106

Creating a Secure Architecture

Christopher A. Pilewski
Bonnie A. Goins

106.1 What Is Network Security?

As discussed in the chapter entitled "Network Security Overview," network security may be thought of as the mechanism for providing consistent, appropriate access to confidential information across an organization and ensuring that information's integrity.

106.2 Why Is Network Security Essential?

An organization cannot leave itself open to any attack on any front; exposures, left unattended, may prove fatal to business continuance. In many cases, the government requires appropriate security controls. In the cases where there is no government mandate, business partners, vendors, and other entities may preclude conducting business with the organization unless it employs appropriate security mechanisms. This also extends to the creation and maintenance of a secure architecture.

106.3 Security Is a Process

Many organizations view security as a technology. This can be seen by the number of organizations that expect all security initiatives, as well as their planning, design, execution, and maintenance, to be carried out solely by technical departments, such as Information Systems, Application Development, or others. This is an incorrect perception. Technology most certainly plays a part in protecting an organization against attack or loss; however, the diligent provision of a secure architecture involves all aspects of the organization. *People* must be educated regarding their responsibilities for security and then enabled by the organization to properly carry out these responsibilities. *Processes* must be reviewed across the entire organization, to determine where assets reside, how they interact, the results produced from interactions, threats that may be present in the environment, and the mechanisms that protect organizational assets. *Facilities* must be evaluated to ensure that they are constructed and maintained appropriate to function. Security considerations must also be taken into account when evaluating a facility.

As if the resources necessary to properly address all the aspects listed above were not enough, all of these aspects must be evaluated periodically, over time. Why? Let us say an organization mustered a team to address all of these aspects, with the requirement that it detail any discovered exposures and fix them, as appropriate. Once completed, the organization is confident that it has done its work for the long term. Six months down the road, the government enacts legislation that requires executives to sign off on a document indicating that the organization has done its job and provided a secure environment in which to do business. The government gives all organizations six months to comply prior to audit. Any organizations failing to meet regulatory requirements will be fined, at minimum; at maximum, litigation and possible jail terms for personnel will also ensue.

Sound familiar? Organizations that will be bound by Sarbanes–Oxley legislation in July 2005 face this very scenario. Healthcare and financial organizations are enmeshed in meeting security and privacy regulations at this writing, through the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm–Leach–Bliley Act (GLBA).

Now go back to the scenario described above. Would it be prudent, as a senior executive, to sign an affidavit asserting that the organization is rock-solid from a security perspective with the information available from an assessment conducted six months ago? Perhaps the executive is not aware that the Information Technology department has performed a major network redesign over the past six months. Perhaps she has just been informed that Applications Development has completed and integrated a world-class data warehouse, developed entirely in-house. Human Resources has also informed her that the updates to employee job descriptions, as well as the personnel policy additions that commenced a year ago, are now complete and awaiting her signature. Would it be prudent, as a senior executive, to attest to the organization's security state using information that appears to be outdated?

This scenario, although it may seem unlikely at first inspection, happens daily in the business world. A static organization is one that has ceased to function. Because the natures of business and technology are dynamic, security must be periodically evaluated, as well as diligently documented and reported. A discussion of the security cycle follows.

106.3.1 Assess

As stated in the chapter entitled "Network Security Overview," an assessment is a snapshot, or a point-in-time view of the current state of security within an organization. While it is never possible to identify and neutralize all risks and threats to an organization and its function, the assessment process goes a long way toward identifying exposures that could impact the organization.

Some organizations argue that the moment an assessment is completed, it is out-of-date. While this argument may seem sound on its merits, and while the authors would concur that periodic assessment plays an important role in obtaining current information about an organization's state of security, organizations typically do not experience major changes on a daily basis, every day, for an extended period of time. Organizations that find themselves in a chaotic state of change, on a major scale and on a daily basis, may indeed require assessment on a more frequent basis, in order to accurately depict the changing environment.

106.3.2 Nonintrusive Assessment Methods

Nonintrusive security assessments provide a "snapshot" of the organization's current state. The final analysis relies on accurate and truthful representation by the organization and its interviewees. No assessment can discover 100 percent of the exposures within an environment and, as such, it is highly recommended that organizations review their current states of security periodically and diligently to minimize risk and threat.

It is important to note that nonintrusive assessments are very important to the health of the network. Based on the fact that network security is driven, as discussed, by people, processes, technology, and facilities, all these aspects must be appropriately assessed in order to provide a holistic view of network security.

106.3.2.1 Document Review

Documentation present within the organization is obtained and reviewed to provide background information for the security assessment. Documents evaluated vary, and typically include information security documentation, such as results from previous assessments and audits; security policies and procedures, disaster and incident response plans; service level, nondisclosure vendor and business partner agreements; insurance carried by the organization that relates to the network environment; network architecture designs and drawings; configurations of network devices, servers, and workstations; facilities blueprints; human resources policies; job descriptions; etc.

106.3.2.2 Interviews

Interviews are conducted with representation from each role in the organization as they fulfill the scope of the assessment. Roles typically interviewed include senior management, line or technical management, departmental management, full-time technical and business resources, and casual employees, such as part-time employees, temporaries, and interns. Sample size can be kept low, such as one to two appropriate interviewees per role, if the information obtained from the interviews can be generalized across the role for the organization.

106.3.2.3 System Demonstrations

System demonstrations are conducted with selected interviewees. This is done to verify information obtained during the interview, but also to gain insight into the technical operations of the organization, without intrusion, so that a determination can be made whether it is possible for users to bypass existing security controls. The assessor makes no attempt to access the organization's network; the interviewee is the "driver" and the assessor merely an interested observer.

106.3.2.4 Site Visits

Site visits, or "walkthroughs," fulfill a number of objectives during a security assessment. First, they provide the assessor with information relative to the physical security of the facility. Aspects observed can include appropriate, conspicuously posted evacuation instructions for personnel in the event of emergency; appropriate, conspicuously posted hazardous materials handling procedures; appropriate fire suppression equipment, such as extinguishers and FM-200 systems in any resident data center; appropriate climate controls; the presence of an access-controlled data or network operations center; appropriate facility construction (i.e., can the building withstand weather-related or catastrophic disasters?); "clean" workspaces (i.e., sensitive material is obscured from public view on walkthrough); inappropriate posting or otherwise public display of access credentials, such as user IDs or passwords; proper orientation of monitors and other display devices; any individuals inspecting visitors to the facility (i.e., receptionists, guards) and the methods by which they track facility access; etc.

Many organizations are distributed among multiple sites. It is important for assessors to determine whether it is prudent to visit each facility separately or whether there are sufficient and justifiable grounds for aggregating sites for reporting purposes. If aggregation for reporting does occur, it is still important to conduct the documentation and interviewing components of the assessment at these sites, either through standard telephone or video conferencing, or by another appropriate method. Substantiation of the information obtained should occur as soon as possible after the initial remote meeting.

106.3.2.5 Business Impact Analysis (BIA)

This method is often associated with the organization's business continuance efforts. As the method's title suggests, this assessment is conducted to determine how the loss of a particular asset or collection of assets impacts an organization.

The inventory and classification of assets in the organization is critical to the successful application of this method. Potentially, this is one of the most difficult tasks an organization can undertake. Where to start? A starting point for many organizations is to identify and document information assets, or data, present in the environment. This initiative can begin with any data that is sensitive within the environment. Unfortunately, many organizations do not have a data classification scheme in place; this makes determination of whether data is "sensitive" more difficult; fortunately, however, organizations can apply some common-sense rules to start this process. For example, healthcare organizations are bound by regulations that stipulate that all personally identifiable healthcare information must be kept strictly confidential; therefore, it follows that this information would be classified at the highest sensitivity level. The organization would then proceed to identify and classify data at the next level, and so on, until the task is completed. Many organizations choose to undertake this activity at a departmental level, so that it can be completed in a timely manner.

Threats to the assets, as well as countermeasures to those assets, are also evaluated in the method. This allows the organization to determine the impact of an asset or assets' loss to the organization. Data is then collated and presented to the organization for analysis and dissemination, as appropriate.

106.3.2.6 Risk Assessment

A risk assessment, or risk analysis, is a method that utilizes metrics to characterize exposures in the environment, as well as the probability of their occurrence. These assessments can be quantitative or qualitative in nature. If the organization has a significant amount of data it can employ in analysis, as well as a sufficient amount of time and resources, the analysis can be made more quantitative, or metric driven. If time, resources, and historic (or trend) data is not readily available, a qualitative (but still metric) analysis can be undertaken. Organizations interested in researching risk assessment will find a wealth of information on the Internet and in reference books, including this book. The Society for Risk Analysis is also a good site to visit for this information.

106.3.2.7 Auditing

Auditing is an assessment against the controls present to protect an organization. Control methodologies include COBIT; details on this method can be viewed through the ISACA (Information Systems Audit and Control Association).

106.3.3 Intrusive Assessment Methods

Intrusive methods are used in conjunction with data gathering to provide a more complete view of exposures to the environment. The following are some of the activities conducted during intrusive testing.

106.3.3.1 Footprinting and Enumeration

It is useful during the data-gathering process for the intrusive assessor to evaluate information that may be publicly available about the organization. Web sites, listservs, chat rooms, and other Web sources may contain information that has been illicitly obtained or has been posted by staff. Personnel may have a technology question that can be legitimately answered through the Internet; however, it is important to remember that the Internet is also mined for information by attackers. While the intent of the staff member may be good, posting too much information, or sensitive information, can give an attacker a leg up into the organization.

106.3.3.2 Social Engineering

It is highly impractical for an attacker to attempt a technological means of entry into an organization when tricking a staff member or obtaining sensitive information through "dumpster diving" or "shoulder surfing" is available and effective. Attackers using this method to obtain information prey upon people's desire to assist and their lack of understanding of security responsibilities, in order to gain access to an organization's resources. Social engineering is an activity that directly tests an organization's processes and its security awareness. Social engineers attempt to gain access to information or to restricted premises by means of distraction, misdirection, impersonation, or other means. Although social engineering is often performed anecdotally, it is a surprisingly effective activity. A common social engineering technique is to acquire an organization's phone directory and call its help desk impersonating a manager or an employee and demand that the target's password be changed to a simple word or phrase. Although it is a simple deception, it often works, particularly when shifts are ending. Other, more imaginative methods might employ social engineers disguised as package or food delivery persons, or as the organization's own uniformed staff.

106.3.3.3 Password Cracking

While many organizations provide guidance to staff regarding the construction and maintenance of passwords, many others do not. Intrusive assessors often use software tools to attempt to "crack," or break, passwords. These tools make multiple attempts to force the discovery of passwords used in the environment. This method is called "brute force." The majority of passwords can be discovered in an organization in a very short period of time.

106.3.3.4 Network Mapping

Network mapping is a technique used by intrusive assessors to "draw" the current network architecture. This "map" is used by the assessor and network administrators or information technology resources to review devices that are able to access the organization's resources. If there are any devices on the network that are unfamiliar to, or not approved by, the organization, they may belong to an attacker and, as such, should be disconnected from the architecture pursuant to the organization's security incident response plan.

106.3.3.5 Vulnerability Scanning

Vulnerability scanning uses open source or commercially available software to "scan" (probe) its target for specific technical vulnerabilities. The target may be a server, workstation, switch, router, firewall, or an entire network range. The information returned by the scanner can be quite extensive. It represents specific information about the target(s), such as the IP and MAC addresses, the operating system and version, and a list of that target's technical vulnerabilities.

The exact quantity and types of vulnerabilities that the scanner detects is the product of two factors: (1) the set of vulnerabilities that the scanner is instructed to look for (often called its profile), and (2) the vulnerabilities present on the target(s). It is possible for the target to have vulnerabilities that the scanner's profile does not instruct it to look for, and therefore are not found. Scanning profiles are often restricted to contain the time that the scan will take, or to help minimize the impact on the target device. It is also possible for a scanner to reveal vulnerabilities that the target does not have. These are called false positives. As scanning software evolves, false positives are becoming increasingly rare.

Common vulnerabilities discovered during scanning include detection of specific information that would lead, if exploited, to unrestricted access to the target device (an administrator account without password protection, for example, or anonymous read or read/write access to network objects). Other vulnerabilities reveal detection of services or protocols that permit or facilitate denial-of-service attacks or simply additional information gathering that could make further attacks possible.

While extremely valuable, data from vulnerability scanning should not be evaluated in isolation. Vulnerability scans frequently reveal information that requires further investigation to clarify. Most of all, vulnerability scanning should not be considered a substitute for security awareness and other measures.

106.3.3.6 Attack and Penetration

Attack and penetration can be thought of as the exploitation of a specific vulnerability, or a set of vulnerabilities, located by vulnerability scanning. The intent of attack and penetration is typically to determine the impact that successful exploitation would have. It may have a specific goal, such as a particular file or piece of information, or it may be more general. In a hypothetical example, successful penetration of a firewall could lead to successful access to an open service, or an openly writable directory on a server. This, in turn, may allow a keystroke logger to be surreptitiously installed where a variety of account names and passwords may be acquired and used later.

106.3.3.7 War Dialing and War Driving

Additional assessment activities may benefit an organization, depending on the environment. War dialing uses software programs to dial large blocks of phone numbers in an effort to locate modems on computers (or on other devices) that can be exploited later. Although war dialing can be time consuming, many commercially available programs can use multiple modems at a time to dial huge blocks of phone numbers in little time.

War driving is similar to war dialing. War driving uses commercial or publicly available software and hardware to detect wireless LANs, determine their characteristics, and break applicable encryption if detected. The war driver can "drive" from location to location looking for random wireless LANs, or use antennas to pinpoint and gain access to a predetermined wireless LAN from a great distance.

106.3.4 Remediate

When assessment activities have been completed and the data has been analyzed to determine where the organization is exposed, those exposures are then prioritized so that they can be appropriately addressed. Addressing and correcting exposures in an environment is called remediation. These fixes are typically activities resulting in a deliverable, such as a policy, procedure, technical fix, or facility upgrade, that satisfactorily addresses the issue created by the exposure.

106.3.5 Remediation Planning

Like any organizational initiative, remediation must be carefully planned for prior to its execution if it is to be successful. Given that resources, time, and dollars are finite, it is prudent to ensure from the onset that they are being utilized in a way that brings maximum benefit to the organization. Nonintrusive and intrusive assessment results must be carefully reviewed; exposures must be prioritized by severity level. This prioritization tells the organization how seriously it would be impacted if an exposure were successfully exploited. An organization might choose to remediate all of its "High" severity exposures as a precaution, or it might remediate exposures across the results. A good rule of thumb is never to fix something if it costs more than leaving it alone. For example, if an organization loses ten cents on a particular transaction that would cost twenty dollars to fix, dollars would be lost in the exposure's remediation. An exception would be any exposure that results in injury or loss of life; these exposures must always be corrected. Finally, if there is an exposure that costs little or nothing to fix, do so, even if it has a lower priority. If it costs nothing to fix, it will reap a benefit for the organization. Remember to calculate both resource time and dollars in the cost of remediation.

106.3.6 Remediation Activities

Remediation activities for organizations vary but may include recommendation of templates to serve as the foundation of a corporate security policy; recommendations for creation of appropriate targeted security procedures; review of an organization's business continuity, disaster, or incident response plans; review and implementation of the organization's technologies and architectures, from a security standpoint; identification of an appropriate scope of responsibilities and skill level for the security professionals; provision of ongoing executive-level security strategy consulting; high-level identification of educational processes and ongoing training required to support the organization's implemented security program; and other remediation activities, as pursued by the organization to meet its business, regulatory, and technology goals.

106.4 Layered Security for Network Architecture

Securing the architecture can be a complicated and confusing task. The network must first be properly assessed and documented in terms of its physical locations, links, and topologies. After a network itself has been properly assessed and documented, the constituent components should be known and indexed. The network perimeter can be clearly identified as the set of all entry and exit points into and out of the network. These also should be identified and indexed.

Typical entry and exit points include portals (or gateways) to the Internet, remote access servers, network connections to business partners, and virtual private networks (VPNs). Entry and exit points that are often unconsidered include the physical server rooms and wiring closets, unrestricted network wall ports, certain types of wide area network (WAN) links, and exposed computer workstations.

Technical safeguards can now be identified and discussed to help ensure controlled access to each entry and exit point. It may be tempting to address only the most obvious or convenient entry and exit points. This can be a serious mistake. While the relative priorities of different network perimeter entry points may be debatable, their importance is not. Locking a door is a sound security measure, but this practice is more efficacious when the window next to the door is not standing open.

A wide variety of technical safeguards and practices exist. Due to the inherent nature of networking technologies, the applicable safeguards are often less than completely effective. A layered approach is indicated in a secure network architecture where technologies and processes work together.

106.4.1 Perimeter Connection Security

Network perimeter connections can be thought of as the first layer of a comprehensive approach to secure network architecture. These connections should be listed individually and appropriate safeguards should be designed and implemented for each.

106.4.1.1 Internet Service Provider (ISP) Connections

An expanding universe of threats exists on the Internet. Attacks from sources on the Internet can be subtle and targeted at precise information that the attacker wants. Attacks can also be dramatic and highly destructive with motives that are unclear or esoteric. Many organizations already protect portals to the Internet with one or more network firewalls. Network firewalls can protect an organization from threats originating from other sources as well. A firewall is a network device that filters and logs network traffic based on a predetermined set of rules, typically called a rule base. Incoming network traffic can be forwarded or dropped. It can be logged in either case.

The correct use of network firewalls represents one of the most useful technical safeguards in a secure network architecture. Correct use, however, is critical. The firewall itself must be located in a secure location, such as a data center, where access is restricted and monitored. The firewall must be properly maintained. Its software operating system must be updated regularly, and it must be configured with a sufficient processor and sufficient memory to effectively use its rule base. The rule base itself must be aligned with the organization’s security policies, which must clearly define the network traffic that is permitted to be forwarded in and out of the organization.

An organization might have one ISP in a single physical location or it might have several ISPs in different locations around the world. Each connection must be identified and protected by a firewall. Properly used, network firewalls can be a highly effective safeguard to address threats originating from connections to the Internet and from a number of entry and exit points to the network.

106.4.1.2 Remote Access Connections

A variety of remote access technologies exist. These include dedicated phone lines, dial-up servers, wireless LANs, and others. Remote access connections must be listed completely and described with their individual business needs. This will allow for matching the appropriate safeguards to each connection identified.

Common remote access connections include two general types of connections: (1) those intended for end users and (2) those intended for use by an organization's Information Technology department. In both cases, the permitted use of these connections must be clearly identified. Specifically, this means that remote access connections must be described in terms of the information assets that they are intended and permitted to access. Dial-up lines or a dial-up server for end-user application or document access would be one example of remote access for end users. A modem connected to the serial port of a router would be an example of remote access for IT uses. In each case, the remote access connection should be configured to permit access only to the intended resources. The organization's security policies must make these information assets clear. Unrestricted forms of remote access should be avoided. Unrestricted forms of remote access can allow a remote computer that has been compromised (by a virus or a Trojan horse, for example) to compromise the organization's computer environment as well.

Access to remote access connections can be restricted by several means. As with connections to ISPs, remote access servers can be placed behind a network firewall (in a segregated network segment called a DMZ) so that only predefined network traffic that matches the firewall's rule base will be forwarded. Network firewalls are particularly effective at segregating network traffic. Other safeguards include thin-client or remote management solutions that access information indirectly. There are advantages to each approach, depending on business goals.

106.4.1.3 Business Partner Connections

Connections to business partners (usually vendors or customers) represent another type of connection that requires definition, examination, and appropriate safeguards. Business partners can connect to the organization with leased circuits, with VPNs, with modems connected directly to servers, or by other means. This type of connection requires similar measures as connections to ISPs and remote access connections. Many organizations will deploy safeguards on connections to their ISP but neglect to employ similar safeguards on connections to other organizations. There are numerous risks associated with unrestricted connections to business partners. If the networks of business partners are connected without the protection of a network firewall, a malicious party that manages to penetrate the partner's network has also penetrated yours.

Connections to business partners must first be fully listed. This may not always be a simple task. Connections to business partners can be confused with other WAN connections. Once they are

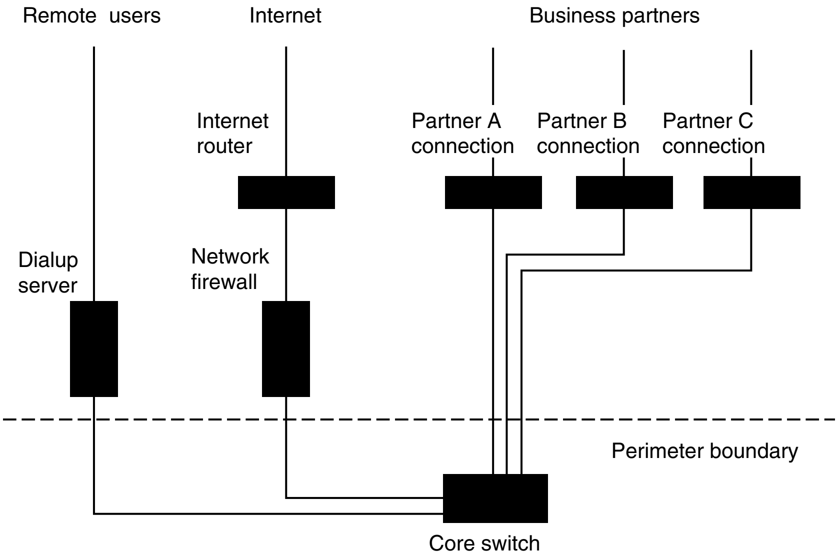

EXHIBIT 106.1 Network perimeter with protected internet connection only.

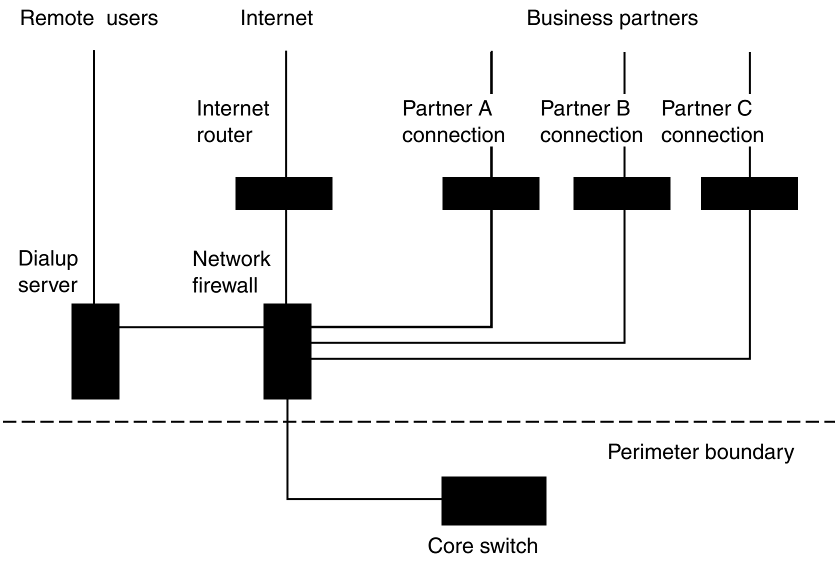

EXHIBIT 106.2 Network perimeter with protected connections.

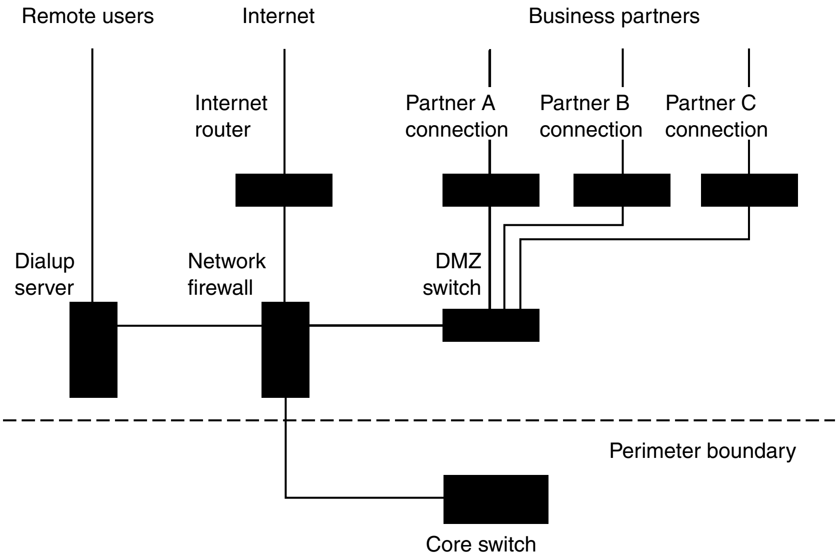

EXHIBIT 106.3 Network perimeter utilizing DMZ switch.

identified, permitted network traffic into and out of the organization must be explicitly defined in the security policy. For each connection, the intended far-end parties, the files transferred, and the applications used must all be identified and documented. This information will be used to construct an effective rule base for the firewall.

106.4.1.4 Perimeter Connection Security Examples

The typical network perimeter configuration shown in Exhibit 106.1 restricts access on some perimeter connections. The firewall protects the connection to the Internet but the dial-up server and business partners bypass the firewall and connect to the network around it.

The network perimeter configuration shown in Exhibit 106.2 restricts access on all perimeter connections. The connection to the Internet is protected by the firewall. The other dial-up servers and business partners connect through the firewall on separate DMZ ports. The firewall can filter and log network traffic with an appropriate set of rules for each connection.

The network perimeter configuration shown in Exhibit 106.3 also restricts access on all perimeter connections, but it employs another device in addition to the firewall. The connection to the Internet and the connection to the dial-up server are protected by the firewall. Business partners connect to the firewall through a separate DMZ switch.

This approach can make connecting business partners easier if the network firewall does not have enough ports for each external source to connect individually. This configuration is preferable to connecting business partners directly to the internal network (without protection), but certain considerations apply. Each business partner must be placed on ports belonging to separate virtual LANs (VLANs). If they are not connected in separate VLANs, two or more business partners could eavesdrop or interfere with each other's network traffic. Further, the firewall rule base must be configured to properly filter and log all the traffic sources connected to the DMZ switch.

106.5 Reassess

It is highly recommended that organizations revisit their environments post-remediation to ensure that the corrections have not created new exposures, and to identify any additional exposures that exist in the environment.

106.6 Summary

It is clear that securing a network, and indeed, network security itself, is process oriented and cyclic. To begin, a determination must be made as to the organization's current state of security. Multiple security assessment frameworks are available to facilitate the assessment process and should be selected based on alignment with the organization's business case and security objectives.

Once that determination has been made, it is possible to prioritize and to address the exposures present. A "layered security" approach permits the organization to correct the exposures by priority and to construct multiple barriers to delay or prevent attackers from exploiting network resources. This concept supports the notion that people, processes, data, technology, and facilities must be addressed during the creation and maintenance of a secure environment.