Chapter 1

Introduction to Intrusion Detection Systems

Solutions in this Chapter:

- Understanding the AVVID Architecture
- Understanding the SAFE Blueprint
- Threats
- Network Attacks
- Overview of IDS
- Defeating an IDS

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

Introduction

The Internet can be a dangerous and costly place. Since its inception, there has been a consistent and steady rise in network and systems security incidents in every existing business and government sector. And, in a world where the number of computers and networks attached to the Internet grows by the hour, the number of potential attack targets has grown proportionally, and now includes a large concentration of home users who are experiencing "always on" broadband connectivity for the first time.

At first glance, the numbers related to Internet security breaches can be staggering, both in terms of sheer frequency and financial impact. Market researcher TruSecure estimates that losses from computer crime in 2003 could total over 2.8 billion. The Code Red worm in 2001 alone caused an estimated $2 billion in damages and cleanup costs. Shortly thereafter, the Nimda worm was unleashed, with estimates of over $2.5 billion in damage.

In the eighth annual CSI/FBI Computer Crime and Security Survey, 251 of 530 companies surveyed reported combined losses of nearly $202 million, most of which stemmed from proprietary information theft and Denial-of-Service attacks. A bright spot in the 2003 CSI/FBI report indicated that reported losses of the companies surveyed dropped for the first time since the initial 1995 survey. This drop in costs occurred even though the number of attempted attacks did not diminish. Could this savings be attributed to increased corporate vigilance and attention to network security?

Perhaps most troubling of these figures, however, is the fact that many security incidents go undetected and most go unreported. Companies and governments readily admit they don't report incidents to avoid competitive disadvantage and negative publicity. Furthermore, the CSI/FBI report also indicates that a majority of known attacks occur from within an organization, proving that it is no longer adequate to "lock the front door."

A new scourge has become a reality as well; the threat of electronic terrorism is widely recognized as a real motivation for attack. Governments and terrorist organizations alike practice overt and covert techniques aimed at disrupting the very network and systems infrastructure on which we so heavily depend.

What can be done to combat these threats? And upon what can we rely as prevention in the face of this constant and genuine danger?

This book presents a combination of intrusion detection systems (IDS) and security theory, Cisco security models, and detailed information regarding specific Cisco-based IDS solutions. The concepts and information presented in this book

are one step towards providing a more secure working and living network environment. This book also exists as a guide for Security Administrators seeking to pass the Cisco Secure Intrusion Detection Systems Exam (CSIDS 9E0-100), which is associated with CCSP, Cisco IDS Specialist, and Cisco Security Specialist 1 certifications.

Cisco has developed two primary and dynamic components that form their security model, the Architecture for Voice, Video, and Integrated Data (AVVID) and the Secure Blueprint for Enterprise Networks (SAFE), that are intended as tools for network and security architects to assist in the efficient, modular, and comprehensive design of today's modern networks.

Along with AVVID and SAFE, Cisco has developed a Security Wheel to provide a roadmap for implementing enterprisewide security and a foundation for effective and evolving security management. Within these security models, Cisco has identified four security threat categories and three attack categories. Administrators should understand each of these categories to better protect their network and systems environments.

In addition to Cisco security theory, there exist many different types of IDS functions such as Network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). We'll examine each of these and other types throughout this chapter and describe in detail how IDS actually function to detect potential security events.

Finally, we'll discuss the potential issues and shortcomings of an IDS so that administrators can understand the limitations of their security devices. Hopefully, armed with this information, white hat security professionals can provide their organizations and governments proper, comprehensive, and forward-thinking security capabilities.

Understanding the AVVID Architecture

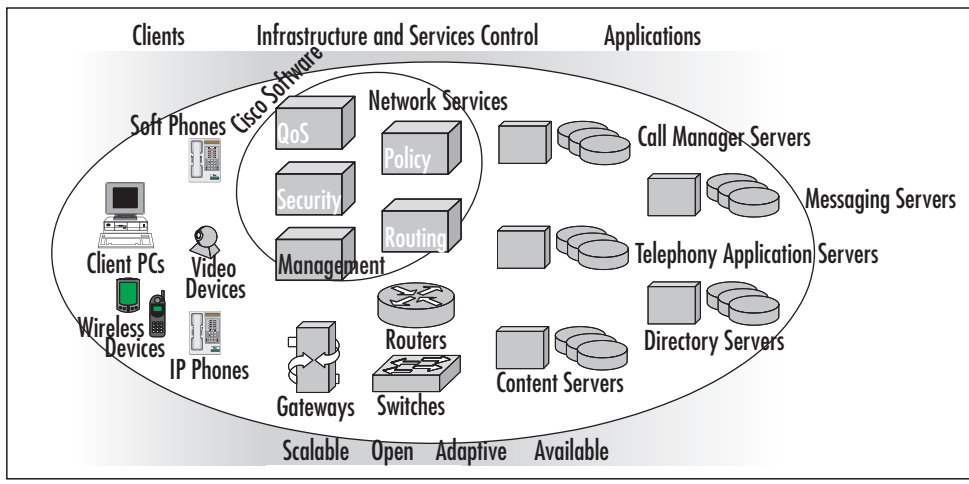
Today's networks transport an increasingly wide array of services such as voice and video, and application traffic including critical e-business and communication services. To assist network architects in the proper design of capable networks, Cisco created the Architecture for Voice, Video, and Integrated Data (AVVID). The AVVID architecture is based on an open, multiservice model and is composed of four interrelated, yet distinct layers as follows:

- Network Infrastructure Layer
- Services Control Layer

- Application Intelligence Layer
- Client Layer

The Cisco AVVID end-to-end architectural model is shown in Figure 1.1.

Figure 1.1 The AVVID Architectural Model



The Network Infrastructure Layer provides the groundwork for the AVVID architecture and is composed of switches, firewalls, IDS, VPN and security appliances, gateways, and routers. These are the devices and services that provide the foundational transport mechanisms for the network. It is in the Network Infrastructure Layer that intelligent logic is functionally applied, providing QoS, security, wire speed switching, and appropriate routing. Specific examples in the Network Infrastructure Layer might include Cisco Catalyst 6500 switches, Cisco PIX firewalls, Cisco 4200 Series IDS, and Cisco 7500 Series routers.

The Services Control Layer provides management of mechanisms applied in the Network Infrastructure Layer such as QoS and policy control, content distribution control, wireless access control, and call control, among others. This layer is composed of control consoles uniquely suited to assist in the management of the complexities present in the Network Infrastructure Layer. For instance, the CiscoWorks management modules and the PIX Device Manager are both examples of systems that could be present in the Services Control Layer.

These components provide reliable and efficient communication between the Client Layer, composed of AVVID appliances such as IP phones, wireless devices, PCs, and video equipment and the Application Layer. The Client Layer has

become increasingly sophisticated in recent years to fully leverage the growing list of advanced applications that promote enhanced business functionality. This sophistication places demands on the Network Infrastructure Layer for increased throughput, reduced latency, and more focused services. For example, the network capabilities delivered to the IP Telephone switch port might be different than those provided to a typical desktop workstation switch port. This could be provided by ingress port QoS classification and marking in the Network Infrastructure Layer and controlled via the Services Control Layer, which proves the need for holistic and comprehensive AVVID design.

The Application Layer provides the tools and logic that promote more efficient and capable business processing. The Application Layer includes functionality such as telephony application, messaging, video content distribution, and e-commerce services. Each of these services relies on the proper implementation of the Network Infrastructure Layer. An example of an Application Layer component is Cisco Call Manager. This application provides the functionality and logic behind the IP phones within the enterprise. It relies on other applications such as Directory Services to provide authentication and unique services to each IP Phone user. Along with the Client Layer IP Phones, it also relies on a well-built and functional network over which it can provide services.

The overarching theme of the AVVID architecture is the use of a single converged IP network for voice, video, and data traffic. Doing so facilitates gains in operational and technical efficiency, and reduces total cost of ownership for those migrating from traditional separation of services across multiple infrastructures. AVVID also incorporates centralized control and management of the infrastructure for increased administrative productivity.

The benefits of AVVID are

- **Integration** By using the Cisco AVVID architecture and applying the network intelligence imbedded within IP, companies can develop comprehensive tools to improve productivity.
- **Intelligence** AVVID promotes the prioritization of traffic and delivers intelligent network services to maximize network efficiency and performance.
- **Innovation** Cisco customers can adapt quickly to a changing business environment.
- **Interoperability** Standards-based APIs enable integration with third-party developers.

With the increased dependence on the IP network infrastructure comes amplified requirements for network capacity, QoS, resiliency, and security, however. These critical network attributes are imbedded throughout the Cisco AVVID architecture. For additional information regarding Cisco AVVID, go to www.cisco.com/go/avvid. To address the need for security, Cisco developed the SAFE blueprint, which augments the AVVID architecture.

Understanding the SAFE Blueprint

Another powerful tool available from Cisco for security administrators is SAFE, a security blueprint for enterprise networks. The SAFE blueprint builds on the Cisco AVVID architecture by incorporating best practices and comprehensive security functionality throughout the infrastructure. Fundamentally, the SAFE blueprint reinforces the absolute need for security in modern enterprise networks and details the management protocols and functions necessary to administer the security infrastructure.

The benefits of SAFE are

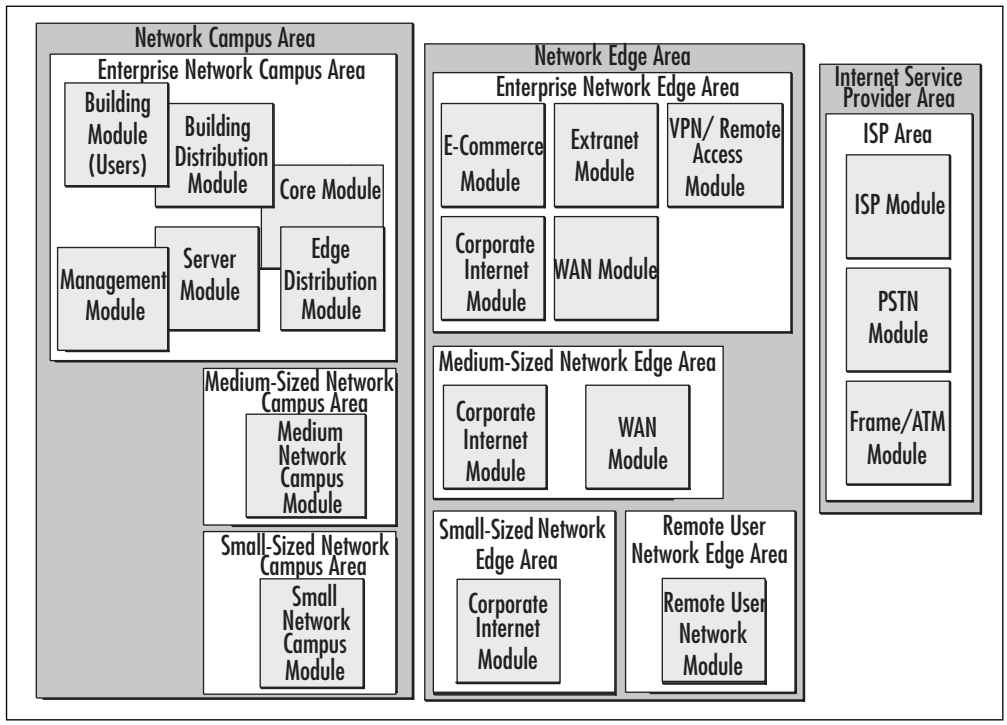
- SAFE provides a detailed blueprint to securely compete in today's Internet and interconnected economy.
- SAFE provides a solid foundation for migrating to a secure and cost-effective network.
- SAFE, by being modular in design, enables companies to stay within their budgets.
- SAFE provides protection at each access point to the network using best-in-class security products and services.

SAFE is organized by network area as follows:

- Network Campus Area
- Network Edge Area
- Service Provider Area

Each area is modular for consistent and rapidly deployable security throughout the enterprise, when and where it is needed. When network managers use SAFE to design their security, the security architecture does not need to be redesigned each time a new service is added to the network. Each area has several modules addressing size and site-specific security functionality. The SAFE blueprint is depicted at a high level in Figure 1.2.

Figure 1.2 The SAFE Blueprint



Each of these modules incorporates designs for maximum performance, yet ensures security and integrity. SAFE modules are designed to address several network attributes including, but not limited to, security and threat response, secure management, availability, scalability, QoS support, and voice support.

Additionally, Cisco has updated the SAFE blueprint with new modules that incorporate Wireless LAN and IP Telephony security. Both address small-, medium-, and enterprise-sized environments and include design topics similar to those listed earlier.

Let's look as these areas in more detail.

The Network Campus Area

The SAFE blueprint includes security architectural information specific to the size of the networks and includes details for small, medium, and enterprise-sized networks. Regardless of size, however, the Campus Area includes security services directed primarily to the internal, corporate user. Common security infrastructure within the Campus Area includes packet filtering and VLAN-capable switch

devices, virus scanning systems, intrusion detection, and security management solutions to name a few.

Let's look a little closer at what each sized campus module provides within the SAFE blueprint.

The Small Campus Module

The Small Campus Module provides security infrastructure sized appropriately for budget-conscious and small organizations. Included within the Small Campus Module are intrusion detection systems, virus scanning servers, proxy devices, and security management systems. Within the Small Campus Module design, users are trusted more internally due to budget and size. For example, internal firewalls to separate Accounting from Engineering may not be practical based on cost.

The Medium Campus Module

The Medium Campus Module is similar to the Small Campus Module, yet includes more security infrastructure to provide protection for an increased number of people and services. For instance, in addition to the security implemented in the Small Campus Module, the Medium Campus Module includes switches capable of separating users via VLANs and filtering based on Layer 3 and 4 attributes. Critical services such as Call Management or Accounting Servers are separated by stateful inspection firewalls. Intrusion detection systems are more capable in the Medium Campus Module and can provide focused analysis in Layers 4 through 7. As in the Small Campus Module, the Medium Campus Module includes network management systems, virus scanning gateways, and proxy devices.

The Enterprise Campus

The Enterprise Campus Area within the SAFE blueprint is targeted at large organizations that may span several geographical locations and provide a multitude of user-focused internal services. The Enterprise Campus is large enough to warrant the creation of several modules, each addressing specific security requirements within the Campus. Let's look at these modules, starting from the user edge and working towards the services.

The Building Module

The Building Module might best be thought of as the Access Layer in the traditional tiered network architecture model. It is where the users are connected to

the network and includes virus scanning software, personal firewalls, and VLAN-separated user space.

The Distribution Module

Within the SAFE blueprint, there are two types of Distribution Modules, a Building Distribution Module and an Edge Distribution Module. As they both contain similar security infrastructure and largely provide the same type of network services, we'll discuss both of them in this section.

From the Building Module, the user traffic is directed through the Building Distribution Module. This module acts as a transport area to quickly provide access to the core networks. Within the Building Distribution Module, security features include RFC 2827 filtering to prevent DoS attacks and address spoofing and continued VLAN separation. Layer 3 separation may also exist if routing occurs in the Building Distribution Module.

The Edge Distribution Module serves as the security handoff to the Network Edge Area, which we'll discuss in a moment. Like the Building Distribution Module, the Edge Distribution Module also includes RFC 2827 filtering and, potentially, Layer 3 access control.

The Core Module

As is traditional in core networks, very little security infrastructure is included so as to not impede high-speed transport across the campus. While the Core Module does not call for security features, there are an increasing number of security devices, such as IDS and firewalls, that can potentially exist within the Core based on their high-speed performance.

The Server Module

The Server Module specifically addresses the needs of server farm or other service areas. Many security capabilities are present in the Server Module to protect enterprise assets such as directory services, messaging servers, DHCP, VoIP Call Management services, and the like. Included within the Server Module are stateful inspection firewalls and packet-filtering devices, IDS in the form of HIDS and NIDS, and VLAN-capable switches.

The Management Module

The Management Module exists as the command and control module for the entire SAFE blueprint. It is within this module that security support infrastruc-

ture resides. The Management Module can include the following services and capabilities:

- AAA services such as Cisco Secure ACS for network device access control
- SNMP-based network monitoring and control services, such as CiscoWorks
- Syslog servers for comprehensive error and event data capture
- Out-of-band (OOB) network access and infrastructure
- Two-factor authentication systems such as SecurID servers
- Device configuration management systems for revision control
- VPN termination systems for remote, secure management

In addition to these services, the Management Module is itself protected by focused Layer 4–7 IDS analysis, various traffic filtering mechanisms such as router filters and stateful inspection firewalls, and, as in other modules, VLAN-capable switches for Layer 2 separation.

The Network Edge Area

Similar to the Network Campus Area, the Network Edge Area consists of security architectural information specific to the size of the networks that includes details for small-, medium-, and enterprise-sized networks. The Network Edge Area also includes a Remote User Network Module focusing on home office and remote access networks. Furthermore, each specifically sized Network Edge Area addresses security regarding the more publicly available services a company may provide. This Area also includes the security features necessary to safeguard an organization's connection to the Internet.

Let's look more closely at the Network Edge Area as it applies to differently sized companies.

The Remote User Network Edge

The Remote User Network Edge Module provides security for users working from external locations such as home offices or small remote offices. There exist four connectivity options within the Remote User Network Edge Module as follows:

- **Software Access Option** Users connect to the central office via VPN and authentication software installed on their computer workstation. Users may have broadband connectivity, but most likely rely on dialup access for remote connectivity. This is the simplest option for remote connectivity.
- **Remote Site Firewall Option** A firewall device is used in this option for more permanent and robust secure remote connectivity. This option infers a broadband connection and provides stateful inspection and/or Layer 7 packet filtering. VPN access and authentication services can be located at the firewall or on the user's computer workstations in this option.
- **Hardware VPN Client Option** Similar to the Remote Site Firewall Option, the Hardware VPN Client Option uses broadband network connectivity and provides VPN and authentication services on behalf of the user. This option relies on user workstation personal firewall software for perimeter security, however.
- **Remote Site Router Option** Nearly identical to the Remote Site Firewall Option, this option uses a router with firewall capabilities to provide perimeter packet filtering and may include stateful inspection and/or Layer 7 filtering capabilities.

Regardless of the connectivity options, the Remote User Network Edge Module includes security infrastructure typical of user network areas such as virus scanning systems, HIDS, and personal firewalls.

The Small Network Edge

The Small Network Edge combines economical and appropriate security measures to protect smaller organizations. The Small Network Edge includes one module, the Corporate Internet Module.

The Corporate Internet Module

The Small Network Corporate Internet Module acts as the demarcation between the company's assets and the ISP Area. It also serves to protect the application systems that the company provides to the public, such as web, database, and mail servers.

The security infrastructure present in the Small Network Corporate Internet Module includes perimeter stateful inspection firewalls, Layer 7 filtering capabili-

ties, and IDS in the form of NIDS and HIDS. The Small Network Corporate Internet Module also includes Remote Authentication services, VPN termination devices, and VLAN-capable switches.

The Medium Network Edge

The Medium Network Edge includes more advanced and comprehensive security mechanisms to protect the larger asset and employee base of the medium-sized company. It includes two modules, as discussed next.

The Corporate Internet Module

Like the Small Network Edge Corporate Internet Module, the Medium Network Edge Corporate Internet Module includes perimeter stateful inspection firewalls and Layer 7 filtering capabilities. These serve to protect the corporate internal networks and services. This module has more focused IDS capabilities, however, and also includes content inspection for mail services, more robust VPN termination, and scalable authentication services.

The WAN Edge Module

The Medium Network Edge has a second module to address WAN connectivity needs. This module may include packet-filtering capabilities, but most likely it simply provides reliable and secure transport to remote office locations.

The Enterprise Network Edge

The Enterprise Network Edge Area within the SAFE blueprint is targeted at large organizations with various customer-focused, publicly available services in several locations. The Enterprise Network Edge necessitates the creation of several modules, each addressing specific security requirements within the Edge Network. We'll discuss these modules in the following pages.

The E-Commerce Module

The E-Commerce Module is intended to house and protect the business-driving public infrastructure of the organization and includes database, application, and web services components, among others. To provide a comprehensive defense, the SAFE blueprint calls for focused Layer 4–7 IDS analysis and Host IDS capabilities. Furthermore, multitiered stateful inspection firewalls and packet-filtering devices are included for perimeter defense. Wire speed switching on VLAN-

capable switches provides server connectivity in the E-Commerce Module for fast, efficient server access.

The Corporate Internet Module

The Corporate Internet Module provides secure connectivity for internal corporate users to the Internet. It also offers logical space for inbound and outbound services such as SMTP, web proxy, and content inspection servers. This business functionality is protected with stateful inspection firewalls, Layer 7 filtering, spoof mitigation, and other basic filtering. It also includes advanced and focused Network IDS analysis and host-based detection systems.

The VPN/Remote Access Module

Due to the potential size and scaling requirements of Enterprise-sized VPN solutions, the Enterprise Network Edge Area includes a VPN/Remote Access module. This module contains the required encryption, VPN termination points, and authentication mechanisms for the Enterprise environment. Included in this module are various IDS components that are placed at the encryption endpoint to inspect inbound and outbound VPN traffic. Stateful inspection firewalls are also integrated into the VPN/Remote Access Module for perimeter security from, and to, remote connections.

The Extranet Module

The Extranet Module is similar to the E-Commerce Module in that it houses application and web-based services. Extranets are typically intended to facilitate access by semi-trusted users such as partners or other remote entities. Like the E-Commerce Module, the Extranet Module includes NIDS and HIDS, as well as stateful inspection firewalls. It also includes authentication and VPN termination services for remote use.

The WAN Module

The Enterprise Network Edge WAN Module includes sparse security features to facilitate efficient network transport. The WAN Module may include Layer 3 access control mechanisms for secure transport.

The Internet Service Provider Area

The Internet Service Provider Area as described by the SAFE blueprint provides companies and organizations with a secure and high-speed transit network to the

public Internet. While the ISP Area is outside the enterprise-, small, and medium-sized business network demarcation, it too includes security features to protect customers and the ISP network itself.

The ISP Area contains the following three modules:

- The ISP Module
- The PSTN Module
- The Frame/ATM Module

Of these modules, the PSTN and Frame/ATM Modules do not include many security mechanisms other than self-protective ACLs and filters on network equipment to protect the ISP routers, switches, and telephony infrastructure.

The ISP module, however, typically includes spoof mitigation, DoS limiting features, and some limited Layer 4 filtering capabilities. These are typically intended to protect the ISP itself, yet as network-based attack frequency and sophistication rises, ISPs face increased pressure to help combat security incidents through additional security mechanisms.

SAFE Axioms

The SAFE blueprint includes key devices to be deployed in each module along with design guidelines and alternatives, and potential threats mitigated by the solution. All of this design information is predicated on several SAFE axioms that follow:

- Routers are targets
- Switches are targets
- Hosts are targets
- Networks are targets
- Applications are targets
- Intrusion detection systems are necessary
- Secure management and reporting are necessary

In the blueprint, each of these axioms has comprehensive mitigation techniques and implementation guidelines.

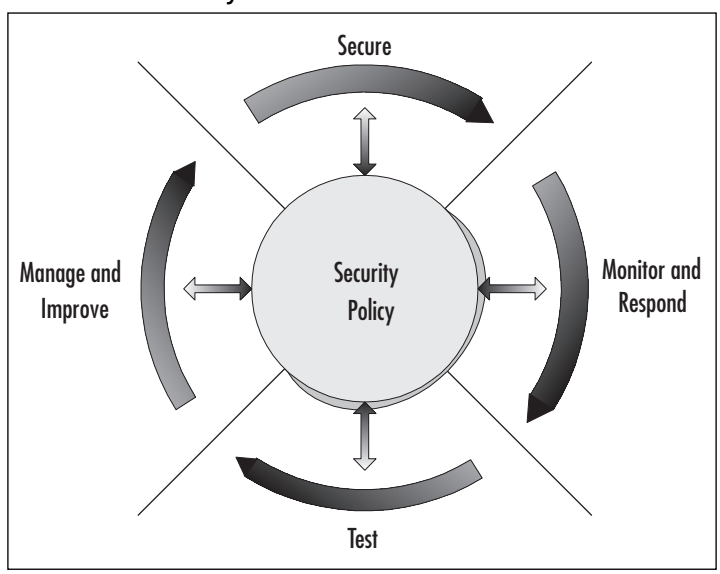
The SAFE blueprint is a detailed and holistic approach to securing the enterprise. It includes in-depth defense strategies and multidisciplined approaches for

security. Security administrators should be familiar with the SAFE design. For additional information regarding Cisco SAFE, go to www.cisco.com/go/safe.

The Cisco Security Wheel

Implementing a comprehensive security stance is critical in successfully defending one's network and services infrastructure. To do so, Cisco recommends a cyclical, evolutionary approach depicted by a wheel (as shown in Figure 1.3) known as the Cisco Security Wheel.

Figure 1.3 The Cisco Security Wheel



This approach incorporates the following repetitive methodology:

1. **Corporate Security Policy** Instantiate a solid security policy.
2. **Secure** Secure all existing networks and systems.
3. **Monitor and Respond** Monitor the infrastructure and respond accordingly to events.
4. **Test** Regularly test security systems, including human response capabilities.
5. **Manage and Improve** Effectively manage and continually improve the security stance.

Use of this methodology can help provide a holistic and evolving security plan that keeps pace with the ever-changing threats present in today's technical environment. Each of these steps is discussed in detail in this section.

Corporate Security Policy

All effective security measures start with a good, comprehensive security policy. Developing a written and well-defined policy must be the first step in addressing an organization's security needs. Indeed, all efforts, both tactical and strategic, should flow from the policy. Furthermore, as a company practices the methodology ascribed by the Security Wheel, the security policy should become an integral feedback mechanism to measure success and failure and should be updated as the need arises.

The security policy should contain a complete set of proactive and reactive measures that an organization should take to prevent, or react to, security events. The security policy should also address the following items: roles and responsibilities, clear delineation of acceptable behavior, and definition of data sensitivity classification. The repercussions of breeching security policy should also be documented. Other considerations within the security policy include the delineation of:

- The incident response team
- The security team
- Response procedures
- Communication procedures
- Logging procedures
- Training/rehearsal plans

Once a clear, balanced policy has been constructed, it must be approved by an organization's stakeholders, such as Executive managers, Human Resources Staff, IT and Security Staff, Legal personnel, and others. With this buy-in, the policy can be universally and consistently enforced rather than being relegated to a shelf in the document library.

There are many resources regarding policy formation available to the security administrator. Good starting points include *RFC 2196 – The Site Security Handbook* (www.ietf.org/rfc/rfc2196.txt) and the SANS "Design and Implementation of the Corporate Security Policy" document (www.sans.org/resources/policies). Ample time should be dedicated to developing a good security policy. Above all, the policy should be realistic, flexible, and should be easily understandable by all within the organization.

Secure

Securing the network involves the intelligent placement of security devices such as firewalls, IDS, and other systems. Before doing so, however, the security team should have a detailed knowledge of the network in which they work. This involves gathering and understanding attributes such as overall network size and topology, ingress and egress points, service locations, and general application flow parameters. Understanding the traffic and how it flows across the network is an essential step in security implementations.

Securing the network also involves the security policy established in the first step of the methodology. Each network and organization differs in their needs, which is why a tuned security policy is necessary. Security administrators will find that the following security solutions are required:

- Access Control
- Encryption
- Authentication
- Vulnerability Patching

Access Control

Access control mechanisms can take many forms. Perimeter barrier devices are often first considered when securing a network. Firewalls in the form of packet filters, proxies, and stateful inspection devices are all helpful agents in permitting or denying specific traffic through the network. Access controls also exist on end systems in the form of a privilege level for access to resources, configuration files, or data.

NOTE

Securing the enterprise requires intimate knowledge of your infrastructure including network design, services locations, and data traffic flow attributes, among others. Knowing these details allows you to place IDS and perimeter security devices such as firewalls in the most effective locations to prevent unwanted intrusions. Without this knowledge, administrators will waste corporate resources by over-deploying security infrastructure, or worse, missing unseen attack avenues into the enterprise.

Encryption

Encryption in the form of IPSec, PPTP, or other protocols can help ensure confidentiality of data transport within networks and between networks. Virtual Private Networks (VPNs) are often cost-effective measures to facilitate private communication across a shared network infrastructure.

Authentication

After thorough planning, security support infrastructure such as authentication, authorization, and accounting (AAA) systems can be implemented to provide verification for access and privilege control through firewalls and VPNs to services. Cisco offers Secure Access Control (ACS) as a means of implementing AAA. Several varying degrees of authentication can be integrated with AAA such as clear-text passwords, Microsoft CHAP, S/Key and SecurID. Administrators should set up logging capabilities for historical and forensic data analysis and monitoring.

Vulnerability Patching

Securing the network also means securing the systems on which services reside. Staying current with patches, operating systems, and application software revisions can mitigate commonly used attack vectors. Policy should dictate regular and systematic upgrades to organizations' software-based systems.

Administrators should regularly check for security patch updates on vendor web sites and newsgroups. Some examples of vendor patch and security advisory web sites are:

- **Microsoft** http://windowsupdate.microsoft.com
- **Sun Microsystems** http://sunsolve.sun.com
- **Red Hat Linux** www.redhat.com/apps/support/errata/
- **Cisco** www.cisco.com/warp/public/707/advisory.html

Finally, securing the network includes the implementation of physical security measures. The best network security methods can prove meaningless without solid security to protect against physical access to servers, firewalls, and other network equipment. Cipher systems, and identity cards and verification systems are all examples of ways to improve physical security.

Monitor and Respond

Once the environment is secure, the next step in the Cisco Security Wheel is realization of comprehensive monitoring and response techniques. This means the use of documented and policy-directed software and human practices to ensure full awareness of potential security events.

Software systems include well-tuned alert thresholds and logging mechanisms on the devices used to secure the network, such as firewalls, IDS, and AAA servers. It is absolutely critical that the reporting mechanisms are properly configured, however. Otherwise, security administrators will be overwhelmed with false-positive data and will be rendered ineffective in actual security situations. Furthermore, in large enterprise environments, it is quite impossible for humans to keep pace with copious logs and alert messages, even with well-configured devices; there is simply too much data to analyze. In these situations, additional software to perform event aggregation and correlation proves necessary to alleviate data overload.

In addition to well-constructed software mechanisms, security administrators must practice proper and methodical monitoring techniques. Administrators should baseline and understand the normal attributes of the network so as to recognize anomalous events. Regular and repeated practices in log and alert monitoring can reduce the chances of missing the precursory events of security attacks and stave off damaging situations before they occur.

With good human and software monitoring techniques, most security issues can be detected. It is at the point of detection that defined and practiced response measures must be implemented. Some responses may be automated, such as automatic shunning or filtering based on an IDS signature detection. Most responses will likely be manual, however. In these situations, administrators should have clear roles and responsibilities to mitigate the effects of an attack and alert upstream authorities, both inside and outside of the organization. Well-developed security policies are often helpful in delineating such roles, responsibilities, and actions.

Finally, administrators should also be prepared to react dynamically in atypical and new security situations. Again, security policy can aid in these situations by defining the realm of the administrators' authority and obligation.

Test

Through the use of the Cisco Security Wheel, an organization may have developed a strong security policy, secured the network properly, and implemented compre-

hensive monitoring and response techniques. The next step is to thoroughly and regularly test these constructs to ensure validity, accuracy, and effectiveness.

Testing can take the form of scanning across firewalls, servers, and IDS to ensure correct configuration. Oftentimes, an organization will seek external audits of the infrastructure for objectivity. Testing should also include assessment of administrative responses through mock events and practice drills. Doing so not only helps identify areas of weakness, but provides training and rehearsal time to finely tune the security team's responses.

Testing should be regular and repetitive, and should be clearly defined in the security policy.

Manage and Improve

Finally, as a security team practices the methodology of the Cisco Security Wheel, they should seek to continually improve their capabilities through proper management. This involves not only the cyclical actions associated with the Security Wheel, but also the unrelenting defense against new and unknown threats.

Good security management includes continuous education through training, practice, and reading. Administrators should keep pace with security newsgroups and publications and should appreciate potential vulnerabilities as they are discovered and before they are automated.

Postmortem sessions after security events should be conducted to investigate lessons learned and reveal places for improvement. Administrators should develop education systems for the employees of the organization who may not be well-informed of good everyday security practices.

The threats against and consequences of participating in the networked environment have not, and will not, stop changing and challenging those who seek to protect an organization's assets. Above all, the security team and infrastructure of an organization must continually evolve to defend against such threats.

Threats

The threats against an organization's networks and systems can be categorized into four general types, as follows:

- Unstructured
- Structured