Your Short Cut to Knowledge

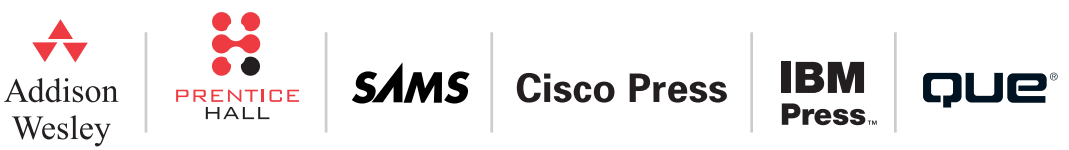
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



Network Security

An enterprise network design must include security measures to mitigate network attacks. Fortunately, with the modularity of the Cisco Enterprise Architecture, you can address security concerns on a module-by-module basis. This section introduces the concept of a security policy, reviews various types of network attacks, discusses the elements of the Cisco Self-Defending Network, and helps you select appropriate security design components for the various locations in an enterprise network.

Network Security Concepts

Organizational requirements and potential threats drive the scope of a security design. At its essence, network security measures should not only defend against attacks and guard against unauthorized access, these measures should also prevent data theft and comply with security legislation, industry standards, and company policy.

Consider the following threats and risks facing today's enterprise networks:

- **Threats:**
  - **Reconnaissance**—A reconnaissance attack gathers information about the target of an attack (for example, the customer's network). For example, a reconnaissance attack might use a port-scanning utility to determine what ports (for example, Telnet or FTP ports) are open on various network hosts.
  - **Gaining system access**—After attackers gather information about their target, they often attempt to gain access to the system. One approach is to use ***social engineering***, where they convince a legitimate user of the system to provide their login credentials. Other approaches for gaining access include exploiting known system vulnerabilities or physically accessing the system.
  - **Denial of service (DoS)**—A DoS attack can flood a system with traffic, thereby consuming the system's processor and bandwidth. Even though the attacker does not gain system access with a DoS attack, the system becomes unusable for legitimate users.
- **Risks:**
  - **Data confidentiality**—Companies should ensure that sensitive data on their systems is protected against theft. Without such protection, the company might be subject to legal liabilities and damage to the organization.
  - **Data integrity**—Besides stealing data, attackers could also modify sensitive data. Therefore, security measures should only allow authorized users to alter data.
  - **Data availability**—As previously mentioned, a DoS attack could make a system (and therefore the system's data) inaccessible by legitimate users. Therefore, security measures should be used to maintain system and data availability.

CHAPTER 6

When designing a network security solution, realize that although hosts are the primary targets of an attack, other potential network targets also need protection. Other potential attack targets include routers, switches, DHCP/DNS (Dynamic Host Configuration Protocol/Domain Name System) servers, user PCs, IP phones, and IDS/IPS (intrusion detection system/intrusion prevention system) devices, in addition to the bandwidth available in the network infrastructure.

To guide security design decisions and provide a guideline to future security enforcement, organizations need to formulate a ***security policy***. A security policy is a documented set of rules that specify how people are allowed, or not allowed, to access an organization's technology and data.

Other considerations in a security design include the following:

- **Business needs**—Determine what the organization wants to accomplish with their network.
- **Risk analysis**—Determine the risk/cost ratio for the design.
- **Industry best practices**—Evaluate commonly accepted industry best practices for securing a network.
- **Security operations**—Define the process for monitoring security, performing security audits, and responding to security incidents.

In addition to a security policy, organizations might need to prepare the following documents to address specific risk categories:

- **Network access control policy**—This document defines levels of data security (for example, confidential or top secret) in the network and outlines procedures for gaining access to different security levels.
- **Acceptable-use policy**—This document should be distributed to all end users and be clear for what purposes a user is allowed to use the system and what types of data can be retrieved by the user.
- **Security management policy**—This document describes how an organization manages its network security.
- **Incident-handling policy**—For when security incidents occur, this document describes an orderly set of procedures for responding to the incident or an emergency situation.

The previously described security policy is a continually evolving document that changes in response to technology and organizational requirements. Like the continually evolving security policy, the process of securing the network is also continuous. Specifically, designers use the following four steps to continually secure the network, as illustrated in Figure 6-1:

- **Secure**—Securing the network involves such measures as authorizing and authenticating users, filtering unwanted traffic, encrypting data, and providing secure remote access using virtual private networks (VPN).
- **Monitor**—Monitoring the network involves the use of detection mechanisms (for example, IDSs) to send notifications if a security incident occurs.

- **Test**—Testing the network involves proactive verification of the network's security capabilities. For example, administrators might periodically perform vulnerability scanning on the network.
- **Improve**—Based on newly emerging security risks and analysis of the network's current ability to mitigate attacks, improved security measures are instated.

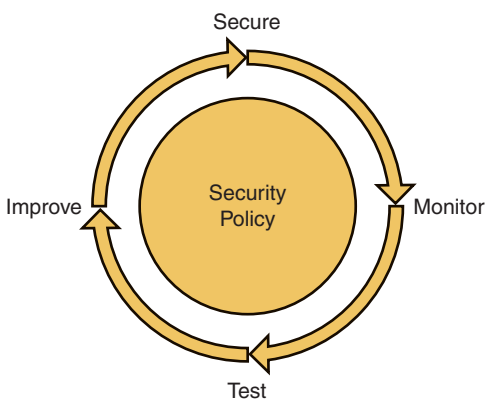


FIGURE 6-1 Network security process.

Cisco Self-Defending Network

Security needs to be fully integrated into a network to combat data theft. Fortunately, Cisco has defined the concept of the ***Self-Defending Network*** to leverage the security abilities of network components to protect the network from both internal and external threats. Network security integration consists of three components:

- **Trust and identity management**—Access is limited based on a user's access level. The three components of trust and identity management are as follows:
  - **Trust**—Defines how two or more network entities are allowed to communicate.
  - **Identity**—Validates the user accessing network resources. Identity can be proven by means such as passwords, tokens, or certificates.
  - **Access control**—Limits access to specific resources by specific users. The main concepts of access control are ***authentication*** (which determines the identity of the user) and ***authorization*** (which defines what a user is allowed to do on a network).
- **Threat defense**—Security breaches are minimized and mitigated through three primary approaches:
  - **Physical security**—Limits physical access to network resources.
  - **Infrastructure protection**—Takes measures to ensure network devices are not accessed or altered by an attacker.
  - **Threat detection and mitigation**—Threat detection and mitigation use technologies that provide proactive notification of suspicious network traffic patterns.

- **Secure connectivity**—Cryptography features provide the following protections for data flowing across a network:
  - **Privacy**—Privacy provides confidential communication through the network. The cryptographic service that offers confidentiality is encryption. Encryption scrambles data such that if an attacker were to intercept the data, the data would not be readable. However, the legitimate recipient of the data can decrypt the data into a readable form.
  - **Data integrity**—Cryptography mechanisms such as hashing algorithms and digital signatures can verify data was not manipulated in transit.

The Cisco Self-Defending Network is based on an underlying secure network platform (for example, Cisco routers, Cisco Catalyst switches, and Cisco Adaptive Security Appliances [ASA]). Layered on top of the network platform are advanced security technology and services. The use of these technologies is then governed by security policies and security management applications. These security management applications are used by network administrators to monitor and control the network.

If you properly plan security measures to protect your network architecture, the primary security risk is an error in security policies. Network managers and administrators must be intimately familiar with security policies and predefined procedures to respond to a security breach. A thorough understanding of these policies can help provide efficient incident response.

Cisco offers a suite of security management solutions, including the following:

- **Cisco Router and Security Device Manager (SDM)**—SDM offers a graphic user interface (GUI) to Cisco router configuration for features such as VPNs, quality of service (QoS), IPS, and Cisco IOS Firewall.
- **Cisco Adaptive Security Device Manager (ASDM)**—ASDM offers security management and monitoring features for devices such as the Cisco ASA 5500 series, Cisco PIX 500 series security appliances, and the Cisco Catalyst 6500 series Firewall Services Module (FWSM).
- **Cisco Intrusion Prevention System Device Manager (IDM)**—IDM is a Java application that supports the configuration and management of intrusion prevention sensors (IPS) through a web-based interface.
- **Management Center for Cisco Security Agents**—The Cisco Security Agent (CSA) is a Host Intrusion Prevention System (HIPS) that runs on hosts' machines, such as servers and personal workstations. The Management Center for Cisco Security Agents allows hosts to be classified into different groups and have different policies applied to the different groups.
- **Cisco Secure Access Control Server (ACS)**—Cisco Secure ACS is an application that supports identity-based services for a wide range of Cisco devices (for example, routers, switches, and firewalls). For example, instead of creating a username entry in every

router in the network for a newly hired administrator, the administrator could simply have an account added in an ACS server, which could be referenced by all routers in an organization.

- **Cisco Security Manager**—The Cisco Security Manager is a GUI-based application that aids in the configuration of firewalls, VPNs, and IPS policies on a variety of Cisco devices (for example, routers, switches, and firewalls).
- **Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)**—Cisco Security MARS is a network appliance that allows network administrators to monitor, identify, contain, and combat network attacks.

The Cisco Self-Defending Network consists of three layers:

- **Integrated security**—Security technology is built in to network components such as routers, switches, and wireless devices.
- **Collaborative security systems**—Network security elements work in a collaborative fashion to enable the network as a whole to meet the goals of an organization's security policy.
- **Adaptive threat defense**—Behavior-recognition tools defend against emerging security threats and dynamic network conditions. These tools can defend against threats such as worms, viruses, spyware, and distributed DoS (DDoS) attacks.

Figure 6-2 shows an example of a network containing many of the elements of a Cisco Self-Defending Network.

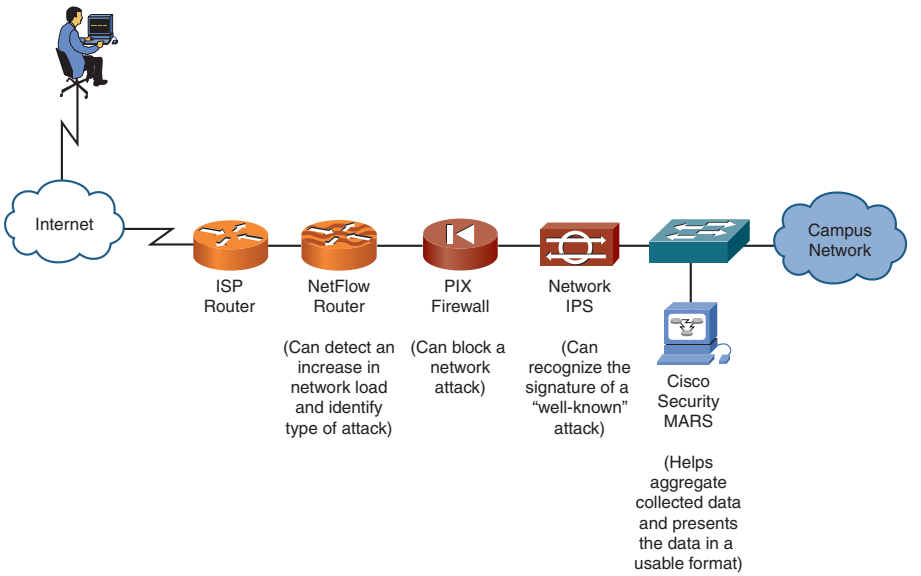


FIGURE 6-2 Cisco Self-Defending Network example.

Network Security Solutions

To secure a network, integrate security solutions into all parts of the network. Consider how the following network elements integrate security solutions:

- **Cisco IOS router**—Depending on the feature set, a Cisco IOS router can act as a firewall/IPS. Also, a router can be used to set up an IPsec tunnel. Trust and identity solutions include authentication, authorization, and accounting (AAA), public key infrastructure (PKI), Secure Shell Protocol (SSH), and Secure Sockets Layer (SSL).