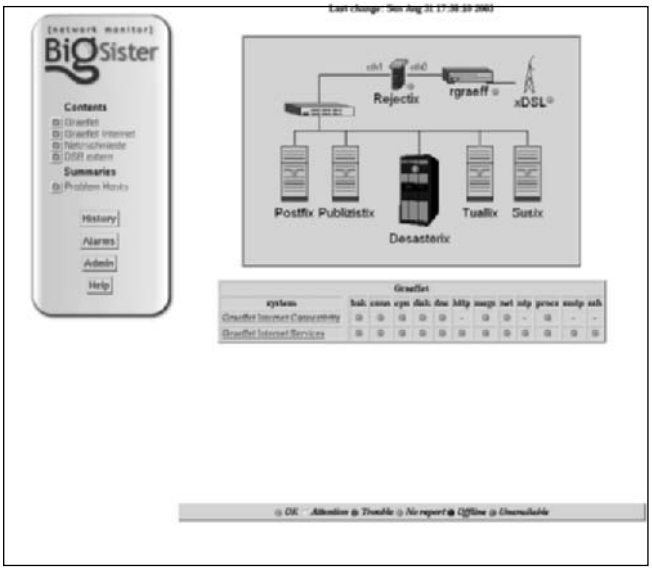
**Figure 6.9** Big Brother HTML status display




# Big Sister

Borrowing its name from the success of the Big Brother network monitor, Thomas Aeby from Switzerland wrote the Big Sister software to also provide basic network monitoring functionality in an open-source format. Version 0.99b1 was the most recent as of our publication date, and it has both a Windows binary as well as Unix distributions. For each item in its HTML output, you may drill-down into the details and see statistics and status down to the partition level for a monitored server. Changes in status (up and down) are maintained in a log for service-level agreement (SLA) monitoring. And, if you're a real Big Brother fan, you can even apply a stylesheet to Big Sister to make the entire interface appear like Big Brother.

**Figure 6.10** Big Sister Network Monitoring with Graphical Map



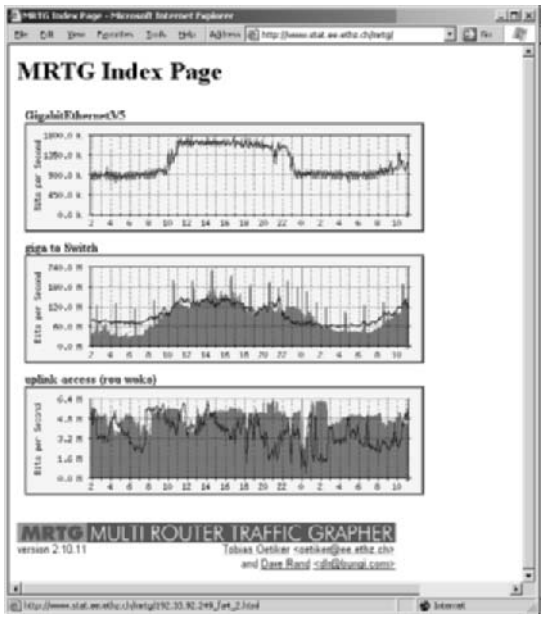

# MRTG

MRTG is one of the most versatile statistics graphing packages on the market. You can't walk into a network operators' group meeting without someone trying to show off their impressive connectivity backbone by using MRTG statistics and graphs. Chances are, even your ISP uses MRTG to monitor your dedicated Internet connection. There are certainly more expensive solutions, but MRTG is such a well-focused solution for basic monitoring and historical performance logging reasons, it is no wonder it has thousands of happy companies on its user list.

MRTG is based entirely on a PERL script that performs the SNMP polling of traffic counters. MRTG marries the real-time data from the SNMP requests to trending information on what has happened within the past day, week, month, and year. A lightweight C program logs all information, performs the trending calculations, and generates beautiful (at least in our mind) graphs that can be embedded in HTML for presentation to management or geeks alike.

Anything with an SNMP addressable counter can be used as an input for MRTG, so don't feel like you have to limit yourself to monitoring the outbound traffic on your company's Internet link (the most common use for MRTG). There have been some creative people that have turned MRTG into an early warning system for DDoS attacks on their IIS web farm, but just graphing the amount of web requests per second that the IIS web servers were taking.

**Figure 6.11** MRTG HTML Output showing router utilization statistics



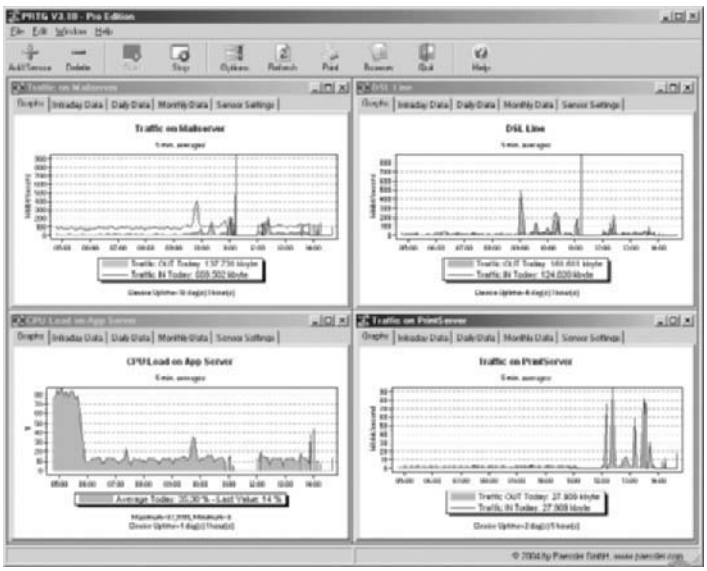

# Paessler PRTG

Borrowing on the same logic that Big Sister used with its Big Brother analog, the PRTG product from Paessler provides much the same functionality as MRTG, but with an easier installation process and a much simplified configuration interface. If you are installing on a Windows-based machine, PRTG is a better bet for you than MRTG because the former can install as an NT service under Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003. Combine this with the fact that you don't need to install your own PERL interpreter and PRTG starts sounding pretty good.

A free version of PRTG is available for non-commercial use and will do most of what any normal user could want in terms of monitoring and graphics. A Professional version of PRTG is available for only $49.95, and offers the ability to monitor unlimited amounts of devices and can customize the HTML reports that are presented to the user. PRTG maintains trending and statistics for up to one year, and can present hourly, daily, and weekly reports. Additionally, an automatic e-mail can be sent out nightly to keep the entire IT team abreast of the sensor usage statistics. Notifications can also be sent out when a certain threshold of usage (daily or monthly) has been exceeded. This is very useful for ISPs and

Web Hosting companies that sell their services under contract not to exceed a certain number of bytes transferred.

**Figure 6.12** PRTG HTML Output showing network utilization




Tools & Traps

### IPCheck Server Monitor

Paessler also makes IPCheck Server Monitor, which does more than PRTG can do in terms of monitoring. Furthermore, IPCheck has an advanced notification engine which PRTG itself lacks. IPCheck lacks the strong accounting features of PRTG, but it makes up for that in a very slick web-based user interface that is extremely easy to configure.

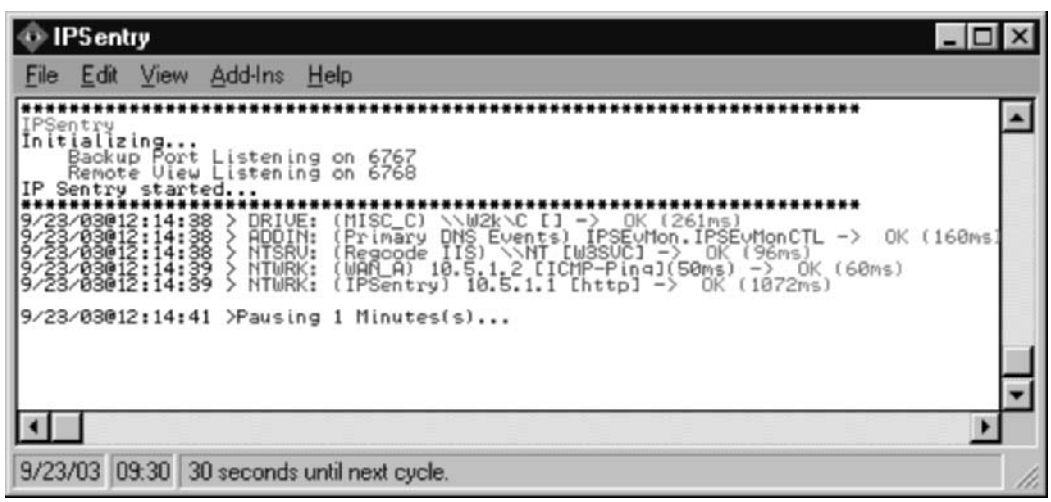
## IPsentry

A small step above open-source software is the realm of shareware software. IPSentry, by RGE Inc., is a simple network monitoring tool that concentrates

more on notification than on a graphical user interface with network maps. In fact, most of the IPsentry system is text-based. As you can see from Figure 6.13, the software will run through a battery of "checks" to run against predefined machines at a predefined schedule. For debugging purposes (as well as just plain nerdy fun), you can see exactly at what stage of the monitoring process the program is in, and the outcome of the monitored machines.

IPsentry is able to perform not only ICMP PINGs to determine if a remote host is alive, but also TCP open port monitoring, drive space monitoring, ODBC data source monitoring, NT event log monitoring, File content monitoring (looking for keywords in log files), and even third-party temperature probes to report environmental conditions. In terms of notification options, IPsentry does not disappoint. Along with standard e-mail messages, IPsentry is able to perform an audible notification using a pre-recorded .WAV file, SMS messaging on your cellular phone, launch an external application (presumably for further notification features), send an error report to your centralized SYSLOG server, restart the machine or the service, transmit an HTTP POST command, or even control the lights in the office (provided the lights are part of an existing X10 home management system). Through the use of plug-ins, IPsentry is able to quickly respond to the emerging needs of the small-to-medium business which cannot afford Unicenter, but are still willing to pay some money for software that is a cinch to install, configure, and use.

**Figure 6.13** IPSentry Shown Modeling Different Devices

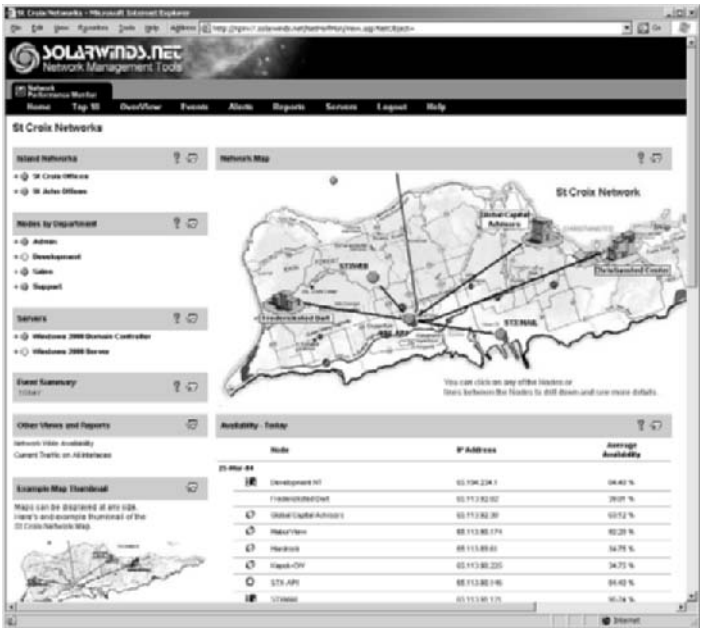


## SolarWinds Orion

Many network engineers have become familiar with SolarWinds by downloading the company's free Advanced Subnet Calculator and free TFTP server. Beyond their free products, SolarWinds offers a slew of networking tools that they've divided into nine separate categories, which they bundle into five different packages. Each package targets a different position, ranging from the system administrator to a ISP network engineer. For our purposes, we want to look at the "Orion" suite of utilities for network monitoring.

This powerful set of web-based monitoring tools definitely does not disappoint. While more pricey than the open-source alternatives (currently $2370 to monitor up to 100 devices), the money is well worth it in terms of a rich user interface and detailed reporting—down to the raw SNMP data that it is capturing. Network Computing magazine awarded Orion their Editor's Choice award for its "…uncluttered and flexible display show[ing] network status, diagnostic direction, and trends clearly and without requiring customization." Out of the box, Orion is able to perform PING as well as TCP sweeps of your network, and can report on bandwidth, CPU, Memory, and Disk Space utilization. With a completely customizable report writer interface, you can customize Orion to product details service level agreement (SLA) justification documents for your customers or management. You can also create an entire role-based access control system, so that you can give your more trusted IT employees the ability to login and view certain areas of the network, while not being able to edit some other areas. All together, we were quite intrigued by Solarwinds Orion. If you have a couple thousand dollars lying around, I think it would definitely be a wise purchasing decision.

**Figure 6.14** Solarwinds Orion Details Location Monitoring




# IPSwitch WhatsUp Gold

IPSwitch gained recognition by offering quality shareware before the Internet grew into a household word. Educational professionals and students probably recognize the name since IPSwitch produces the freeware FTP client program WS_FTP LE. WhatsUp Gold grew from an earlier IPSwitch offering, WS_Ping, a shareware utility that allowed network administrators to graphically map their network resources for scheduled ping sweeps or telnet access. Since its humble beginnings, IPSwitch has added a laundry list of features to the product that make it a logical choice for monitoring small to medium sized networks for which Computer Associates Unicenter or Hewlett-Packard OpenView would be overkill.

The original version of the product from 1996 monitored devices at the network layer of the OSI model, but the current version has monitoring abilities at the application layer for some popular databases and groupware applications. A powerful network profiling function can detect and create a map of all the TCP, NetBIOS, and IPX services (yes, even IPX) detected on the wire. As expected, WhatsUp Gold can produce all of the expected real-time alerts that we all hate to receive at 2 AM in the morning. With their most recent version 8.01, WhatsUp Gold has added a failover option, which automatically switches monitoring control to a secondary machine should the primary machine fail.

# Cisco Systems CiscoWorks

Cisco actually produces five versions of its CiscoWorks management software: IP Telephone Environment Monitor, LAN Management Solution, Routed WAN Management Solution, Small Network Management Solution, and VPN/Security Management Solution. Each bundle specializes in configuring and monitoring the devices in one of the previous five categories. Within the LAN Management Solution alone, there are six sub-components: nGenius Real Time Monitor, Device Fault Manager, Campus Manager, Resource Manager Essentials, CiscoView, and Common Services. This isn't a network management system for the faint of heart.

Unlike the other tools mentioned here, CiscoWorks only works with Cisco products. For campuses that have homogeneous Cisco networks, or even heterogeneous networks with a large number of Cisco devices, this suites of products make management much easier. CiscoWorks allows administrators to backup device configurations on their entire inventory of Cisco routers and switches, as well as roll out new configuration changes across the board. This sweeping power comes in handy when the next DDoS attack knocks on your door, and you need to apply very particular access control list (ACL) filters to all of your perimeter routers.

CiscoWorks also provides a wealth of statistics and health-monitoring functions for your Cisco devices and presents them in a way that is more easily digestible than a *show counters* command within the IOS software. Naturally, CiscoWorks provides real-time alerts in case we're sleeping during some of the really exciting network attacks.

## Computer Associates Unicenter

Computer Associates' Unicenter calls itself an Enterprise Management solution based on its capability. Since no network will contain everything that Unicenter can monitor, you purchase the core product and then purchase individual modules based on your network needs. For instance, Unicenter has Lotus Notes, Microsoft Exchange, and DB2 modules. Many of these modules do more than just monitor the health of systems. The Exchange module, for example, includes backup capabilities in addition to a full barrage of statistic monitoring.

Unicenter allows the IT Director to run the department as if it were a completely separate service business, mapping IT needs directly to Business costs and benefits. This helps immensely with the "business side" of justifying a server upgrade to the C-level management. Decisions can be made using a stack of historical performance metrics and TCO trending. If something happens on the network, Unicenter has numerous ways to get your attention in real-time. The real power, however, is in an intelligent event correlation engine, that can tell you whether the blast of a hundred SNMP failure alerts the NOC just received from retail stores all over Australia is really due to the single event of a distribution switch in Buenos Aires being restarted. Because of its support for industry-based standards such as SOAP, XML, and UDDI, Unicenter can be as extensible as you have the patience for it to be. IT can link to your custom point-of-sale cash registers in rural Minnesota, as well as your home-grown payroll software, with just the need for a lightweight API between them.

## Microsoft Systems Management Server

The Microsoft entry into the world of management and monitoring is more of a server-based management tool, than a network-centric one. Coming a long way from the version 2.0 release in May 1999, Microsoft Systems Management Server (SMS) 2003 has a massive amount of fixes and new features built in to the November 2003 release. SMS 2003 has an entirely re-worked GUI client, new *server roles* for easy one-click deployment, integrated reporting, and a healthy dose of stability (remember how we harped on reliability a few page ago?). While,

sadly, Microsoft has now removed support for Novell NetWare (along with eight others) in the list of OSes that SMS will attempt to manage, we still think that this is a solid management tool for networks that are mostly Windows-based.

SMS allows you to perform true asset-based management of your large enterprise network, collecting a bunch of inventory data in one place to bring smiles to the faces of your auditors. Using Windows Management Instrumentation (WMI), you can drill down to a crazy amount of detail for each managed resource, including BIOS chip revision and chassis enclosure data (if supported by your CMOS). SMS allows for detailed software metering, to ensure that not only are you not exceeding your software licenses, but that you also don't over-purchase licenses for software that is underutilized.

Notes from the Underground…

### Microsoft System Center 2005

Still in development, Microsoft is definitely positioning all of its enterprise management tools and software to end up being plug-ins to the Microsoft System Center 2005, to be released sometime during 2005 (we hope). As part of their Dynamic Systems Initiative, Microsoft hopes that System Center 2005 can bring together all of your management resources into one view, "reduce the total cost of ownership for IT investments", and virtually eliminate the manual operational tasks that contribute to configuration errors, "…the underlying cause of failure more than 50% of the time."

The behemoth that will be named System Center 2005 will be comprised of SMS 2003, the OS Feature Pack, the Device Management Feature Pack, the Administration Feature Pack, Microsoft Operating Manager (MOM) 2005, and the System Center Reporting Server. They will also have a lighter version called MOM 2005 Express, which has most of the functionality of MOM but targeted for smaller environments.

## Hewlett-Packard OpenView

OPenView is the management product that needs no introduction. Arguably, HP OpenView sets the standard for network management with plug-ins for virtually

any device or application currently in use in enterprise networks today. This device fills the same niche as CA Unicenter, though it arguably has better name recognition. Any large network with 24/7 operations needs to give this package a serious look. Of course, you do not purchase this product lightly. Due to the extensive modules, you need to plan the purchase carefully to make sure that you have all of the necessary systems covered. As many people mistake the stack of manuals for a phonebook of the United States, taking a week long class to use this product will make sense, especially since this package costs tens of thousands of dollars.

Tools & Traps…

## Eyeballs in the NOC

While outside the scope of this chapter, we did want to mention an excellent monitoring hardware appliance called WallBotz from a company called NetBotz. These little devices (you almost want to say "cute") are about the size of a VHS cassette and have a ton of functionality packed in them. They come with an on-board surveillance camera, many environmental sensors, and an RJ45 on the side. Plug them in, give them an IP address, and ta-dah! You can now monitor the inside of your server room *racks* with just an HTTP session. Attach a dry contact sensor and you can get emailed every time the rack door opens. After getting the email, just a quick trip over to the web browser and you can actually *watch* the technician as he corrupts your database after-hours.

Newer versions allow you to zoom the camera lens in and out, as well as pan/tilt the camera head with an amazing video capture rate of 30 frames per second, at 1280 x 1024 in stunning 24-bit color. A full complement of temperature, air flow, humidity, amperage, and fluid sensors can be purchased and plugged right into each WallBotz. A small microphone built-in to the camera housing allows you to even listen in on the conversations happening in the NOC. This is truly one toy that I hope to get in my Christmas stocking this year—can't wait to set one up inside my fridge and catch whoever is stealing my Butterfinger bars. Stop by at www.netbotz.com to find out more information, or to purchase me one of these units.

# Checklist

- ☑ Know what you have.
- ☑ Control Access Vectors
- ☑ Plan for the unexpected.
- ☑ Backup your Management Data
- ☑ Watch your back.
- ☑ Always use encryption
- ☑ Plan your management network.
- ☑ Plan for a redundant management network or hot site.
- ☑ Use an end-to-end encryption method like IPSec.
- ☑ Start with the free tools, and then work your way up the ladder.

# Summary

While Network Management might not be the most interesting topic of the many that we will present throughout the course of this book, it is the one that reflect on a year from now, after you've turned your hodgepodge collection of standalone workstations into a well-connected, properly segmented and firewalled enterprise network. Once you have the infrastructure in place and the means by which to diligently monitor and proactively manage the network, you can lean back in your chair, remember what a smile felt like, and slide a stack of network performance statistics over to your CEO.

Using the five basic network management and security principles, we can construct a framework for designing and implementing our new, secure network management center. Once we have a good idea of what we have in our very own network, we can begin to classify and categorize devices, users, and access control lists. By controlling access vectors, we can cast a watchful eye towards the most likely network invasion conduits and hopefully stop them from growing out of control. If we plan for the unexpected we can rest easy at night, knowing that two sets of monitoring equipment are making sure that your company's vital operations are still running strong, even in the middle of the night. After taking the time and effort to create this elegant management system, the last thing you want to do is see all of that torn down by the next big tornado, earthquake, or theft. If you backup your management data at least half as often as your customer data, you would sleep better at night too. Finally, watch your back. Use layered encryption (or the built-in encryption of your network monitoring protocol) to protect against eavesdropping. In this fashion, you protect against discovery of the service port being open, as well as the contents of the message sent.

Take the time now to design a separate management network, away from the general user population on the internal segment. This is extremely important due to the sensitive nature of the data being transmitted back and forth. Encryption

on the entire network segment is not a bad idea either. With dedicated management consoles on the management network, you will be able to parade the venture capitalists through the room without worrying about the impression it may make on them.

IPSec is a great tool that helps hide the contents of your message while they are in transit. The pre-defined policies in Windows 2000 or 2003 are most definitely preferred, as they are less prone to error and likely to be a good fit. For those network devices that can perform the IPSec encryption themselves, attempt to perform encryption from the originating management console to the remote network device. Cisco has a step-by-step discussion of their IPSec implementation, so help is available.

Once your network infrastructure is in place, you're ready to install all the exciting network monitoring and management software that your wallet can afford. Starting out with something small, inexpensive, and uncomplicated is a good strategy. As you find yourself bumping up against the limits of the software's capabilities, you need to purchase one of the more expensive and robust application product suites. Your choice in network monitoring software should consider the support structure in place behind some of these open-source companies. You want to make sure the same company is going to be around next month when your network goes down and you need to track down an old router configuration. Back up all of your network management data just like your customer data, but you can feel free to do it less frequently. A good rule of thumb is to take a backup image whenever a router configuration or other critical monitoring device is changed, and then just store that CD off-site.

Intermission is over! Now onwards to the wonderful world of Network Switching in Chapter 7.

# Solutions Fast Track

## Network Management and Security Principles

- ☑ **Knowing What You Have** Without a good idea of what you're in charge of managing, you have little hope of effectively controlling.
- ☑ **Control Access Vectors** Know where your enemy will strike from, and fortify those locations.
- ☑ **Plan for the Unexpected** If you have the ability to afford redundant networks and management consoles, implement them! When the downtime hits (and you know it will), you will at least prove due diligence.

- ☑ **Backup Management Data** Remember to backup your valuable management information; in case there is tragic loss of building or property, you'll be able to land on your feet at a different location.
- ☑ **Watch Your Back** There are malicious people out there and there are casual sniffers, but both groups are out to get your passwords. Make them work for it; encrypt all your network management communications.

## Management Networks

- ☑ Segregate your network management activities on to its very own segment
- ☑ You will be able to keep an eye on network health without worrying about internally initiated attacks

## IPSec and VPNs

- ☑ **IPSec Purpose in a Management Network** Not only does IPSec assist in providing confidentiality to your clear-text protocol traffic, it also allows you to mask any open port activity by hiding everything within the tunnel.
- ☑ **IPSec Modes and Protocols** Depending on the capabilities of your network devices, you can either perform end-to-end encryption (preferred) or have the gateways nearest to the devices perform the encryption on behalf of the devices.
- ☑ **IPSec Configuration Examples** Windows 2000 and 2003 make the IPSec task simple with predefined policies. Cisco is much more configurable, but has a much steeper learning curve.

## Network Management Tools and Uses

- ☑ **Reliability** If you have to spend time monitoring your management software, it just isn't useful anymore.
- ☑ **Ease of Use** Spending hours to figure out the user interface of a complex management system completely ruins your ability to respond to network outages in a timely fashion.
- ☑ **Flexibility/Configuratbility** Your network management software needs to grow along with your organziation

# Links to Sites

- **http://nsa2.www.conxion.com/win2k/guides/w2k-20.pdf** National Security Agency guide to setting up and properly configuring Windows 2000 IPSec services.
- **www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp** Microsoft's step-by-step guide to IPSec (including planning and deployment methodologies).
- **www.blueridgenetworks.com** Blue Ridge Networks makes commercial end-to-end encryption tunneling products, like their CryptoServer.
- **www.openview.hp.com** HP OpenView network management suite.
- **www.ca.com/etrust** Computer Associates eTrust Security Command Center.
- **www.ipsentry.com** RGE, Inc. IPSentry network monitoring software.
- **www.bb4.com** Big Brother flexible network monitoring.
- **http://bigsister.graeff.com** Big Sister network monitoring.
- **http://people.ee.ethz.ch/~oetiker/webtools/mrtg/** Multi Router Traffic Grapher (MRTG).
- **www.paessler.com/prtg** Paessler Router Traffic Grapher.
- **www.paessler.com/ipcheck** Paessler IP Check Server Monitor.
- **www.solarwinds.net/Orion/** Solarwinds Network Monitoring software.
- **www.cisco.com/en/US/products/sw/netmgtsw/** CiscoWorks Network Management software
- **www.cai.com/unicenter/** Computer Associates Unicenter
- **www.microsoft.com/smserver** Microsoft Systems Management Server (SMS) 2003
- **http://csrc.nist.gov/CryptoToolkit/aes/rijndael/** Advanced Encryption Standard (AES); Rjindael.
- **www.rsasecurity.com/products/securid/** RSA SecurID two-factor authentication.
- **www.cryptocard.com** Cryptocard two-factor authentication.
- **www.authenex.com** Authenex two-factor authentication.

- **www.activcard.com/products/tokens.html** ActivCard two-factor authentication.
- **www.wardriving.com** Information on wireless local area network (WLAN) eavesdropping.
- **www.shiva.com** Legacy dial-up modem pools.
- **www.vericenter.com/products/disasterrecovery** Disaster Recovery "hot sites."
- **www.netbotz.com** NetBotz WallBotz server room monitoring devices
- **www.solarwinds.net** Solarwindws Network Management suite of applications

# Mailing Lists

- **www.nanog.org/mailinglist.html** North American Network Operators' Group
- **www.canog.org** Canadian Network Operators' Group
- **www.swinog.ch** Swiss Network Operators' Group
- **www.frnog.org** French Network Operators' Group
- **www.sanog.org** South Asian Network Operators' Group
- **www.afnog.org** African Network Operators' Group
- **http://list.waikato.ac.nz/mailman/listinfo/nznog** New Zealand Network Operators' Group
- **www.mplsrc.com/mplsops.shtml** Great resource for people involved in large, MPLS networks
- **http://listserv.nd.edu/cgi-bin/wa?SUBED1=resnet-l&A=1** Must-read information for anyone in charge of a University's Residential Housing Network

# Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

**Q:** It seems like a ton of work to setup dedicated management networks (in some cases you even recommend redundant management networks) and dedicated management consoles. I can just load up my trusty Sam Spade utility and troubleshoot whatever I need on my laptop. What's the point?

**A:** Listen, we're not going to pretend that everyone reading this book is going to run out and implement all of the suggestions. Moreover, a management network when your "enterprise" consists of about 20 machines is complete overkill. But once you get to the point where you need to worry about multiple internal routers, multiple internal segments, several Class-C blocks' worth of user workstations, and some site-to-site VPN connections, you really owe it to yourself to invest in a management infrastructure that begins with a separate network and a dedicated console.

**Q:** Okay, you've sold me on the management network, but I don't see why I need to waste money on a dedicated management console. Why can't I just have my Network Engineer's computer be designated as the management console?

**A:** Well, one reason is because we told you not to, but that answer never worked real well with your parents either. The main reason is for separation of duties. While your network engineer might be primarily responsible for the uptime of the network, what happens when he/she steps out to lunch and locks their workstation (as all good security-conscious users should do)? A router went down in Duluth and instead of fixing the problem, you're trying to crowbar your way past the engineer's workstation lock. Then what happens when the engineer goes on Jury Duty? Are you going to make that person change their password before they leave, and change it back? Should they just write their password on a sticky-note and put it on the screen? You can see where we're going with this one, and you should really consider that with prices for reliable desktop computers sliding well south of $1000, it's a no-brainer.

**Q:** How often should I backup my Management Network data?

**A:** Excellent question with an easy answer: as often as the data changes. In most networks, the router configurations, topology layout, and routing tables are fairly static over several months. If this describes your network, I would just backup each time you had a change in configuration or routing or anything else that has a material effect on your ability to manage and monitor your network. If the only thing that changes about your network management is your log files, we would suggest moving those logs onto a dedicated SYSLOG server, and backing up that server nightly along with the rest of your dynamic data.

**Q:** Should I place my wireless access points in front of, behind, or parallel with my corporate firewall? I've heard arguments for all three, but since you're the experts I'm going to ask you.

**A:** Although it sounds tempting and is very convenient, we're going to strongly urge that you do *not* put your wireless access points behind your firewall. You just don't want to invite that level of risk into your sphere of influence. Treat your wireless segments just like hotel broadband access; allow people to connect and receive a DHCP address, but they can only access the Internet after agreeing to a boilerplate end-user license agreement and entering in their employee ID and password. This just gets them on to the Internet, however. If they want access to their network file share, they need to use their VPN client just as if they were connecting from home or a hotel room. In this manner, you protect yourself from wardrivers that just want to use you for free Internet, plus, you stop people from inadvertently creating a conduit from the airwaves directly to your Oracle Financials server.

**Q:** The IPSec section of the chapter frightens me; is this level of encryption really necessary is all I want to do is monitor the bandwidth pumping through our core routers?

**A:** Absolutely! Do you think we would write all of this if it were optional? Okay, you're right—we probably would, but you should still implement IPSec. Even when you are using encrypted protocols such as SSH, you still give away information to a potential attacker about the methods in which you manage the network. If they see a lot of port 22 activity from you machine to a router, they can safely assume that the router has an SSH daemon listening. In contrast, IPSec tunnels all the communication such that anyone sniffing on the wire would only be able to see the tunnel itself and not any data inside.