Chapter 2

Windows 2000 DMZ Design

Solutions in this chapter:

- **Introducing Windows 2000 DMZ Security**
- **Building a Windows 2000 DMZ**
- **Windows 2000 DMZ Design Planning List**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

Microsoft has taken great strides in the past few years to enhance its security posture. Windows 2000 is only as secure as you can make it, so it's very important that you follow this chapter closely; everything you learn here will be used in the demilitarized zone (DMZ) of your network. In Chapter 1 we learned the fundamental security concepts revolving around the DMZ, what the DMZ is, and how to design a basic DMZ with traffic flows. In this chapter we now start to populate the DMZ with systems and the specifics of designing those systems to work within the DMZ. From Chapter 1, you'll recall what you learned about the basic DMZ and its overall reason for existence as well as its basic design. Here we cover how to design a Windows 2000-based network solution that will work within and around the DMZ segment. It's important to know this information as a security administrator or engineer because the DMZ (as you are now starting to see) can be very complex to work with and around. It will get even more complex as we move through this book. Building on the content of Chapter 1, this chapter shows you how to use your Windows systems within the DMZ design.

In this chapter you learn about Windows 2000 security but only as it relates to this subject matter. In other words, this chapter is not a general Windows 2000 security chapter, but rather is one customized to fit the needs of designing security within the DMZ. Of course, the chapter covers many security topics revolving around Windows 2000, but all the content will be tailored for the most part to security administrators working within a DMZ environment.

This chapter can serve as a rough design document to help you place your Windows 2000 systems and the services they run within the DMZ. Many administrators wonder how to place their systems within the DMZ, especially when those systems are Web or FTP servers facing the Internet and publicly accessible. It can be nerve shattering, especially with all the past publicity about Microsoft being an insecure system with many bugs, unchecked buffers, and a plethora of other problems, resulting in its products becoming the biggest target on the Internet today. This chapter (and following chapters) will remedy those fears by providing you with the answers and solutions you need to not only place the systems in and around the DMZ but also to protect them.

In this chapter we cover the basics of Windows 2000 DMZ security and introduce to you the proper placement of systems in and around it. (Chapter 13 and Appendix A focus entirely on how to lock down and harden Windows 2000 and other services such as IIS, so if you are only looking to harden systems, you might want to jump directly to those sections of the book.)

NOTE

If you are looking for a book on how to harden and implement security with Windows 2000 in more granular detail without a focus on the DMZ segment, you can check out these other Syngress titles:

- *Hack Proofing Windows 2000 Server* (ISBN: 1931836493)
- *MCSE/MCSA Implementing and Administering Security in a Windows 2000 Network: Study Guide and DVD Training System (Exam 70-214)* (ISBN: 1931836841)

Introducing Windows 2000 DMZ Security

In this section we take a broad look at security concepts for Windows 2000 systems, tailoring all the content to DMZ-based hosts. This section of the chapter covers the following details:

- Fundamental Windows 2000 DMZ design
- Windows 2000 DMZ bastion hosts design
- Engineering Windows 2000 traffic in the DMZ

An introduction to Windows 2000 DMZ security must start with a general discussion of the concepts of applying a secure foundation to the core services running within the DMZ, all based on the Microsoft product line. When discussing Windows 2000-based security in the DMZ, we need to look at a few general concepts. What will be publicly accessible? Why do you need these services available? How will you control access to and from such resources? How will you maintain these services? Everything else is all about hardening the systems. Here we look at the general design. Remember, DMZs are the best place for you to place and secure your publicly used information and services such as an e-commerce site, a Web site, an FTP site, VPN-based services, and so on. In this chapter we look at proper placement of these needed services.

In this section of the chapter we also look at basic Windows 2000 DMZ bastion host design. This is really about placement of servers and why you would place them in specific spots on your network. Again, this is just placement; if you need to learn more granular details, turn to Chapter 13 to learn how to lock down the Windows 2000 OS to be placed on the DMZ.

The last section discusses basic traffic flows and the services and protocols Microsoft products use. With this information, you can design your systems so that all needed traffic will go through the firewalls, as well as preventing traffic that you do not want to go through the firewall. In later chapters, we show you how to configure those firewalls

to allow the traffic to pass; you can come back to this chapter to get the data you need (such as port numbers for access control lists) to engineer your solution. As mentioned before, you need to read this book in its entirety to be able to complete your solution if you are not sure what to do at all, but if you have a Cisco PIX firewall that you need to implement with a Windows 2000 IIS 5.0 Server, you can probably just read this chapter, the PIX chapter (Chapter 5), and the chapter on how to secure Windows 2000 bastion hosts on the DMZ segment (Chapter 13).

Remember, you need to understand three very important concepts: why you are building a DMZ, where to place specific services, and how to engineer the traffic to and from those services. After that, you can worry about locking down those individual systems.

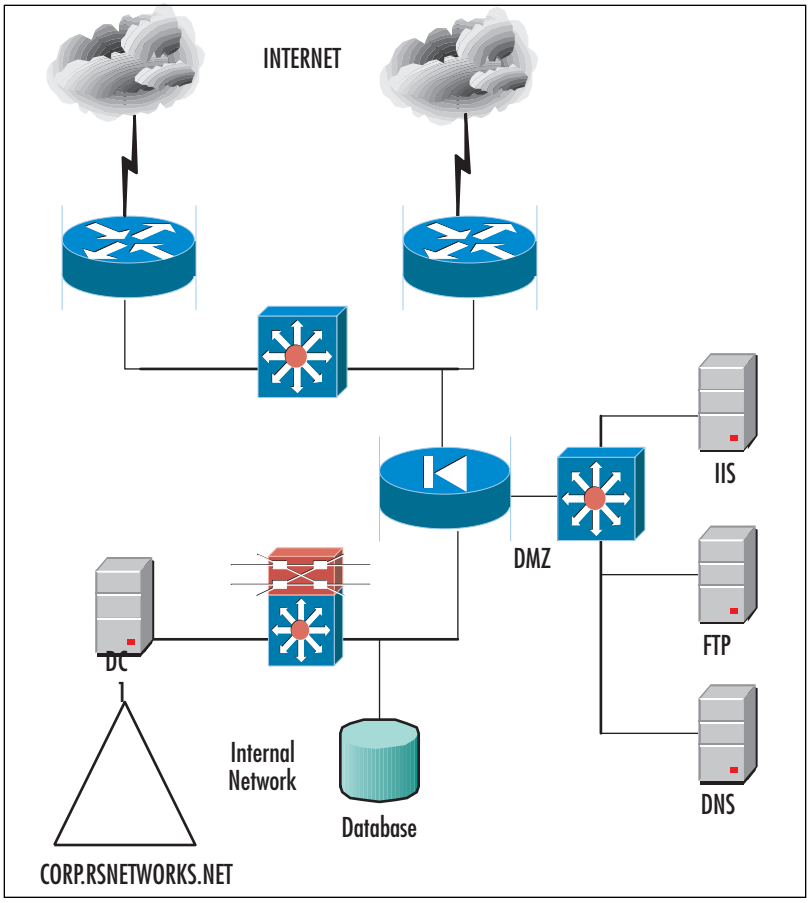
Fundamental Windows 2000 DMZ Design

Before we look at the fundamentals of securing the DMZ segment and its hosts, we need a general idea of what it's going to look like on a map. All good network designers plan the topology (hopefully with a topology map) and figure out in advance traffic flows, logical addressing, and any other factors that would affect the systems planned operation. If you choose not to follow this recommendation, you could find yourself very discouraged when the network does not function properly and systems cannot be accessed due to a simple (or complex) mistake you made in the design. A DMZ segment can be one of the most complicated segments on the network that you can design and implement. When you add Windows 2000 to the mix, you not only have to be an expert in security—you also must be an expert in network engineering, Windows 2000 system design, and the services to be made available. Look at it from this point of view: You want to set up a DMZ segment with a PIX firewall and a Windows 2000-based Web server. This should not be a complicated task in your mind, but think of all the areas you need to focus on:

- Network engineering
- Systems engineering
- Security analysis

Now take a look at Figure 2.1, which points out all three of these areas.

Figure 2.1 Fundamental DMZ Design



The reason we have segmented this figure into three sections is that it represents how you should design each section. Let's take a look at each section in more granular detail.

NOTE

In Figure 2.1, note also the use of high availability in your design. If your resources need to be in high demand, it is critical that you design high-availability features so that you can keep your services available in time of disaster. Here you can see the need for firewalls, redundant routers, and Internet connections to different points of presence (POPs), highly available Web services, and database services. Never rule out high availability for your solution if you can afford to implement it.

Network Engineering the DMZ

Your first step in designing a Windows 2000-based DMZ is to select all the networking hardware you will need. You must do an assessment of your needs to figure out what the hardware infrastructure will cost your company. You need to look at your *needs* first. When you are looking at the networking end of it, you should ask yourself, "What devices will I need, and how should I scale them?" Exploring these questions will bring answers based on networking gear and its cost. Since we've already mentioned Cisco, let's stick with that company's products for this example. In Figure 2.1 we looked at a very basic network infrastructure, but the needs are quite high for the future, so let's say that we decide to scale up the network hardware. We interviewed all departments that are part of the project to design and implement a DMZ infrastructure with an IIS Web server. After talking to everyone involved, we came up with a few important items:

1. We need to scale up the number of connections to the Internet, since the VPN services, external DNS, and other services will be added sooner than later. For this reason, we might need to have more port availability on our switch that is publicly accessible via the Internet.
2. We need to add more bandwidth and site-to-site VPN services off the external Internet routers. This need will become critical next year. This tells us that we had better not skimp on the Internet-facing routers and make sure that we purchase models that either have crypto cards (to use IPSec for VPNs) installed or that are upgradeable to them.
3. We need to eventually set up a load-balanced solution with multiple IIS servers and a possible backend database cluster. This tells us that we will need to scale the firewall, switches, and all other infrastructure to meet the needs for a possible e-commerce site, a load-balanced cluster, and so on.

Can you see why you must really plan this project out very well? There is nothing more frustrating than having to constantly replace equipment because you have not anticipated future needs and requirements. It always winds up costing more in the long run, so make sure that you do a solid needs assessment up front and scale your design to what you might need in the future.

NOTE

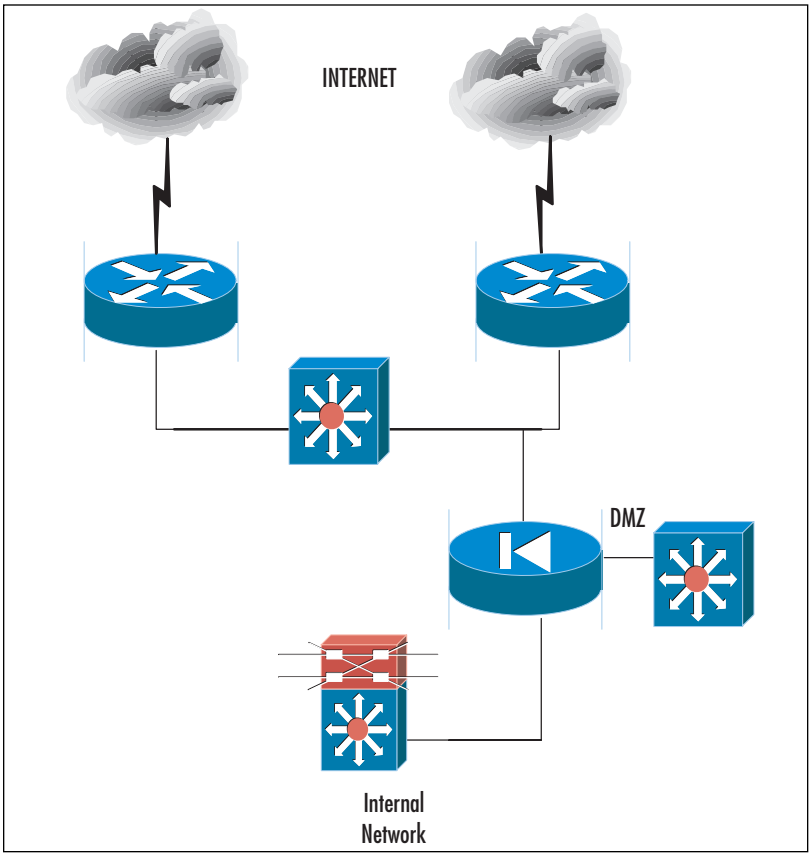
Even if your management team or project stakeholders decide it's not in the best interest of the project, organization, or the IT group to scale up or out resources (which adds immensely to the cost of the project), at least they'll know you brought it up—and when the need comes up in the future (as it usually will), it is on record that you at least tried!

Now you have done a complete needs analysis and have designed the infrastructure. (The initial design is shown in Figure 2.1.) You have noted that a redundant firewall should be used to ease the pain of failure as well as your scaling requirements. The management team responsible for purchasing and approving this design has stated that all is approved except the redundant firewall, which will be considered and purchased at a later date.

Now the network segment is designed, and after you run a test (maybe even a pilot or prototype), you are ready to implement it. Again, this chapter focuses on overall design. Since this book was written with all types of systems in mind, you can replace that firewall (currently PIX) with a Nokia firewall, a Check Point firewall of Microsoft ISA 2000. This book allows for that flexibility in design so that you can pretty much replace that firewall with whatever you are currently using or plan to use. We look at the specifics of adding rules and so on in later chapters.

Now that you have an idea of network design, let's continue with our plan to design it. Take a look at Figure 2.2.

Figure 2.2 Network Design of the DMZ



Since you have already selected your vendor's product line (Cisco) and have your needs analysis done, you can lay out your infrastructure. In Figure 2.2 you see that we have used Cisco routers, switches, and a firewall to build our DMZ segment. The Layer 3 switches in the internal network position were already in place. This is the LAN's default gateway and the switch responsible for segmenting the LAN into virtual LANs (VLANs). Chapter 9 of this book is all about building those VLANs; for now, we'll focus on design.

We've decided to use the following components for our DMZ:

- Two Cisco 3725 routers with T1 WAN interface cards (WICs) with which to connect to the Internet and Fast Ethernet ports to the external switch. We decided on two routers because we want to have a highly available solution to the Internet. If one link goes down, we have another to use, and we can offset the load in times of high demand. ISPs drop lines often. We chose this router model because we foresaw a future need to implement site-to-site VPNs, add more redundancy to the network, and leave room for a possible upgrade in not only bandwidth but also in the number of connections for backup lines later.
- We selected two Cisco switches for our external public network segment and for the DMZ. Now you have to do some research (or refer to Chapter 9 for more information), but basically your switch choice will be based on how many ports you need, the amount of traffic you will have going through it, the quality-of-service enhancements you would like, and other features such as dual power supply. Basically, your switch should be scaled to what you need and scaled up (or out) based on future needs. The best piece of advice we can offer you in terms of a decision on a switch is to research very heavily on the vendor's Web site to find what each model offers and how it can fit into your design based on current and future needs as well as cost.
- We selected a Cisco PIX firewall to be the "traffic cop" among the Internet, the DMZ, and the private LAN. Again, Chapter 5 focuses on this design (you will be shown the exact configuration to implement this solution), and that is where you can find all the details on a specific model. One design flaw we pointed out (but had to live with) was the single firewall design. Basically, we asked for a redundant solution (two firewalls with failover, as you will see in Chapter 9), but the cost was too high for now and the need was not as great. Again, this solution was implemented to make the DMZ and to control traffic to and from it, so the needed design was met with this requirement, but a second redundant firewall would be ideal.

NOTE

When planning your infrastructure, you always need to ensure that you plan the proper equipment list, no matter what vendor you pick. Basically, if you are purchasing this much equipment, presales support could be in order. Ask you vendor to show you user limits per device (how many users can use this device without affecting its performance simultaneously) as well as what type of traffic you will be pumping through it. Many times, the vendor can help you to design your network so that you don't fall short on what you need or you don't go into overkill where you might not need the extra power.

You can see that implementing a DMZ is not a cakewalk; it's all based on needs and analysis. It is something that you have to really plan out and design so that it comes out the way you want it and need it instead of becoming a costly disaster. In addition, note that we have only designed the actual infrastructure—we have not even plugged any intelligence into it. Future chapters point out how to add intelligence so that you can configure rules and other settings to make all the components work together. In the next section, we look at adding the systems into the segment.

Designing & Planning…

What Is a Site-to-Site VPN?

We have eluded to the need for a site-to-site VPN as a future requirement in our design. The purpose of this VPN is twofold. First, we want you to "think outside the box" and consider that there are such things as future requirements when designing a DMZ. Second, we want to ensure that this book is relevant to today's and tomorrow's future technology trends. Let's look at the Cisco router that we selected for this DMZ design as an example.

Key features for the Cisco 3725 and 3745 are:

- Two integrated 10/100 LAN ports
- Two integrated Advanced Integration Module (AIM) slots
- Three integrated WIC slots
- Two (Cisco 3725) or four (Cisco 3745) Network Module (NM) slots
- One (Cisco 3725) or two (Cisco 3745) High-Density Service Module (HDSM)-capable slots
- 32MB Compact Flash (default); 128MB maximum

Continued

- 128MB DRAM (default, single 128MB DIMM); 256MB DRAM maximum
- Optional in-line power for 16-port EtherSwitch NM and 36-port EtherSwitch HDSM
- Support for all major WAN protocols and media: LL, FR, ISDN, X.25, ATM, fractional T1/E1, T1/E1, xDSL, T3/E3, HSSI
- Support for selected NMs, WICs, and AIMs from the Cisco 1700, 2600 and 3600 Series 2 RU (Cisco 3725) or 3 RU (Cisco 3745) rack-mountable chassis

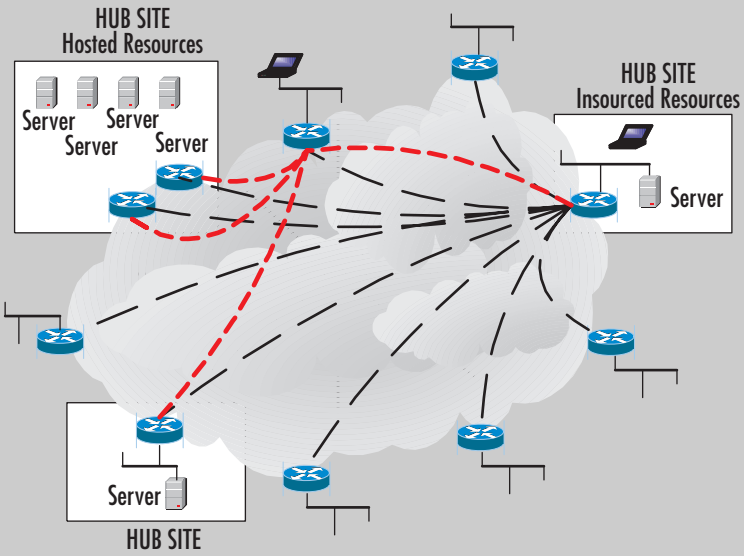
The VPN and encryption AIM are:

- AIM-VPN/HP DES/3DES VPN Advanced Integration Module for 3660 and 3745—High Performance
- AIM-VPN/EP DES/3DES VPN Advanced Integration Module for 2600 and 3725—Enhanced Performance

You are using this router because of the addition of the VPN and encryption AIM that are available with it. You need this added crypto card to be able to tunnel from one site to another over the Internet. You understand why we selected the router we did (for its scaling and functionality), so you need to know what a site-to-site VPN is now that you have the router hardware lined up. A site-to-site VPN (as shown in Figure 2.3) is a network solution that utilizes both public and private IP Internet connections to establish the WAN between all sites that you want to connect to like remote branch offices, business-to-business partner connections, and so on.

Continued

Figure 2.3 A VPN-Based Network



The benefits of using this solution are many. For one, VPN technology can run over public or private Internet-based solutions. In other words, you can utilize this design in just about any country in the world. Frame Relay (especially in international deployments) can be quite costly, so you might want to utilize a VPN connection to connect a remote branch more cheaply than with a costly Frame Relay connection. You can also augment your WAN with a backup solution based on VPN. VPN services are better in some ways because there is no Layer 2 breakdown, whereas VPN traffic is all Layer 3. Since there is no breakdown of data and rebuilding of data, it can be argued that a VPN solution is better when you're trying to utilize voice over IP (VOIP), QoS-based IP traffic, or the like. The difference we mentioned before (public vs. private VPN technologies) is that a public VPN network setup will utilize any ISP's Internet service, whereas a private VPN network would be (for example) AT&T's private IP VPN network built only for use with private business and not publicly accessible via the Internet if you do not want it to be, basically using a Layer 3 private network. Both can be used at the same time with this solution, adding another degree of flexibility to your design.

The reason this information is so important is that in the future, you might only have an Internet connection to worry about for all your remote e-mail, Internet access, and WAN access. Therefore, the DMZ becomes even more critical at this point in the design phase. Each router you see in Figure 2.3 should be firewalled (with a DMZ, if the services are needed) especially if you are not using an ISP's private VPN solution. One last note: The design used

Continued

in Figure 2.3 is called a *partial mesh*. This keeps the tunnel endpoint to a minimum, with no more than one to three hops to get to any site from any site. A full mesh keeps hop counts down, but tunnel maintenance is harder to maintain because you will have many more tunnels to maintain with a full mesh.

Now that you have designed your network, it is time to populate the segment with systems. In the next section we look at systems-engineering your DMZ.

Systems-Engineering the DMZ

You can now start to populate the DMZ and its surrounding areas. First, you need to think about access to and from the DMZ and the services that are needed. The reason behind this initial thought is that your end user, customers, potential customers, and outsiders will be able to utilize resources needed and only those needed resources—nothing more, nothing less. To start the engineering process, you will have to first make certain that you have these answers! What do you need? You should make sure that users can obtain the information that they need about your company without accessing the internal network and only accessing the DMZ, or accessing the Internal network safely if you chose not to implement a DMZ. Working with DMZs can be tricky (hence the need for this book), so if you can, it's always better to segment Internet-based resources via the DMZ for an added level of safety.

Now that you know your network layout, you have to think about other access to and from the DMZ. Your secret, protected, confidential, and proprietary information should be stored behind your firewall and DMZ on your internal network. Servers on the DMZ shouldn't contain sensitive trade secrets, source code, or proprietary information, or anything that can be used against you or your company—or that can be used to exploit or hack into your systems. (There's more on DMZ hacking techniques in Chapter 14.) A breach of your DMZ servers should at worst create an annoyance in the form of downtime while you recover from the security breach.

Here are examples of systems that could wind up on your DMZ:

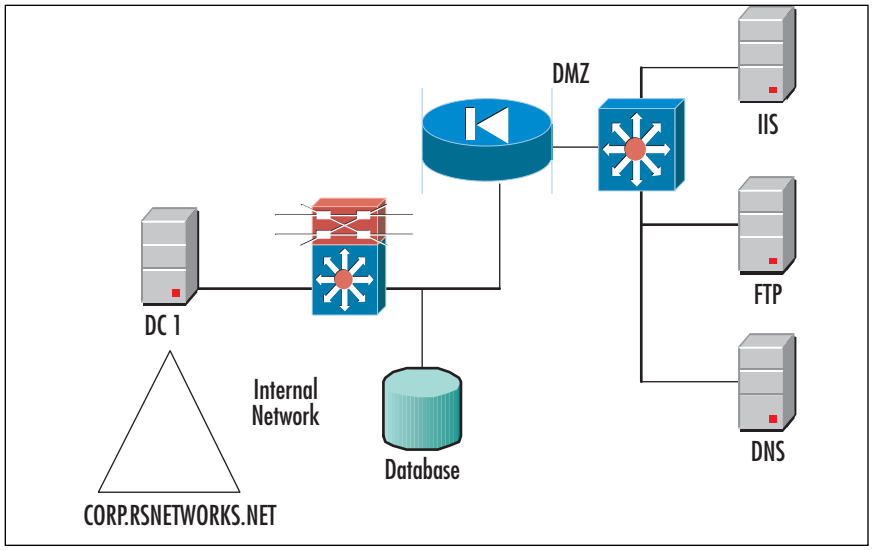
- A Web server that holds public information. This can be IIS (since we are discussing Microsoft technologies in this chapter) or any other publicly accessible Web server. You can also think of FTP services, NNTP services, and other Web-based services to be accessed and utilized.
- Electronic commerce-based solutions always wind up on the DMZ. The front end of an e-commerce transaction server is the one through which orders are placed. Keep the back end, where you store client information, behind the

firewall. You want to design this properly, because if you don't, you could compromise your entire client database (or personal and private data) if it's exploited.

- A mail server that relays outside mail to the inside will be a highly utilized solution, especially since spam and other e-mail exploits are common DMZ host-based targets for attacks.
- VPN solutions are prevalent in the DMZ. Other than the site-to-site VPN we already learned about, you also have VPN solutions in which you have a remote access solution so that clients can attach over the Internet to get to their files and other data needed on the corporate network. This data also has to be publicly accessible via the DMZ.
- Security devices such as intrusion detection solutions, honeypots, and other items you will learn about in Chapter 15.

These areas all need to be addressed when it comes to providing a solution for your systems and where to place them within the DMZ or around it. Take a look at Figure 2.4, which shows the placement of the systems within the DMZ.

Figure 2.4 Systems on the DMZ



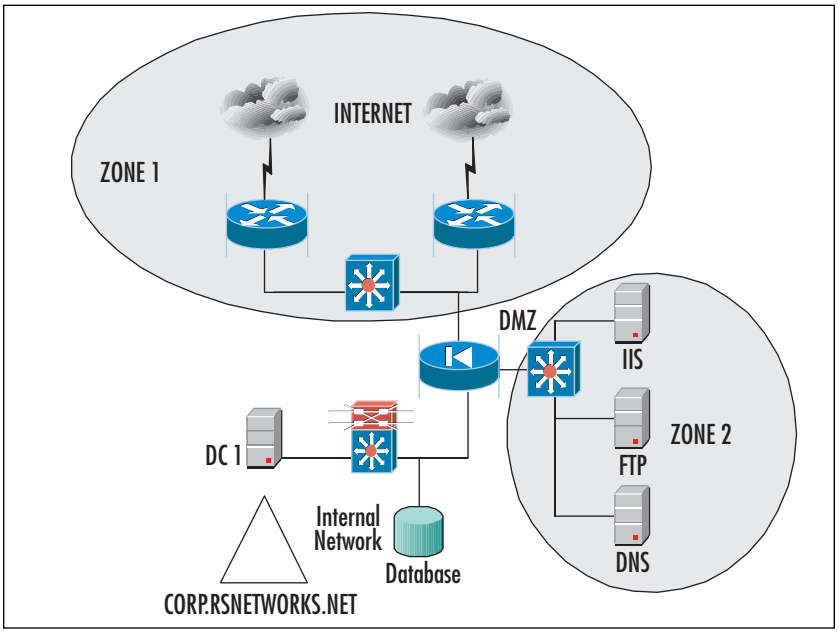
We have placed all the publicly accessible systems (such as Web, FTP, and DNS) on the DMZ so that Internet users can access them and not come into and through our internal network, which is to remain private. You can also see that we have placed our

domain controller and all-important data (such as a SQL Server database) on the internal network. This keeps these resources secure and only accessed via proper channels and not exposed to the Internet for malicious exploits to take place.

Security Analysis for the DMZ

Once you have finalized the DMZ network segment design and placed your systems where they need to be (and you understand why they need to be there), you have to consider the security of such systems. Basically, to learn how to harden the systems themselves, you need to read through the chapters in this book that concern what security measures you need to take in the DMZ. If you want to implement an IDS for intrusion detection, for example, you can read Chapter 15 to learn how to do that, but to understand placement for your DMZ, take a look at Figure 2.5.

Figure 2.5 Implementing Security in the DMZ



To keep the security analysis potion of your DMZ design to a minimum (the rest of the book is based on configuring security), you need to know the two biggest targets of attack and what you should be concerned about when considering your design.

Zone 1

Zone 1 of Figure 2.5 is where your public Internet connection is and where you are most vulnerable to exploitation. Zone 1 is where you need to consider your external router and switch security as well as the outside port of your firewall. You can read Chapter 9 to learn how to lock down this zone. Furthermore, Zone 1 is where you would consider placing your network-based intrusion detection system (although you can place it just about anywhere, depending on what you are trying to capture) as well as your honeypot. You can read Chapter 15 to learn about IDSs and their implementation around the DMZ.

Zone 2

Zone 2 is the actual DMZ. The DMZ is where we have placed our Windows 2000 servers and the services they offer, such as external DNS and Web services. To learn how to harden the systems on the DMZ (also called bastion hosts), you can read Chapter 13.

Building a Windows 2000 DMZ

Building a Windows 2000 DMZ is not very difficult; it's just that there are many moving parts that you need to be concerned with in the initial design and for consistent maintenance.

Consider this solution: You are the systems engineer responsible for designing, implementing, and maintaining a Windows 2000 DMZ segment that consists of an IIS Web server, an FTP site, an external DNS server, and an e-mail relay. That doesn't sound like a lot, but this is one tall order. Consider the following: You will have to know (or find the people who know) how to configure hardware such as routers, switches, and the firewall. You must have security applied to these items and others, such as an IDS if you need it or the design requires it. You have to place bastion hosts on the DMZ and configure security on them, including hardening the base OS (Windows 2000) and then applying the needed services and hardening them, too. Lastly, you need to know how to engineer the traffic to and from those services to other front-end or back-end systems, depending on what the design calls for. In this last example, consider having an internal DNS namespace and an external DNS namespace. How do you configure them to work together through the firewall? This is the point behind this chapter (and much of this book), which is to get you to think about these details so that your DMZ is a success, works properly, can be maintained, and is secure.

Now that we have taken a look at the fundamentals of laying out the hardware to create the DMZ, let's examine the details of populating it with a Windows 2000 solution.

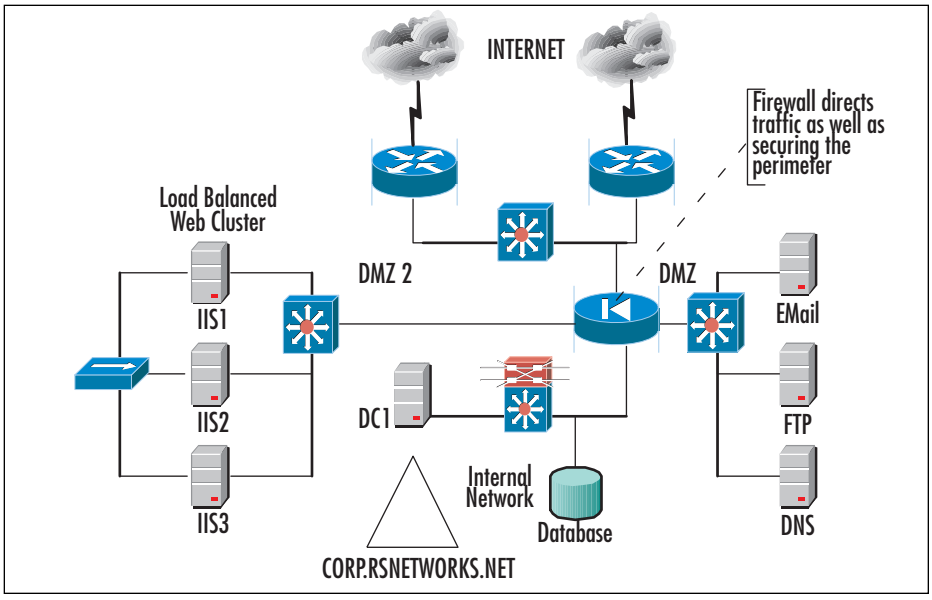
Designing the DMZ Windows Style

Now that you have the fundamental placement, design, and understanding, let's get into more detail concerning the Windows 2000 platform, since there is much to think about and much to plan. In this section we cover domain models (how to configure your domain), devices that sit on your DMZ segment, the names and definitions of systems revolving around the DMZ, and much more. In this next section we look specifically at the domain model, which can confuse many architects who might not know the exact placement of the domain controllers (DCs) and where the logical boundaries of the domain sit with the DMZ segment.

Domain Considerations

Building a domain with a DMZ segment can be confusing. For one, you have probably heard many times that you should never expose a DC to the general public. If this advice is sound, how in the world do you set up domain-based logins if you need a domain-based account for a particular service to work? Consider the following: You need to implement a load-balanced cluster in your DMZ, and the cluster account must log into a domain for the service to work. If this were the case, where would you place the DC? Figure 2.6 offers a possible solution.

Figure 2.6 A Cluster in a DMZ



This solution is not impossible, but it can be tricky. Think of the traffic flow and other issues you need to consider with your design:

1. As you can see. with the Internet, your IIS load-balanced cluster will need to be accessible to the Internet users who will want to see your Web site.
2. If e-commerce solutions are available, the IIS servers need to know how to get to the back-end database, if that is what you need for your solution. You must have a way to get your IIS servers to communicate through the firewall to get to the SQL server.
3. You have two DMZ segments from your PIX firewall. You need to know how to set security levels on each and how to deny traffic coming from one segment to the other. If someone exploits your DNS server, it might only be a matter of time before they get to your second DMZ if you do not apply security so that it does not allow this type of activity.
4. Your cluster needs to access a DC if it is using the Cluster Service. Since this is a load-balanced solution, you can forgo that need, but if you place a cluster on the DMZ, you need a nearby DC to service your requests.
5. Your firewall should be configured to allow for external public Internet traffic to come to your Web sites, but your Web servers can only make requests to the database of the DC behind the firewall. The Web servers need to deliver what was requested of them to the Internet users.
6. Your firewall should also be configured so that your internal DNS server (not shown) can communicate with its forwarder on the DMZ. The internal e-mail server (also not shown) should be able to send e-mail back and forth to the relay on the DMZ. Users should be able to get to the FTP site.

As you can see, now that you have planned it, you only need to pay for it, implement it, and maintain it. That's easier said than done, which is why you have this book. Remember, this chapter is conceptual in nature; it's not until you get to some of the later chapters that you actually learn how to configure all this on the firewall.

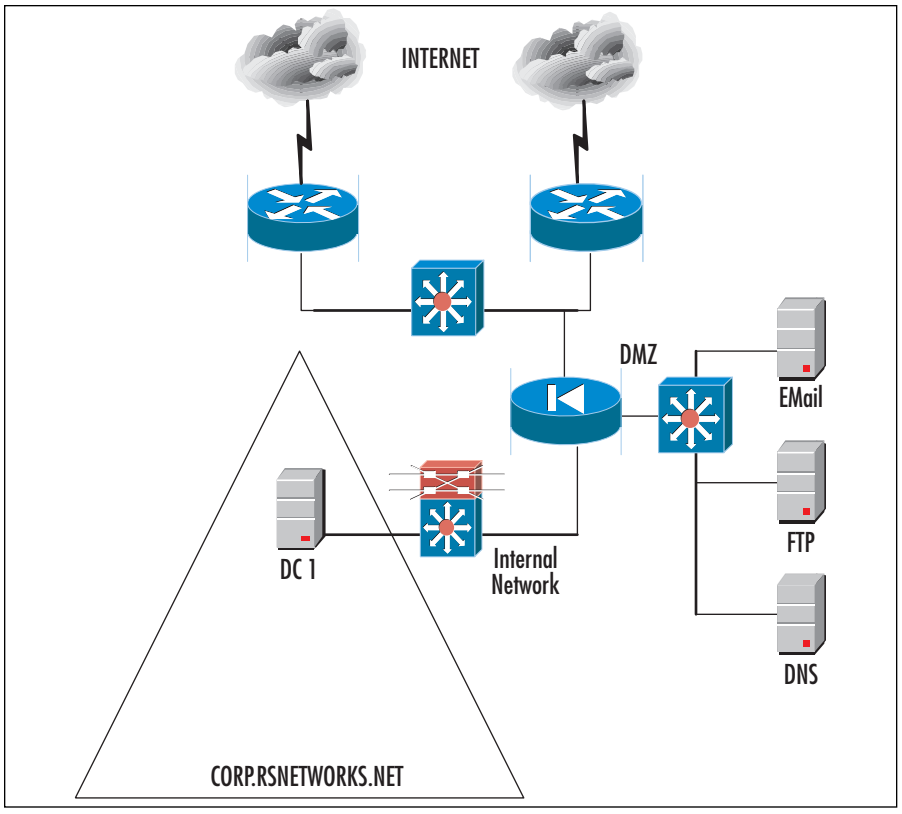
NOTE

Depending on what model and type of firewall you use, you can in fact have different DMZ segments with different services on each to add even more security to your DMZ segments and hosts.

The Contained Domain Model

The type of domain model you need to deploy depends on your needs analysis. We cannot stress enough the importance of design when it comes to very detailed implementations that have many moving parts. With Windows 2000, you need to implement a *contained domain*, which is a Windows 2000 domain that will not cross or extend across any networks that are not controlled by the organization. In other words, you will have a domain isolated to your network, and nothing more. If you consider the DMZ, a contained domain is one that is isolated to the private LAN and does not extend past it, as shown in Figure 2.7.

Figure 2.7 A Contained Domain Model

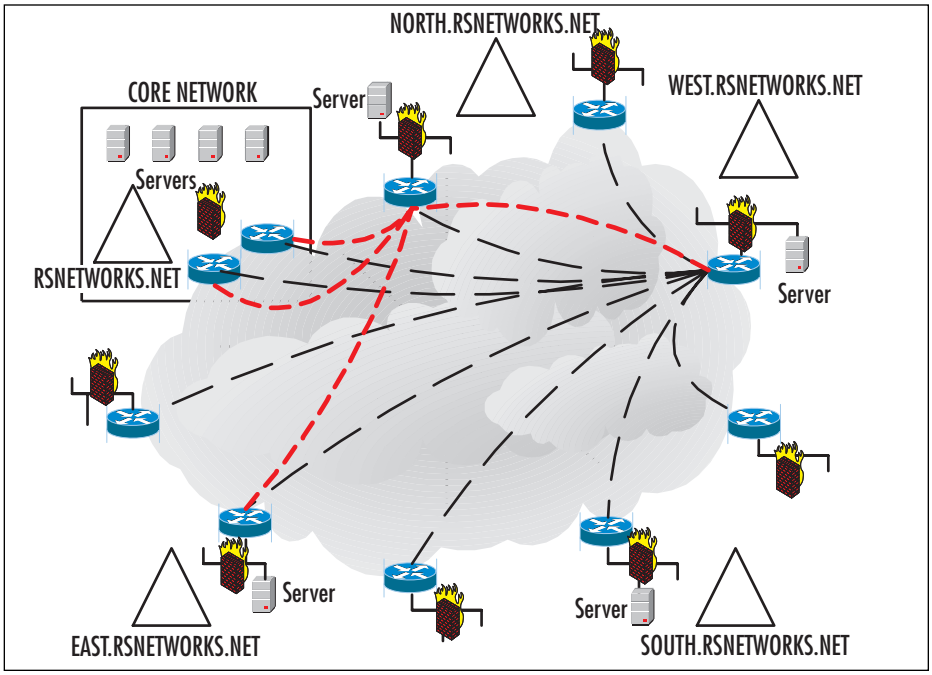


You can also view this model very simply as a single domain that incorporates all your needs and is only located at the hub site or the corporate office. If you extend a DMZ segment, the DC sites behind the firewall and the logical domain remains behind the firewall. You will not have remote sites with their own domains or DCs.

The Extended Domain Model

Now that you know what a contained domain is, let's look at the reverse—an *extended domain* model. The extended domain is a Microsoft Windows 2000 domain that extends past the protected network. The extended domain extends past the boundaries of the site and across WAN links. You can see an example in Figure 2.8. This type of network needs more functionality, including DCs from higher in the domain tree located at lower branches' sites. This can prove to be quite complicated, especially if you are using the partial mesh VPN layout that we looked at earlier in the chapter. Now that you have a firewall protecting your Internet connections, you must consider allowing ports needed by your DCs to open at each site that is firewalled. If you do not, you will not receive your synchronization and replication updates as well as other necessary services. This also needs to be considered when you're building and designing your DMZ, public Internet access, and so on with a Windows 2000 solution.

Figure 2.8 Examining the Extended Domain Model



The Internet Connection

Your Windows 2000 solution revolving around the DMZ needs to allow for Internet access. What must be known about the Internet connection is that it should be able to handle the required bandwidth needs of the site. If you are using this Internet

connection as your LANs Internet access for surfing and e-mail, and you decide to use it for a VPN as well, you need to analyze your requirements first. You can do a traffic flows analysis to ascertain the needed requirements quite quickly, but you need to know how to do the analysis and have the tools with which to do the analysis. If you do not, it is in your best interests to work with an outside vendor that does have the tools and experience to do so. Failing to do so will almost always result in bad performance and increased cost later when you need to reprovision the lines to a higher bandwidth. Everything you need to consider is shown in Figure 2.9.

Figure 2.9 Internet Connection Considerations

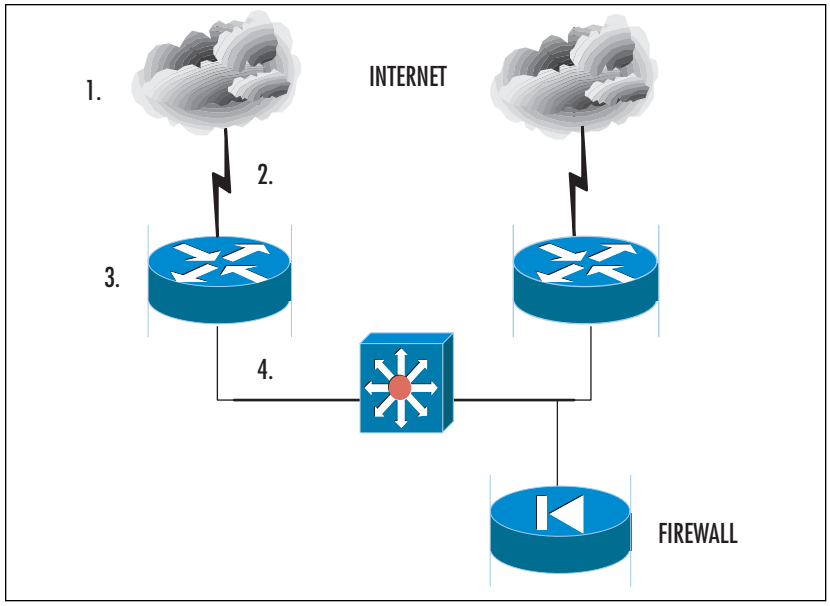


Figure 2.9 shows four sections:

1. The first section you need to consider is the actual ISP you are connecting to. You see here that we have two clouds; the reasoning here is that our Internet connection should be highly available. We suggest having at least two connections if your company's livelihood depends on use of the Internet. You can also diversify the connections between providers and POPs. If you have both POPs in, let's say, New York, and if New York has a major problem (or a single ISP goes down completely), you will still be available on the Internet.
2. Make sure you size your connections properly. Most vendors and ISPs have sizing tools that help you determine how much bandwidth you need to the

Internet. Basically, if we had two T1s here, we would have almost 3MB of traffic to and from the Internet, which is not too bad at all.

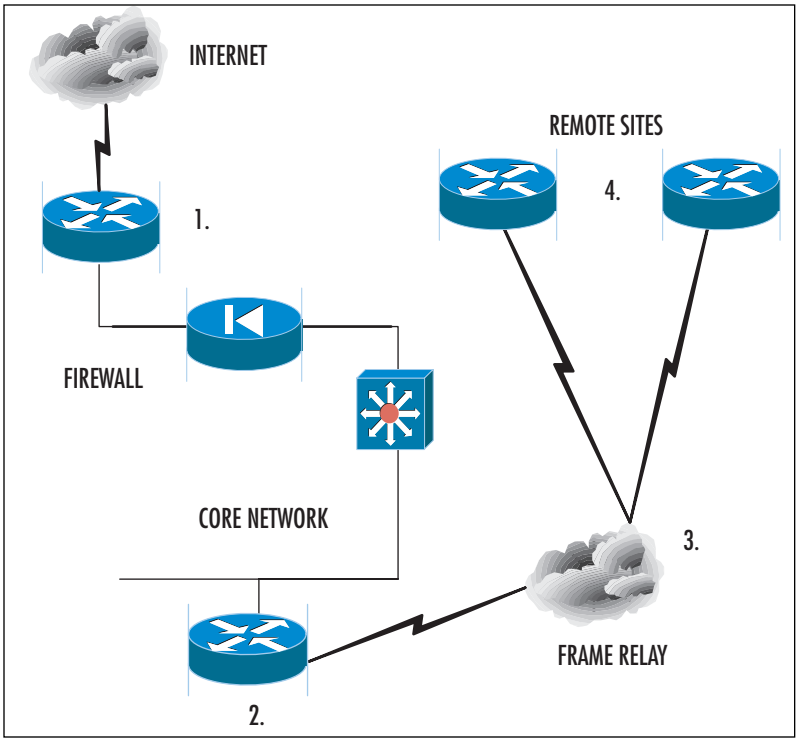
3. Make sure that you have the properly sized router. Make sure that the router can handle all the Internet-based traffic coming and going. Processing power, available memory, and other factors can hinder your response time, so do not make the router the bottleneck on the Internet.
4. Do not let the last leg of the segment (for the Internet connection), which is the connection into the firewall, be the bottleneck. Make certain that you have 100MB/full duplex or better here if possible. Most firewalls allow for Fast Ethernet connectivity.

Remember, anyone can connect to and use the Internet, so the number (and frequency) of your vulnerabilities will become much higher. Always make certain that all these areas are secured properly, and you can learn how to lock all this down in later chapters in the book.

Wide Area Network Link

A WAN link is really not much different from the Internet connection (they both use some form of leased lines), but in a traditional sense, a WAN link basically describes the connections from your company to others through the use of private lines. When we say *private*, we mean in the sense that it is not accessible via the Internet, which is a publicly accessible arena. The WAN link (T1, Frame Relay, ISDN) connects your remote sites up to the backbone located within the core site. Most traditional designs show a hub-and-spoke formation. Here, in Figure 2.10, a hub and spoke are shown connected to an Internet-based segment with a DMZ.

Figure 2.10 A WAN Connected to a Backbone with an Internet Connection



The reason that this concept is so important is that you will have to know how to get traffic from the LAN to either the WAN links or perhaps out to the Internet. How do you do this? Let's go through the process step by step while looking at Figure 2.10:

1. You need to consider the design. Look at Figure 2.10. We have a core network (where the major resources are located) connected to the Internet and also to a Frame Relay network with two remote sites. How do you direct the traffic? How do the remote sites access the Internet?
2. Look at Area 1; you can see that the Internet connection has been established correctly, as shown in the last section. Now you need to visualize how users will gain access the Internet. Basically, to the user, this process should be transparent: Click the Web browser and out you go! This is set via the proxy settings in the Web browser (as shown in Figure 2.11) or via the default gateway of the client (as shown in Figure 2.12). The proxy setting will be valuable to you if you use a proxy server to get to the Internet. (A proxy server DMZ-based system is described in Chapter 8, when we take a granular look at ISA 2000.) If you need to see what your default gateway is set at, you can do an

IPCONFIG /all to get all the IP settings for your Windows NT or 2000/2003 system. If you are using older 9*x* versions, WINIPCFG will do the same. You need to know what your default gateway is because this is how you will direct traffic in an enterprise DMZ. Remember, if you only have an Internet connection, the Internet connection-based router (or the firewall in front of it) can be your default gateway.

Figure 2.11 Proxy Settings for a Web Browser

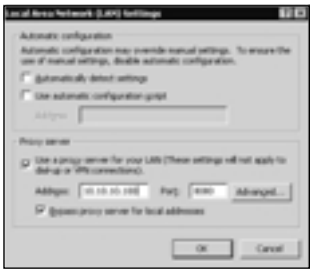


Figure 2.12 Default Gateway Settings for a LAN Client

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . . . . . . . . : SHIMONSKI-LAPTOP
Primary DNS Suffix  . . . . . . . :
Node Type . . . . . . . . . . . . : Hybrid
IP Routing Enabled. . . . . . . . : No
WINS Proxy Enabled. . . . . . . . : No
DNS Suffix Search List. . . . . . : rsnetworks.net

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix  . : rsnetworks.net
Description . . . . . . . . . . . : Wireless Network PC Card
Physical Address. . . . . . . . . : 00-23-15-26-1E-3D
DHCP Enabled. . . . . . . . . . . : Yes
```

Continued

Figure 2.16 Continued

```
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 192.168.2.100
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.2.1
DHCP Server . . . . . . . . . . . : 192.168.2.101
DNS Servers . . . . . . . . . . . : 192.168.2.102
                                    192.168.2.103
Lease Obtained. . . . . . . . . . : Sunday, May 25, 2003 8:04:49 AM
Lease Expires . . . . . . . . . . : Monday, May 26, 2003 8:04:49 AM
C:\>
```

3. Now that you understand that portion, you need to understand Area 2, which is the default gateway for the LAN, as shown in Figure 2.10. Now you need to engineer the WAN link behind your default gateway, or it must be the default gateway if you have an Internet connection to get to. To get to the Internet or the Internet-based proxy/firewall, you need to know how to view the routes in your router. In Figure 2.13, we did a *show IP route* command on the Cisco router. This gave us a routing table, which we only show the beginning of. You can see here that the last line shows what's called the *gateway of last resort*. Your Windows systems will need to know what this is to get out to the Internet if they are connected anywhere on your internal LAN or if they are one of your remote sites. Figure 2.14 shows you the command to add this route.

Figure 2.13 The Routing Table on the WAN Router

```
WANROUTER#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.100 to network 0.0.0.0
```

Figure 2.14 Adding a Route to the Router

```
ip route 0.0.0.0 0.0.0.0 10.10.10.100
```

4. Area 3 is the frame cloud. The frame cloud needs to be engineered and provisioned properly, with the proper access port size and Committed Information Rate (CIR) based on your needs. Make sure you size the frame cloud properly and ask for a bandwidth and utilization report a few months after you use it to make sure you are not overpaying for what you don't need or undercutting your remote sites by not giving them the bandwidth they need to do their jobs. Remember, you need to allow your remote sites to access the Internet through your core, so you need to size the frame links (or any other WAN connection technology) properly.
5. Last but not least, take a look at the remote sites. Note that these sites need to travel up to the core router, and then the core router needs to send the Internet requests up the firewall, which directs the requests out to the Internet. Look at Figure 2.15. It clearly shows the traffic flow needs. And remember the gateway of last resort we saw in Figure 2.13? This same gateway will be used in the remote-side router, with one exception—the IP address of the gateway will be the core router, as shown in Figure 2.16.

Figure 2.15 Internet Traffic Out from a Remote Site

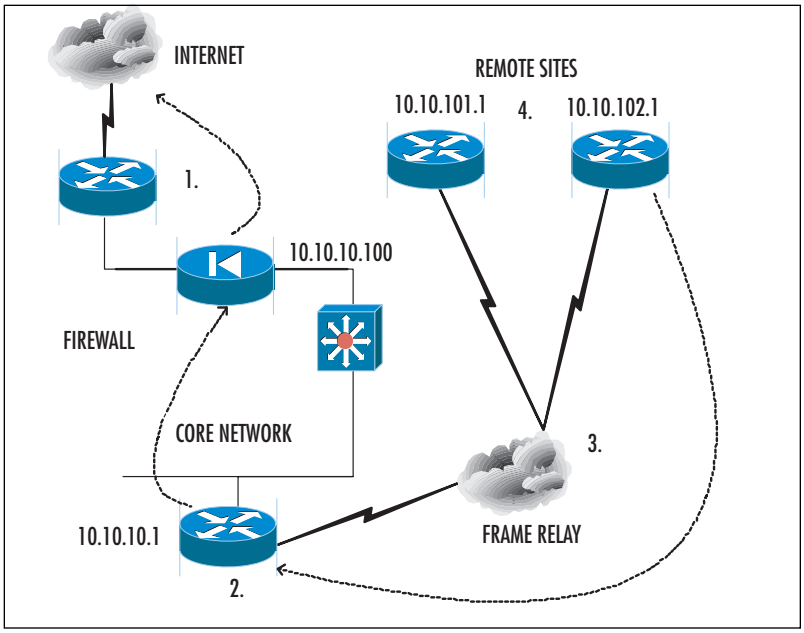


Figure 2.16 The Routing Table on the WAN Router

```
WANROUTER#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0
```

Take another look at Figure 2.15. It is imperative that you understand the flow here. A user at a remote site needs to access the Internet via the WAN link. The user is on the remote site LAN with an IP address of 10.10.102.5 /24 given via a DHCP server. The default gateway for the LAN is the 10.10.102.1 router. The user makes a request of the Internet, and because the IP address is not local to the LAN (10.10.10.100), the request must be forwarded to the default gateway on the LAN. Because of the route added (as shown in Figure 2.16), the router knows to forward the request up through the Frame Relay WAN to 10.10.10.1, which is the main core router through which the Internet is connected. You should start to see the picture here now. The core router now sends the request to the firewall (or proxy, or whatever you have configured), and it forwards the request once again to the Internet router on the perimeter of your network.

NOTE

Never forget: You will have to engineer the way back to the remote site router as well. You can add a routing protocol or static routes in reverse, depending on what you need to do. For help, you can use ping and tracing tools (*tracert* for Windows and *Traceroute* for UNIX) to figure out how to get to and from each site.

As you can see, the WAN link (in conjunction with the Internet connection) is very important to know how to design and engineer or you will be running around in circles trying to figure out why your Windows workstations cannot communicate over the Internet.

DMZ Perimeter Security

The DMZ is an isolated segment through which you simply allow services to Internet users while still maintaining some form of security on your network. To allow users to come into your corporate network unknown, unwatched, and consistently will surely lead to a hack attack down the line somewhere, if not instantly. In this section we look at all the areas you need to consider while building your Windows 200 DMZ. In the last section we took a good, hard look at where your internal resources need to be, how they need to be laid out, and some special considerations to take into account. Here we look at the reverse of your protected network (where your LAN meets your internal firewall port), which is the unprotected network. This is your DMZ and Internet connection, which make up your network perimeter. Although the claim is that they are "unprotected," we will make them "highly protected"—or as much as we can! Let's take a look.

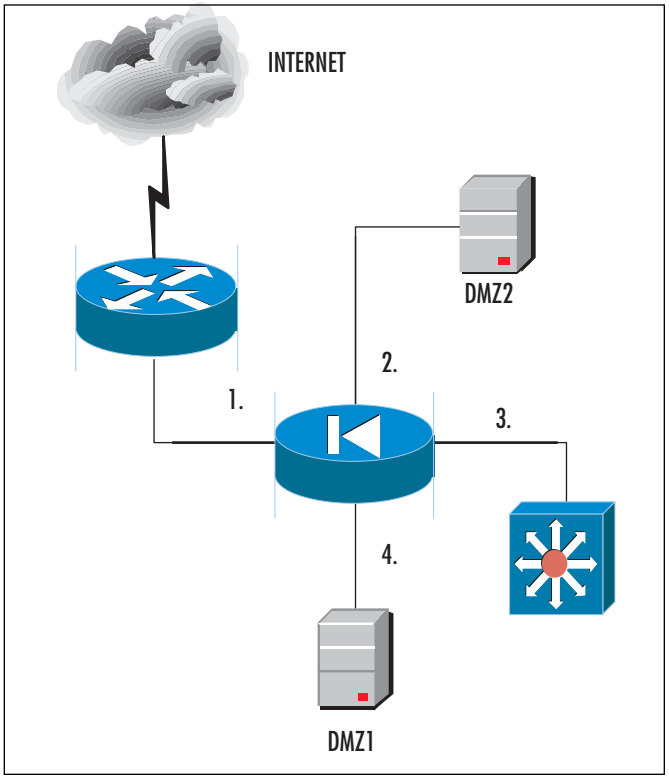
External Router

The external router is the router that connects you to the Internet. Again, there can be more than one, and it's recommended (depending on your needs) that you have at least two connections the Internet. The external router connects the protected network and DMZ to the WAN Link. The router provides the first opportunity to actively permit or deny access for clients and servers and for network services. This means that you can apply ACLs, AAA, logging, and much more to the first line of defense of your network. Basically, you will want to read Chapter 9 in its entirety to learn how to lock down the Internet router, but for now, simply understand its importance in the design.

Firewall

As you already know, a firewall is the "traffic cop" in the middle of your DMZ, public Internet, and private LAN that handles incoming and outgoing traffic and places that traffic where it needs to be against the rules that you create for it—simple as that. Your firewall, if configured properly, will aid you in building and maintaining security on your perimeter network. A firewall is simply an enforcer of a security policy. (A security policy is explained in detail in the sidebar "Guidelines for Creating a Good Security Policy-Based DMZ.") A firewall should reside at the perimeter of your network and protect your data from malicious attackers and wrongdoers. As shown in Figure 2.17, your firewall can have many interfaces.

Figure 2.17 Firewall Interfaces



Let's look at each section to see what these interfaces can connect to. First off, Section 1 is the external WAN port on the firewall. This is the Ethernet connection that connects you to the external router. Section 2 is the first DMZ leg and has IIS Web services on it. Section 3 is the connection into the corporate network—the private network. Section 4 is the second DMZ leg with a DNS server on it. Basically, the point to show you that you could have multiple DMZs set by one single firewall! As you will see in Chapter 5, there are many ways you can deliver secure services though multiple DMZs with only one firewall. Three interfaces are recommended: one for incoming traffic, one for access to the demilitarized zone, and one that connects to the protected network. But remember, if you need more than one DMZ, you can create multiple ones.

NOTE

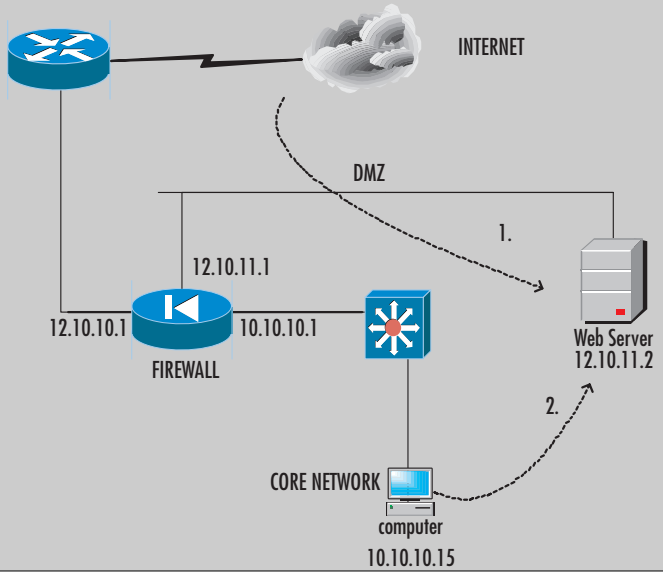
In Chapter 8, you will learn all about Microsoft's Windows-based proxy and firewall product, ISA Server 2000. ISA (which stands for *Internet Acceleration and Security*) allows you to build a DMZ firewall and create a protected solution with a Microsoft product.

Designing & Planning…

Guidelines for Creating a Good Security Policy-Based DMZ

We mentioned the importance of a firewall and alluded to the fact that a firewall is basically the enforcer of a security policy. This means that your firewall will be configured to mirror the needs and requests of the corporation. For instance, if you want to create a security policy that states, "no remote user can pass the DMZ. Only users needing to access our IIS Web server from the Internet can access that single server, and nowhere else can they go though or pass the DMZ." All you need to do is configure the rules on the firewall (PIX, Check Point, Nokia, ISA) to reflect that need, as shown in Figure 2.18.

Figure 2.18 Traffic Directed to an IIS System on the DMZ

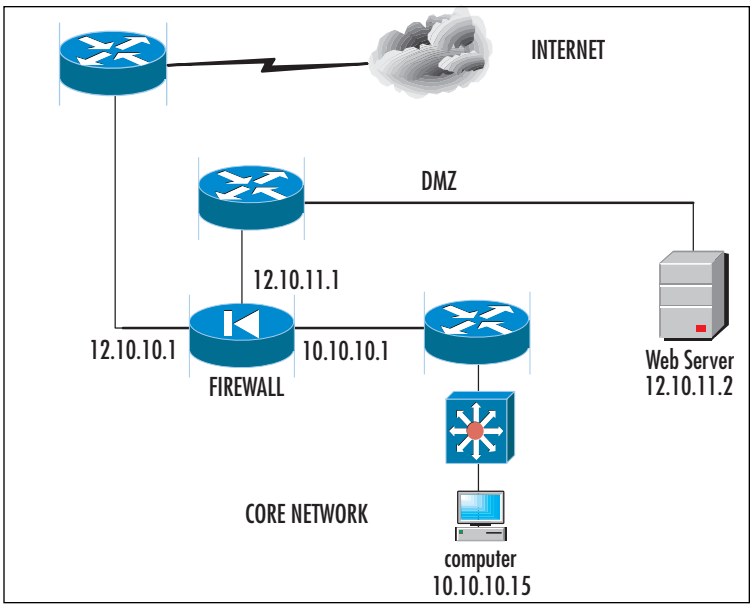


Let's dissect that need again against what we actually configure: The need was to have only Internet users access the IIS server at 12.10.11.2. This is done through the firewall and its ruleset. Basically, you add a rule to the firewall stating that any user needing to get to an IIS server should be sourced from the Internet. The firewall also knows that if the IIS server is compromised, no request from the 12.10.11 network needs to be going to the 10.10.10.0 subnet in the private network. As you see from Request 2 in the figure, you can't allow users to go through the firewall to attach to the Web server, because this capability is not in the security policy.

Extra DMZ Routers

Sometimes (if the size and complexity of the network dictate) you'll need to have a router on each leg of the firewall. This concept is illustrated in Figure 2.19. At times, you will get requests to either add security to the segment you are working on or add more and more devices to it, where you might need to either route or direct traffic. Many firewalls will not route like a router; in other words, a typical firewall will route the RIPv1 protocol where a router will route IS-IS, OSPF, EIGRP, RIP, and so on. A router does just that—it routes. A firewall can in fact route if it is configured to do so, but often, depending on how paranoid you are, you could decide to keep these services dependent on the device in which they sit.

Figure 2.19 Extra Routers Added into the DMZ Segment



The added routers can increase security and flexibility, but they can also add complexity. The only real time you need to use this is when the firewall is not part of the protected network. The DMZ router filters on the services the DMZ provides and denies all other traffic. A good way to envision this is if you have a firewall that will do NAT. If the firewall provides NAT, the DMZ router will verify that all connections originate from the firewall, which will add to your safety. With the internal network router (shown in Figure 2.19), you can see another level of security against attack. The threat that lingers most on the internal network is the user. The end user can be the biggest threat on the internal network. If configured properly, the internal router can be used to protect your firewall and DMZ from internal attacks. The rules you set up on the router should mimic what is configured on the firewall. Remember when I mentioned that we only wanted external users to hit that IIS server? This is the way you can guarantee it with another level of security. (Router hardening and lockdown are covered in Chapter 9 of this book.)

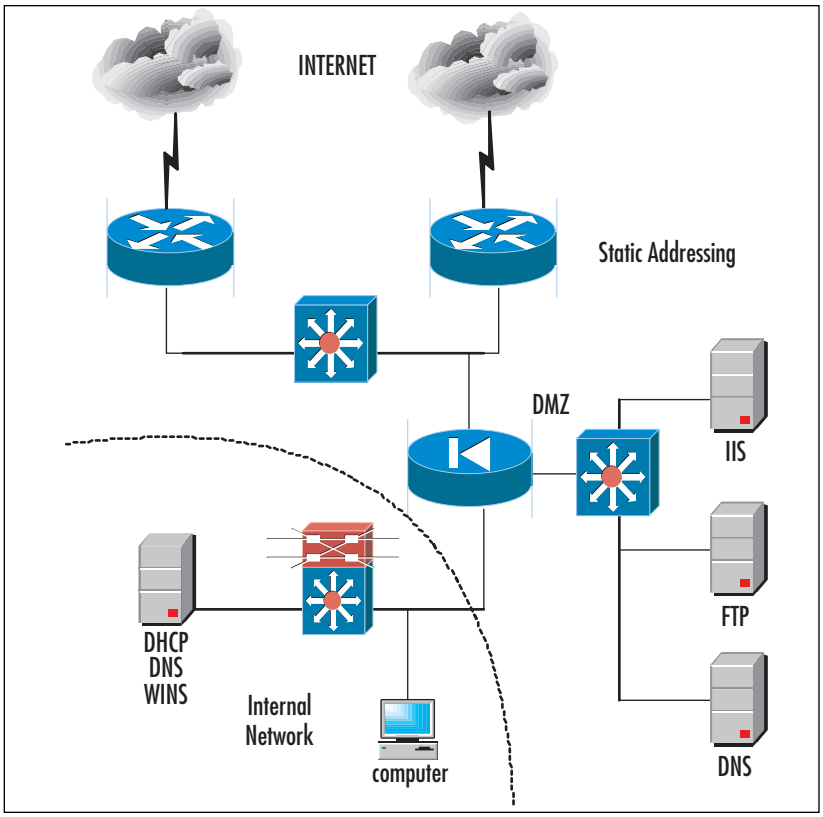
NOTE

Although this solution might be deemed overkill, you never know what level of security a company and its security team are willing to use for the most protection. Never underestimate the client's needs; always bring up options in design meetings so that you can let the stakeholders in the project decide what they want to spend for the level of decreased risk.

Name Resolution for the DMZ

Too often, DNS and WINS servers are misplaced when people work with the DMZ. Is there a specific design you need to follow? In essence, yes, there is. The importance of name resolution in the DMZ only matters if you in fact need it. Let's look at a quick design map so you can follow along. Figure 2.20 shows you that it is very important to use static addressing on your DMZ and on your public Internet segments. This is because it minimizes the number of exposed hosts on your segment, it reduces the number of attackable hosts on those segments, and more important, it does not create a repository of information that can be used against you if exposed. If a hacker is able to tap into and exploit your DNS server, for example, they would have all IP and name information for your network. If your DMZ is not very large (which it normally is not), you should use static addressing. DNS, WINS, and even DHCP are more suitable for the internal network, where you are more likely to have more hosts and the like, so it is safer to put it there and only have to look for internal attacks.

Figure 2.20 Name Resolution in the DMZ



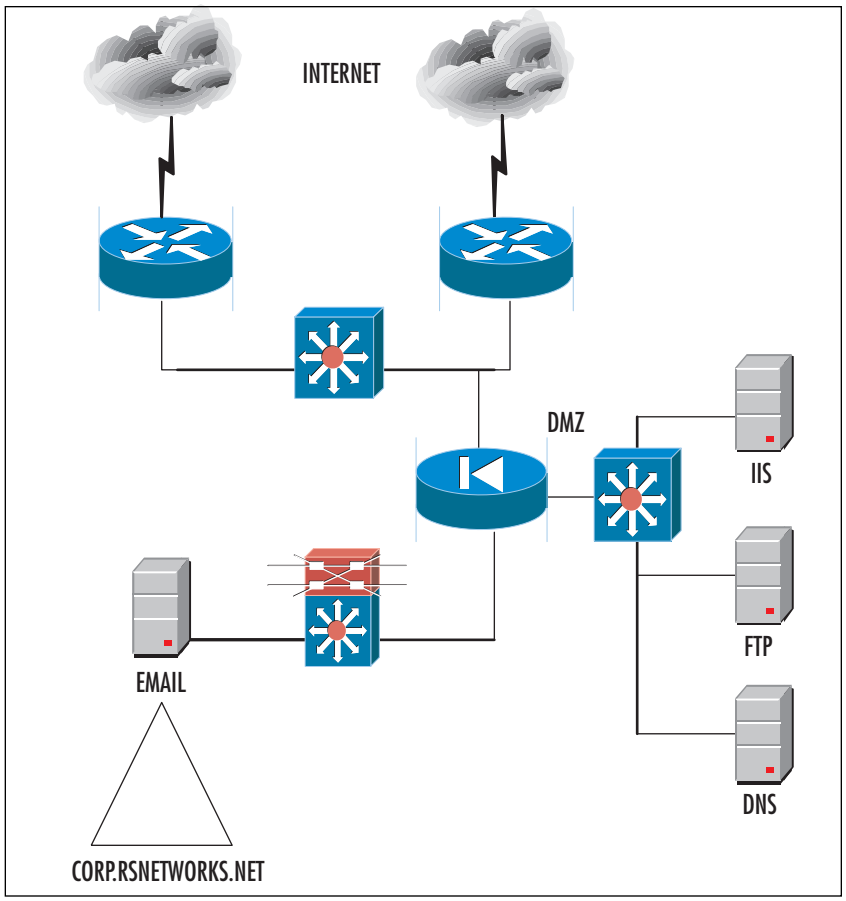
If you do decide to allow WINS (NetBIOS-based traffic), DNS, and DHCP through your firewall, you must allow for it by specifying the port number. Later in this chapter we cover traffic engineering, where you can find the details and port numbers for engineering this type of communication. Another item to mention with DHCP is that DHCP communication is done over User Datagram Protocol (UDP) ports 67 and 68, so this will allow the traffic through, but if you want the broadcasts from clients to pass through "looking" for a DHCP server, you need to add a relay address (called an IP Helper address by Cisco) to a routing device so that it will allow the broadcast through and you can specify the IP to deliver it to.

DMZ Mail Services

Too often, mistakes are made with e-mail service placement due to the administrator's lack of knowledge of how and where to place such services! There are really only two ways to place an e-mail server easily within a DMZ. For one, you can place the e-mail server (only one for this example) in the private network. The firewall in front of

the e-mail server would be responsible for taking all requests in and out of the network and for securing the traffic to the e-mail server. Due to the server's design, it made the relaying of outbound Internet-based e-mail the responsibility of the e-mail server—only one single server. The question is then asked, however, "Why would we want to expose our e-mail server to the public Internet? What if somehow, someway, there was a way to attack the e-mail server directly through the firewall?" Figure 2.21 shows you the design we are talking about. You can see the e-mail server behind the firewall, allowing the public Internet access directly to your private corporate network.

Figure 2.21 E-Mail Server Behind the Firewall



Mail Relay

There are several risks associated with the receipt of e-mail from potentially untrusted entities outside the site. Now that you can visualize this situation, let's consider an

alternative. Would you want your Exchange 2000 server exposed in this manner? Would you want your Sendmail server attacked and penetrated so that the attacker has direct access into your network? Of course you wouldn't. Because of this vulnerability, it is common to simply add another e-mail server to the DMZ segment and use this server as a relay to and from the protected e-mail server in the private network. The server now becomes what's called an *e-mail relay,* and it will relay the mail to and from the Internet and to and from the mail server. If mail relays (IIS has an SMTP service that can be used as a relay) are compromised, you can simply reinstall the server from scratch and not lose a thing because all the server did was relay traffic. It is also common not to add any mail relay or forwarder to a Windows domain—again because it will most likely be attempted for an exploit in the future.

Web Servers

Web servers are the most common form of DMZ-based hosts today. Other services are needed, such as DNS and e-mail, but if you really think about it, the main reason DMZs even exist is due to the public Internet Web surfer feeding frenzy. Almost every company in business in the world now has a publicly accessible Web site, which means that just about every company worldwide either has an Internet presence or is looking to have one. Thanks to all these personal invitations to companies' corporate networks, it is imperative that you also think out your security plan completely or your network could be exploited.

External Web Server

Organizations frequently have data they want to publish to the external network via a Web server. Again, to allow direct access to the Web server via the Internet while the server is sitting in your private and protected LAN would be suicide. For that reason, allow an external Web server to be placed on the DMZ. This way you can allow all your visitors to come directly to your IIS server and not have them exploit that server only to find ways to get to other systems. If the IIS server is external on the DMZ, you can at least have some defense against it if it is compromised in any way.

Internal Web Server

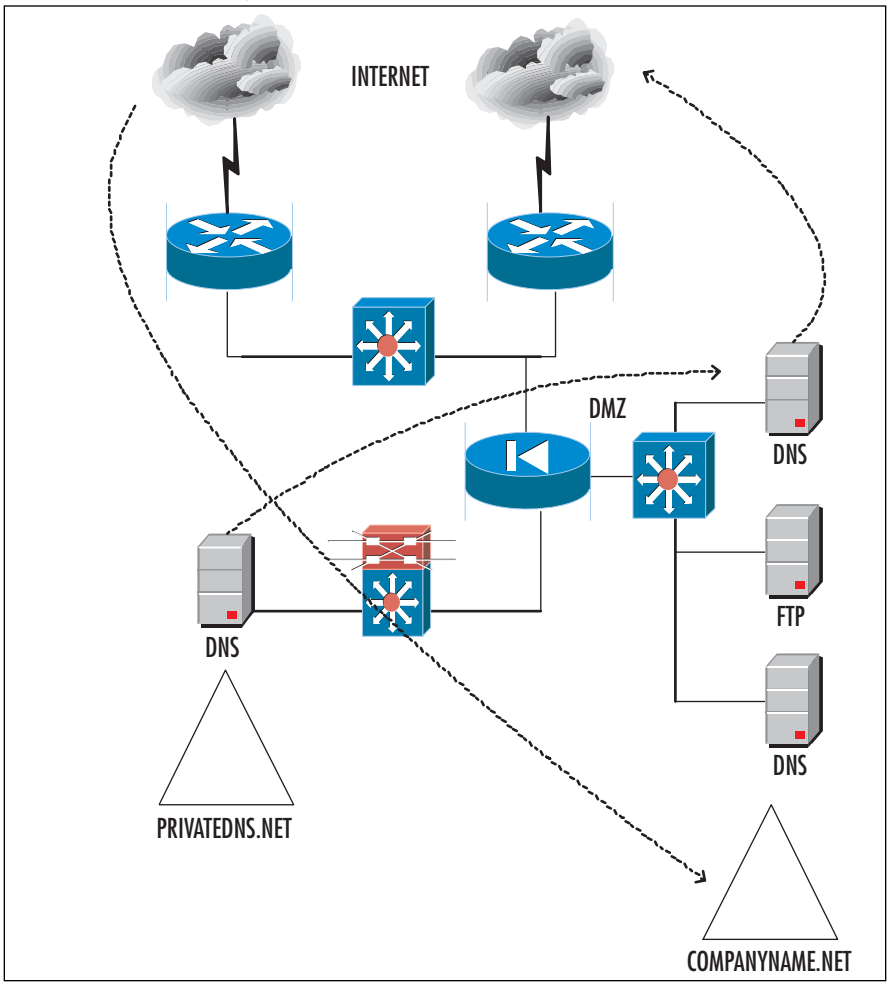
Your internal Web server is nothing more than an intranet you set up for HTTP and other Web-based access for use within the LAN and not for public access. Your internal Web server will be secure from the Internet only if you never connect it to the Internet. Once you do, you move the server out to the DMZ and it becomes an external Web server.

Designing Windows 2000 DNS in the DMZ

The last (and most common) services to see on the DMZ both internally and externally are the DNS servers for your organization. If you are using DNS to resolve your company's IP address to easy-to-remember names, this section is for you. DNS services are now more than ever the most common service used for name resolution. Because of DNS's growing use, it is important that when you plan your Windows 2000 network, you are able to design the Internet namespace and the external namespace for the organization. You can also set up your own primary servers in the DMZ, or you can forward requests to others.

Figure 2.22 shows both solutions at work. For one, you can set up an internal namespace called PRIVATEDNS.NET. This is the company's Windows 2000 DNS solution that the entire Active Directory depends on. We do not want to expose that to the Internet if we don't have to. Now we can put a forwarder on the DNS server that resides in the DMZ. This is called the *external DNS server*, which will be explained shortly. The last scenario is to host your own public DNS servers. That means that even more traffic will come to your site, since others can use your DNS servers as well. If you opt to do this, make certain that you secure your solution perfectly.

Figure 2.22 Examining DNS in the DMZ



External DNS Server

The external DNS server resides in the DMZ and is for public use. The only information that should be on the external DNS server is the information that needs to be advertised to Internet clients—nothing more. You can use a Windows 2000 server, but it is not uncommon to see Linux on the DMZ doing DNS forwarding. Not one piece of internal DNS information should be kept on this system. The internal DNS server is unable to communicate directly with the external network, because it will be configured to send queries and receive the responses via the external DNS server. You have to ensure that DNS UDP connections are allowed through the firewall to the external DNS server or your solution might not work.

Engineering Windows 2000 Traffic in the DMZ

Once you have finalized the DMZ network segment design and placed your systems where they need to be (and understand why they need to be there), you have to consider traffic and applications flows, ACLs, and filtering. In this section of the chapter we review the concepts you need to allow for the proper traffic to flow where it is needed to and from the DMZ segment.

Traffic engineering can be tough. Think of it like this: You build your DMZ (using whatever firewall product you like—PIX, Nokia, Check Point, ISA 2000) and now you have to let services in and out. Other chapters in this book show you exactly how to do that (with these exact vendor products), but it is inherent that you at least understand the concept of it here and the fundamentals of design. Each chapter of the book grows more detailed as to how to configure each device, but the concepts of design and the initial layout are the most important by far.

First, you need to know what a port is. A port number is a number assigned to a service. You can think of an IP address and a port number as analogous to a street address and an apartment number. If you have ever lived in an apartment, you know that everyone in the apartment complex has the same street address. So what tells the mail carrier where to put everyone's mail? The apartment number does. If it weren't for the apartment number, all organization would end once the mail got to your street address. You would have to search through everyone's mail to find yours. This is the same concept behind IP addresses and port numbers. The port number is used by a particular service. When a request is made, the port number tells the computer which service it wants to talk to. You could say that the port number defines the endpoints of a connection. The format for using port numbers is the IP address followed by a colon and the port number. For example, let's say that we want to connect to the IP address 10.10.10.10 and we want to use the port for HTTP (port 80). The syntax would be 10.10.10.10:80.

There are three categories of port:

- Well-known ports
- Registered ports
- Dynamic/private ports

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for managing port numbers. The well-known port numbers range from 0 to 1023. The registered port numbers range from 1024 to 49151. The dynamic and private ports

range from 49152 to 65535. Most systems use the well-known port numbers to run system processes or privileged programs. The registered port numbers are not controlled by ICANN. Most of the time they are used with nonsystem processes or nonprivileged programs, such as an ordinary user running a program. Table 2.1 lists the well-known port numbers.

Table 2.1 Well-Known Port Numbers

Port Number	Transport Layer Protocol	Description
7	TCP, UDP	Echo
13	TCP, UDP	Daytime
19	TCP, UDP	Character generator
20	TCP, UDP	File Transfer Protocol (default data)
21	TCP, UDP	File Transfer Protocol (control)
22	TCP, UDP	SSH Remote Login Protocol
23	TCP, UDP	Telnet
25	TCP, UDP	Simple Mail Transfer Protocol (SMTP)
53	TCP, UDP	Domain Name Server (DNS)
67	TCP, UDP	Bootstrap Protocol Server
68	TCP, UDP	Bootstrap Protocol Client
69	TCP, UDP	Trivial File Transfer Protocol (TFTP)
79	TCP, UDP	Finger
80	TCP, UDP	World Wide Web HTTP
88	TCP, UDP	Kerberos
110	TCP, UDP	Post Office Protocol Version 3 (POP 3)
118	TCP, UDP	SQL Services
119	TCP, UDP	Network News Transfer Protocol (NNTP)
123	TCP, UDP	Network Time Protocol
137	TCP, UDP	NETBIOS Name Service
138	TCP, UDP	NETBIOS Datagram Service

Continued

Table 2.1 Well-Known Port Numbers

Port Number	Transport Layer Protocol	Description
139	TCP, UDP	NETBIOS Session Service
143	TCP, UDP	Internet Message Access Protocol (IMAP4)
156	TCP, UDP	SQL Service
161	TCP, UDP	SNMP
162	TCP, UDP	SNMPTRAP
179	TCP, UDP	Border Gateway Protocol
194	TCP, UDP	Internet Relay Chat Protocol
213	TCP, UDP	IPX
369	TCP, UDP	Rpc2portmap
389	TCP, UDP	Lightweight Directory Access Protocol (LDAP)
401	TCP, UDP	Uninterruptible Power Supply (UPS)
443	TCP, UDP	HTTP over TLS/SSL (HTTPS)
445	TCP, UDP	Microsoft-DS
464	TCP, UDP	Kpasswd
500	TCP, UDP	Isakmp
513	TCP	Remote login via Telnet (login)
514	UDP	Syslog
530	TCP, UDP	Rpc
563	TCP, UDP	NNTP over TLS/SSL (NNTPS)
568	TCP, UDP	Microsoft shuttle
569	TCP, UDP	Microsoft rome
593	TCP, UDP	HTTP RPC Ep map
631	TCP, UDP	Internet Printing Protocol (IPP)
636	TCP, UDP	LDAP over TLS/SSL (LDAPS)
637	TCP, UDP	Lanserver
689	TCP, UDP	NMAP

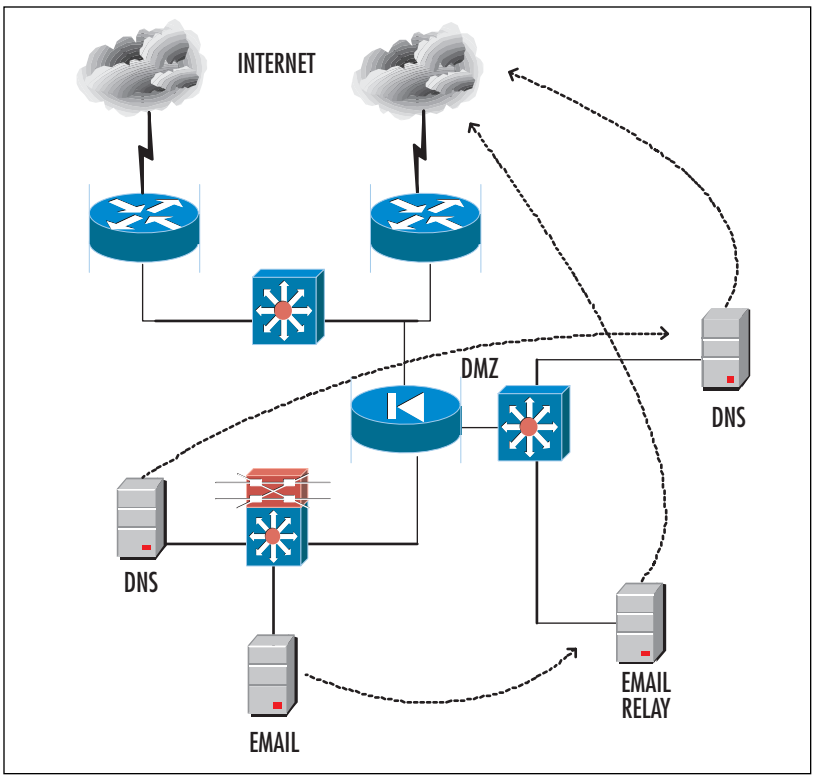
Continued

Table 2.1 Well-Known Port Numbers

Port Number	Transport Layer Protocol	Description
691	TCP, UDP	MS Exchange Routing
749	TCP, UDP	Kerberos administration
750	TCP, UDP	Kerberos version iv

What is so important about these ports is that when you get to later chapters of this book, you will have to come back here to get the numbers to plug into the ACLs and filters you create with your firewall of choice. Make sure that you understand the placement of DMZ hosts and then what traffic to let through before you attempt to configure your firewall, because the firewall configuration will solely depend on that information (port, service, placement) first! You can't direct traffic if you don't know where to send it and what numbers you need to plug in to get that movement in the first place. Use the following example for all the rest of the examples in future chapters. If you have the network design shown in Figure 2.23, what traffic map would you design?

Figure 2.23 Windows 2000 Traffic in the DMZ



Let's look at this in more detail:

- You have an internal DNS server that needs to communicate with an external DNS server to forward requests.
- You have an external DNS server that needs to communicate with the Internet DNS.
- You have an e-mail server and its e-mail relay to the Internet to consider.
- You have an e-mail relay that needs to send mail to the Internet.

Now that you have looked at the traffic map, you need to configure the rules in the firewall. You will have to use DNS and e-mail ports from Table 2.1. For DNS, you can use port 53, and for e-mail services, you can use SMTP or POP3, which use ports 25 and 110, respectively. Again, there are many more services and many more ports, but if you lay out the map and think about the communication paths, you can easily plug in the numbers and then go to the appropriate chapter in the book to find out how to configure the necessary rules, filters, and ACLs.

Assessing Network Data Visibility Risks

Now that you have engineered the traffic to flow in and out of your network, what is really the risk of others seeing this traffic? Tools to eavesdrop on traffic (you can see them in Chapter 14, which is aptly named "Hacking the DMZ") are freely available on the Internet and can cause you much pain when you try to build a Windows 2000 DMZ. If you have NetBIOS traffic traversing your network, a network sniffer is all someone needs to learn, map, and disable your network. We won't spend too much time on this topic because it's really the concept you have to get down here. You need to think about the problems you could encounter while building your DMZ if you do let certain traffic traverse your network and over the Internet. For this reason, Microsoft always tells you to disable file and print sharing on your DMZ hosts, your home PC connected to the Internet—even your servers on your trusted network that are not needed as file or print servers. Yes, it's that serious, and reading through Chapter 14 will help you to realize that.

Configuring & Implementing…

Disable NetBIOS and SMB!

Disabling NetBIOS on servers in untrusted networks (or anywhere in general) is always a good idea. Just remember to test before you do, in case an application you are using is dependent on that service. Other than that, disable away. NetBIOS is by far the poorest form of secure name resolution you can find. Always use DNS if you can, but since your Windows networks are sure to have some legacy systems that are anything predating Windows 2000, you are sure to need NetBIOS. Always disable NetBIOS if it's not needed on your DMZ hosts or they will be exploited, without question. Servers in the perimeter network should have all unnecessary protocols disabled, including NetBIOS and server message block (SMB). These protocols should both be disabled to counter the threat of user enumeration. You can think of user enumeration as a form of information gathering so that the attacker can find other ways to attack from the information he or she has gathered. This information includes domain and trust details, shares, user information, groups and user rights, and even Registry information. You will want to disable NetBIOS whenever possible. To do this from a firewall, you can block all communication using the following ports:

- UDP/137 (NetBIOS name service)
- UDP/138 (NetBIOS datagram service)
- TCP/139 (NetBIOS session service)

SMB uses the following ports:

- TCP/139
- TCP/445

To disable these on a host, you can remove File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks using the **Transmission Control Protocol/Internet Protocol (TCP/IP) Properties** dialog box in your **Local Area Connection** properties. Once you have done that, there is one more option. This is the easy way to disable SMB:

1. Open the **Device Manager** (you can get to it from the **Control Panel** of the Computer Management Console).
2. Once you open Device Manager (in Computer Management view, as shown in Figure 2.24), you can then show the hidden devices

(where the driver is) by right-clicking the **Device Manager** icon and selecting **View** and then **Show Hidden Devices**.

3. Expand the **Non-Plug and Play Drivers**.
4. Right-click **NetBIOS over Tcpip**, and then click **Disable**. Once this is done, you will disable the SMB direct host listener on TCP/445 and UDP 445.
5. Close the Computer Management console to finish.

Figure 2.24 Disabling NetBIOS over TCPIP

In sum, this shows you how to engineer traffic on a Windows 2000 network. You need to know how to direct traffic, as well as how to enable and disable it. A hacker can research just as easily as you can, and this is what they are looking for—the exploits you have forgotten about and left wide open.

Not all traffic engineering does good, so you need to test your efforts before going live into production. You could disable a service or driver only to find out an application that depended on it no longer functions properly. When you disable the NetBIOS over TCP/IP driver, for instance, you have effectively disabled the nbt.sys driver. This driver could be used by another application. Just be careful and test.

Until now we have looked at how to build a Windows 2000 DMZ. We have covered the network hardware needs and basic layout, the devices that will populate the DMZ, the types of systems you need to place on your DMZ, and lastly, the engineering of traffic through the DMZ. The last thing you need to know is the population of systems in the DMZ such as Windows 2000 hosts, DNS, and others. Again, this is covered in detail in Chapter 13.

Windows 2000 DMZ Design Planning List

In order for you to properly plan your Windows 2000 DMZ, follow these checklists to get yourself from start to finish. These are by no means all-inclusive lists, but they should serve you well in getting started, getting the foundation of what is needed up and running. Then, if necessary, you can populate the list with more items you need or want.

To successfully start your Windows 2000 DMZ implementation, begin with our initial discussion on planning: network engineering, systems engineering, and security analysis.

- **Network engineering**
  - First, start with your vision. You must have current network topology maps handy and a map of what it is you plan to do. There are many examples through this chapter and this book on how to make a proper topology map for your organization.
  - After the planning stage, you can either start to work on a prototype (or pilot) or go live. No matter what you decide, you should do some testing or visit a location (or another business) to analyze their Windows 2000 DMZ solution to see if your scaling requirements are right.
  - Don't undercut yourself. If you need to scale up or out, plan that in now, so you can get a jump on future requirements.
  - Get the devices you need, lay them out, test them, and then implement them into the design.
  - Make certain that you harden your network engineering devices. They will be exposed to the Internet and are just as vulnerable to attack as your Web or DNS servers.
- **Systems engineering**
  - Plan the placement (logically and physically) of your DMZ hosts. Since you are using Windows 2000, you can look at IIS for a Web and FTP server as well as an SMTP relay, Windows 2000 DNS services, Exchange 2000, ISA Server, and so on.
  - Once you plan your systems, you need to engineer the communications between devices in the DMZ and behind it.
  - Once you have the planned communications, you can start implementation.

- **Bastion hosts installation and lockdown**
  - As you populate the DMZ with hosts to provide services, you need to harden them.
  - Harden the base Windows 2000 Operating system first. (You'll find details in Chapter 13.)
  - Harden each individual service you implement. (You'll find details in Chapter 13 and Appendix A.)
- **Security analysis**
  - Run tests on your Windows DMZ to ensure that all devices are locked down, hardened, secure, and ready to provide services to the public Internet.
  - Test all connections and all devices, and use a plethora of tools to test different attacks.
  - Run service packs, hotfixes, and anything else to test, harden, secure, and tighten up the perimeter—or your network could be exploited. You can refer to Chapter 14 to learn how to hack the DMZ and test it.

Summary

Although this is only the second chapter in the book, you should start to see many concepts coming together. The demilitarized zone, or DMZ, is probably the smallest, most difficult to design and engineer segment on your network. In this chapter in particular, you should have acquired the foundation to lay out and build a Windows 2000-based DMZ. Again, it's not merely knowing Windows 2000, Cisco, or any other vendor's products that will get you through the design and implementation of a Windows 2000 DMZ, but all this knowledge put together underlies a simple set of concepts: Design the network, design the systems, and then test them all for security. We looked at that process in great detail in this chapter. You learned how to lay out all the hardware you need, set up a plan and a design with a topology map, plan where the systems will be placed—in front of, behind, and within the DMZ segment formed by the firewall you use. Other chapters focus on more granular aspects such as bastion hosts, hardening, testing, and so on, but this chapter should have laid out the groundwork for your design.

When considering Windows 2000 (or any other vendors OS), you need to consider system placement and traffic engineering. You need to know exactly what ports and services that OS needs to rely on to communicate and function properly. Although Windows 2000 is a secure operating system (Windows Server 2003 is even more secure), it is only as secure as you can make it. Therefore, it's very important that you followed this chapter closely since everything you learned here will be used in the DMZ of your network. The DMZ is the segment exposed to the Internet, so it is critical that you understand the concepts not only in this chapter but in this entire book. We can't stress it enough: If you place Windows 2000 on the DMZ, pay close attention to hardening techniques and proper traffic flows, or you could be exploited.

In this chapter we covered how you can design a Windows 2000-based network solution that will work within and around the DMZ segment. It's important to know this as a security administrator or engineer because the DMZ can be very complex to work with and around. In this chapter you learned how to use your Windows systems within the DMZ design.

Lastly, this chapter focused not on learning Windows 2000 security concepts but how to design the proper DMZ layout. In other chapters you will learn the granular details needed to implement security, harden systems, and test those systems to ensure that they were secured properly.

This chapter should have served as a rough design document to help you place your Windows 2000 systems and the services they run within the DMZ. It is common for many administrators to wonder how to place their systems within the DMZ, especially when they are Web or FTP servers facing the Internet and publicly accessible. As

we mentioned in the chapter, it can be nerve shattering, especially with all the publicity Microsoft has gotten in the past as being an insecure system with many bugs, unchecked buffers, and a plethora of other problems resulting in becoming the biggest target seen on the Internet today. This chapter should help you to remedy those fears by providing you with the answers and solutions you need to not only place the systems in and around the DMZ but also to protect them.

Solutions Fast Track

Introducing Windows 2000 DMZ Security

- ☑ Before we look at the fundamentals of securing the DMZ segment and its hosts, we need a general idea of what it's going to look like on a map. All good network designers plan the topology (hopefully with a topology map) and figure out traffic flows, logical addressing, and any other factors that would affect the systems operating as advertised. If you choose not to follow this recommendation, you could find yourself very discouraged when the network does not function properly and systems cannot be accessed because of a simple (or complex) mistake you made in the design.
- ☑ The DMZ segment can be one of the most complicated segments on the network to design and implement. When you add Windows 2000 to the mix, you not only have to be an expert in security but also network engineering as well as Windows 2000 system design and the services to be made available. In sum, make sure you plan your implementation very closely.
- ☑ The three main sections you need to consider when building your Windows 2000 DMZ are network engineering, systems engineering, and security analysis.
- ☑ Your first step in designing a Windows 2000-based DMZ is to select all the networking hardware you will need. You must assess your needs, trying to figure out what the hardware infrastructure will cost your company. You need to look at needs first. When you are looking at the networking end of it, you should ask yourself, "What devices will I need, and how should I scale them?" Exploring these questions will bring about answers based on networking gear and costs.
- ☑ When planning your infrastructure, you always need to ensure that you plan the proper equipment list, no matter what vendor you pick. Basically, if you are purchasing this much equipment, presales support might be in order. Ask

you vendor to show you user limits per device (how many users can use this device without affecting its performance simultaneously) as well as the type of traffic you will be pumping through it. Often, the vendor can help you design your network so that you don't fall short on what you need or do not go overkill where you might not need the extra power.

- ☑ When you want to populate the DMZ with Windows 2000 hosts, you need to think about access to and from the DMZ and the services that are needed. The reason behind this initial thought is that your end users, customers, potential customers, and outsiders will be able to utilize resources needed and only those needed resources—nothing more, nothing less. To start the engineering process, you have to first make certain that you have these answers! What do you need? You should make sure that users can obtain the information that they need about your company without accessing the internal network and only by accessing the DMZ or accessing the Internal network safely if you chose not to implement a DMZ. If you can, it's always better to segment Internet-based resources via the DMZ for an added level of safety. Now that you know your network layout, you have to think about other access to and from the DMZ.
- ☑ Your secret, protected, confidential, and proprietary information should be stored behind your firewall and DMZ on your internal network. Servers on the DMZ shouldn't contain sensitive trade secrets, source code, or proprietary information, or anything that can be used against you or your company—or be used to exploit or hack your systems. (There's more on DMZ hacking techniques in Chapter 14.) A breach of your DMZ servers should at worst create an annoyance in the form of downtime while you recover from the security breach.
- ☑ A Web server that holds public information is a common example of a DMZ host. This can be IIS (since we are discussing Microsoft technologies in this chapter) or any other publicly accessible Web server. You can also think of FTP services, NNTP services, and other Web-based services to be accessed and utilized.
- ☑ Electronic commerce-based solutions always wind up on the DMZ. This is the front end of an e-commerce transaction server through which orders are placed. Keep the back end, where you store client information, behind the firewall. You want to design this properly because if you don't, you could potentially compromise your entire client database (or personal and private data) if it's exploited.

- ☑ A mail server that relays outside mail to the inside will be a highly utilized solution in the DMZ, especially since spam and other e-mail exploits are common DMZ host-based targets for attacks.
- ☑ VPN solutions are prevalent in the DMZ. Other than the site-to-site VPNs we already learned about, you also have VPN solutions in which you will have a remote access solution so that clients can attach over the Internet to get to their files and other data needed on the corporate network. This also has to be publicly accessible via the DMZ.

Building a Windows 2000 DMZ

- ☑ Depending on the model and type of firewall you use, you can in fact have different DMZ segments with different services on each to add even more security to your DMZ segments and hosts. This might be necessary if you plan to segment your DMZ hosts even further. This would mean that you could place an IIS load-balanced cluster on one DMZ and an e-mail relay on another.
- ☑ Your Windows 2000 solution revolving around the DMZ needs to allow for Internet access. The Internet connection should be able to handle the bandwidth needs of the site. If you are using this Internet connection as your LANs Internet access for surfing and e-mail and you decide to use it for a VPN as well, you need to analyze your requirements first.
- ☑ A traffic flow analysis can be done to ascertain the needed requirements (for WAN links, Internet connections, and so on) quite quickly, but you need to know how to do the analysis and have the tools to do so. If you do not, it is in your best interests to work with an outside vendor that does have the tools and experience to do so. Not doing so will almost always result in bad performance and increased cost later when you need to reprovision the lines to a higher bandwidth.
- ☑ Sometimes (if the size and complexity of the network dictate) you'll need a router on each leg of the firewall. At times, you will get requests to either add security to the segment you are working on or add more and more devices to it, where you might need to either route or direct traffic. Many firewalls will not route like a router; in other words, a typical firewall will route the RIPv1 protocol whereas a router will route IS-IS, OSPF, EIGRP, RIP, and so on. A router does just that—it routes. A firewall can in fact route if it's configured to do so, but often, depending on how paranoid you are, you might decide to

keep these services dependent on the device in which they sit. Keep your devices dedicated to what they do best when you can afford to do so and can use the added security.

- ☑ Too often, administrators mistake where to put DNS and WINS servers when working with the DMZ. Name resolution in the DMZ only matters if you in fact need it.
- ☑ Know how to place an e-mail server on the DMZ. There are really only two ways to place an e-mail server easily within a DMZ. For one, you can place the e-mail server (only one for this example) in the private network. The firewall in front of the e-mail server would be responsible for taking all requests in and out of the network and responsible for securing the traffic to the e-mail server. Due to the design of the server, it made the relaying of outbound Internet-based e-mail the responsibility of the e-mail server—only one single server. The question is then, however, "Why would we want to expose our e-mail server to the public Internet? What if there was a way to attack the e-mail server directly through the firewall?"
- ☑ It is common to simply add another e-mail server to the DMZ segment and use this as a relay to and from the protected e-mail server in the private network. The server now becomes an e-mail relay, and it will relay the mail to and from the Internet and to and from the mail server. If mail relays (IIS has an SMTP service that can be used as a relay) are compromised, you can simply reinstall the server from scratch and not lose a thing because all the server did was relay traffic. It is also common to not add any mail relay or forwarder to a Windows domain—again, because it will most likely be attempted for an exploit in the future.
- ☑ Web servers are the most common form of DMZ-based hosts today. Other services are needed, such as DNS and e-mail, but if you really think about it, the main reason DMZs even exist is because of the public Internet Web surfer feeding frenzy. Almost every company in the world now has a publicly accessible Web site, which means that just about every company worldwide either has an Internet presence or is looking to have one. Because of all these personal invitations to their corporate networks, it is imperative that you also think out your security completely or your network could be exploited.
- ☑ Organizations frequently have data they want to publish to the external network via a Web server. To allow direct access to the Web server via the Internet while the server is sitting in your private and protected LAN would be suicide. For that reason, we allow an external Web server to be placed on

the DMZ. This way, you can allow all your visitors to come directly to your IIS server and not have them exploit that server only to find ways to get to other systems. If the IIS server is external on the DMZ, you can at least have some defense against it if it is compromised in any way.

- ☑ The last (and very common) services to see on the DMZ both internally and externally are the DNS servers for your organization. DNS services are now more than ever the most common service used for name resolution. Because of DNS's growing use, it is important that when you lay out your Windows 2000 network, you are able to design the Internet namespace and the external namespace for the organization.
- ☑ Once you have finalized the DMZ network segment design and placed your systems where they need to be (and understand why they need to be there), you have to consider traffic and applications flows, ACLs, and filtering.

Windows 2000 DMZ Design Planning List

- ☑ To successfully start your Windows 2000 DMZ implementation, you need to start with our initial discussion on planning: network engineering, systems engineering, and security analysis.
- ☑ To properly plan your Windows 2000 DMZ, follow the steps in our checklist to get yourself from start to finish. You can use the list incorporated in the end of this chapter to do the planning you need.

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.

Q: I would like to protect my Windows 2000 DMZ. What do hackers use to test, check, and penetrate my DMZ?

A: Tools that allow people to eavesdrop on traffic are freely available on the Internet and can cause you much pain when you're trying to build a Windows 2000 DMZ. If you have NetBIOS traffic traversing your network, a network sniffer is all someone needs to learn, map, and disable your network. You need to think about the problems you could encounter while building your DMZ if you do let certain traffic traverse your network and over the Internet.

Q: I need to look at allowing specific traffic through my firewall, and I am unsure who handles such assignments. Where should I look for this information?

A: The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for managing port numbers. The well-known port numbers range from 0 to 1023. The registered port numbers range from 1024 to 49151. The dynamic and private ports range from 49152 to 65535. Most systems use the well-known port numbers to run system processes or privileged programs. The registered port numbers are not controlled by ICANN. Most of the time they are used with nonsystem processes or nonprivileged programs, such as an ordinary user running a program. Visit www.iana.org for more information.

Q: What is the most common form of DMZ-based system in use today, and what is commonly seen on DMZs big or small?

A: Web servers are the most common form of DMZ-based hosts today. Other services are needed, such as DNS and e-mail, but if you really think about it, the main reason DMZs even exist is because of the public Internet Web surfer feeding frenzy. Because of all these personal invitations to companies' corporate networks, it is imperative that you also think out security completely or your network could be exploited.

Q: I am planning out a new DMZ infrastructure. I am unsure about the hardware I need or what vendor to select. What should I do to start my plan?

A: When planning your infrastructure, you always need to ensure that you plan for the proper equipment, no matter what vendor you pick. Basically, if you are purchasing that much equipment, presales support could be in order. Ask your vendor to show you user limits per device (how many users can use this device without affecting its performance simultaneously) as well as what type of traffic you will be pumping through it. Many times, the vendor can help you to design your network so that you don't fall short on what you need or do not go overkill where you may not need the extra power.

Q: I want to implement a DMZ, but I am hearing from management that there might be a future need for an e-commerce site. How does this affect my design now? Should I plan for this functionality, even though I do not know exactly when it might happen?

A: If there is a need to eventually set up a load-balanced solution with multiple IIS servers and a possible backend database cluster, you should plan for it in the design stages of the initial DMZ setup so that you don't have to repurchase new gear for it later. You should also see if this can be amended into the project plan by the stakeholders and the project manager so that if possible, the need can be finalized and you can scale your equipment for it before, not after the fact. Always get a needs analysis and a future needs analysis done early in the design phase of the project so that you know what you might want to incorporate in the design (such as load balancing). If e-commerce is the need, this tells you that you need to scale the firewall, switches, and all other infrastructure to meet the needs for a possible e-commerce site, a load-balanced cluster, and so on.

Q: Why would I need a site-to-site VPN, and how does it affect my Windows 2000 DMZ design?

A: If there is a need to add more bandwidth and site-to-site VPN services off the external Internet routers, you should at least be familiar with the design and why you are implementing it. For one, the VPN used in this manner replaces your current Frame Relay or other WAN technologies, or if this is a new installation, you can forego using these technologies in the first place. All the VPN does is encrypt your data over a public or private medium so that you can have the private-line feeling without the private-line price premium. These are popping up left and right as companies try to save money, so it is important that you know how to design

them into your DMZ. You should also ensure that you purchase models either with crypto cards (to use IPSec for VPNs) installed or upgradeable to them

Q: When I plan my Internet connection, I am unsure as to what type of switch I need behind the external router, or if I even need a switch at all. Can't I just use a crossover cable to go from the router port to the firewall port?

A: If you need to scale up the number of connections to the Internet, such as the need for VPN services, intrusion detection systems, honey pots, other routers and so on, or you have other services that will be added sooner rather than later, you might need to put a switch in between the firewall and the external router. You might need more port availability on the switch so if you can get a switch, you have set yourself up to scale out in the future if needed. If this need is not there, you can skip this implementation and simply use a patch or crossover cable to connect your systems instead.