**Chapter 6: Evaluating Security Solutions for the Network**

* 1. **Network Security**

Network security is one of the essential network services; it spans the entire network and it must be addressed within each modular block. Modularity ensures that the network designer can focus on a security problem within a particular network module and integrate a particular solution into a global security solution.

The scope of a network security solution is determined by organizational requirements and by potential threats to the organization. To create a secure network, the threats against which the network has to be protected must be determined.

Creating a network security policy is key to understanding and implementing security; network security policies and processes are discussed, and using risk assessment to create a security policy is explained.

### **The Need for Network Security**

In the distant past, networks were designed to be open, and network security was largely a matter of physical security. As networks become increasingly interconnected and data flows more freely, security services become critical. In the commercial world, connectivity is no longer optional; the possible risks of providing connectivity do not outweigh its benefits, including revenue generation. Therefore, security services must provide adequate protection to allow organizations to conduct business in a relatively open environment.

Secure networks are required **not** only to defend against attacks and prevent unauthorized access; legislation, industry regulations, and company policies might also require secure networks to keep data private and ensure that it is not misused.

#### **Network Security Requirements**

Network security should include the following requirements:

* Prevent external hackers from getting access to the network
* Allow only authorized users into the network
* Prevent those inside the network from executing deliberate or inadvertent attacks
* Provide different levels of access for different types of users
* Protect data from misuse and corruption
* Comply with security legislation, industry standards, and company policies

#### **Security Legislation [law, regulation]**

Security legislation and industry standards might define how data has to be handled, how to make sure that private information is protected, and what kind of information can be public. Based on legislative mandates and industry directives, organizations might have to protect customer records and privacy and even encrypt data to help ensure that the network is secure.

### **Terminology [language] related to Security**

* **Hacking** really means to work carefully on a computer system until it performs optimally. The popular use of the term *hacking* is more related to *cracking*, which is defined as the act of **illegally accessing a network infrastructure to perform unethical activities.**
* **A virus** **is a program that causes a damaging outcome**. Viruses often cover themselves as executable with clever filenames like “You won.” Viruses can be delivered via an e-mail or a website; a virus requires a human action, such as opening an e-mail attachment, to be activated. **A *worm*** **is a virus that can self-duplicate**. A worm might also be able to scan a network and infect neighboring workstations.
* **A Trojan horse imagines to be an inoffensive application when in fact it might contain a destructive payload.** An example of a Trojan horse is an attachment that, after being opened, shows a picture of a cute puppy, but in the background, the code is reading the e-mail addresses of the user’s address book and forwarding those addresses to a hacker’s repository for future spam use.
* **Attacks** are becoming more complex. *Malware* is a generic term that describes malicious software such as viruses and Trojan horses. *Combo malware* is a hybrid menace that combines destructive components of different threats. A worm that carries a viral payload is an example of combo malware.
* **Spam** is unwanted e-mail. Spam might contain viruses or other threats, or point to infected or dangerous websites.
* **Spyware** **is a program that gathers information without the user’s knowledge or consent and sends it back to the hacker.** For example, spyware could log keystrokes, upload information (such as all addresses in the victim’s address book), or download a program (known as a *zombie*) that waits for further instructions from the hacker.
* **Spear phishing** is a very targeted phishing attack. For example, a hacker sends an e-mail that appears to be from a company’s Human Resources department, asking all employees to confirm their banking information, or they won’t get paid. If any employees reply with their information, the hacker may use it to gain access to their bank accounts.
* **Social engineering** is the practice of obtaining confidential information by manipulating legitimate users. Examples include the following:
* **Getting physical access:** A hacker might get confidential information and passwords by having physical access to the organization. For example, the hacker might visit an organization and see passwords that are insecurely posted in an office or cubicle.
* **Using a psychological approach:** A hacker might exploit human nature to obtain access to confidential information. For example, a hacker might send an e-mail or call and ask for passwords, pretending that the information is required to maintain the victim’s account.

To provide adequate protection of network resources, the network procedures and technologies need to address the following **security risks**:

* **Confidentiality of data:** Confidentiality should ensure that only authorized users can view sensitive information, to prevent theft, legal liabilities, and damage to the organization.
* **Integrity of data:** Integrity should ensure that only authorized users can change sensitive information and guarantee the authenticity of data.
* **System and data availability:** Availability should ensure uninterrupted access to important computing resources to prevent business disruption and loss of productivity.

Given the broad range of potential threats, everything in the network is a potential target. Hosts are typically the preferred target for worms and viruses. For example, host files could be corrupted in an attack, and the compromised host could be used to launch attacks against other hosts, creating a *botnet*. However, other high-value targets include the following:

* Network infrastructure devices, including routers and switches
* Support services, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System servers
* Endpoints, including IP phones, management stations, and user endpoints (such as PCs and laptops)
* Network infrastructure, including the network capacity or bandwidth
* Security devices, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS)
  + 1. **Network Security threats and risks**

#### **Threat: Reconnaissance Attacks**

Reconnaissance attacks aim to discover information about a network, including the following:

* Active targets
* Network services that are running
* Operating system platform
* Trust relationships
* File permissions
* User account information

A common technique to find active targets such as networking devices and user endpoints is *port scanning*, in which data is sent to various TCP and User Datagram Protocol (UDP) ports on a device and the response from the device is evaluated.

**To avoid reconnaissance attacks,** a network should be tested to see how much it would reveal if attacked. The following are some examples of port-scanning tools:

* **Network Mapper (Nmap):** Nmap is a free open-source utility for network exploration or security auditing. It was designed to rapidly scan large networks; it also maps single hosts.
* **NetStumbler:** NetStumbler is a tool for Microsoft Windows that facilitates detection of WLANs using the IEEE 802.11b, 802.11a, and 802.11g WLAN standards. A trimmed-down version of the tool called MiniStumbler is available for Windows CE.
* **SuperScan:** SuperScan is a popular Windows port-scanning tool with high scanning speed, host detection, extensive banner grabbing, and Windows host enumeration capability.
* **Kismet:** Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and IDS that can sniff 802.11b, 802.11a, and 802.11g traffic. It identifies networks by passively collecting packets and detecting standard named networks, detecting hidden networks, and inferring the presence of *nonbeaconing networks* (networks that do not advertise themselves) via data traffic.

Port-scanning tools are designed to scan large networks and determine which hosts are up and the services they offer.

Other tools, called *vulnerability scanners*, help find known vulnerabilities in a network. The tools use either passive scanning (by analyzing network traffic) or active testing (by sending packets through the network). The following are examples of vulnerability scanning tools:

* **Nessus:** Nessus is an open-source product designed to automate the testing and discovery of known security problems. A Windows graphical front end is available, although the core Nessus product requires Linux or UNIX to run.
* **Microsoft Baseline Security Analyzer (MBSA):**Although it’s not a true vulnerability scanner, companies that rely primarily on Microsoft Windows products can use the freely available MBSA. MBSA scans the system and identifies whether any patches are missing for products such as the Windows operating systems, Internet Information Server, SQL Server, Exchange Server, Internet Explorer, Windows Media Player, and Microsoft Office products. MBSA also identifies missing or weak passwords and other common security issues.
* **Security Administrator’s Integrated Network Tool (SAINT):** SAINT is a commercial vulnerability assessment tool that runs exclusively on UNIX.

#### **Threat: Gaining Unauthorized Access to Systems**

There are many ways that hackers gain access to systems. One often-seen threat is the knowledge of usernames and passwords by unauthorized persons. For example, known vulnerabilities in operating systems or services could be exploited, usernames and passwords could be captured or cracked, or the default administrative or service accounts might be accessible. It might be possible to decrypt or crack passwords from a system password file or by capturing passwords when they are being transmitted over the network. If a hacker gains access to a sufficiently privileged account, that person might gain access to all files on the system and might also be able to exploit other systems based on the user trust relationships across systems.

Another way that hackers gain access to a system is through various methods of social engineering. As mentioned, this could include exploiting human nature and gaining physical access to an organization. The impact of gaining system access could include exposure or compromise of sensitive data or machines, and the execution of arbitrary commands on the system.

#### **Threat: DoS**

DoS attacks attempt to compromise the availability of a network, host, or application.DoS attacks are considered a major risk because they can easily interrupt business processes and cause significant loss. DoS attacks are relatively simple to conduct, even by an unskilled attacker.

Two methods of causing a DoS attack are by sending malformed data and by sending a large quantity of data. A successful DoS attack is usually the consequence of one of the following failures:

* The incapability of a network, host, or application to handle an enormous quantity of data, which renders the system unresponsive or brings it to a halt. The difficulty of defending against such an attack lies in the difficulty of distinguishing legitimate data from attack data.
* The failure of a host or application to handle an unexpected condition, such as maliciously formatted input data, an unexpected interaction of system components, or simple resource exhaustion.

#### **Risk: Integrity Violations and Confidentiality Breaches**

**Key security risks are integrity violations and confidentiality breaches**.  Integrity violations can occur when an attacker attempts to *change* sensitive data without proper authorization.

An example of an integrity violation is when an attacker obtains permission to write to sensitive data and then changes or deletes it. The owner of the data might not detect such a change until it is too late, perhaps when the change has already resulted in tangible loss. Because of the difficulty of detecting changes and the possible cascading consequences of late detection, many businesses treat integrity violations as the most serious threat to their business.

Confidentiality cracks can occur when an attacker attempts to *read* sensitive data without proper authorization. Confidentiality attacks can be extremely difficult to detect because the attacker can copy sensitive data without the owner’s knowledge and without leaving a trace.

The risks of both integrity violations and confidentiality cracks are usually managed by enforcing access **control in various ways**, including the following:

* Limiting access to network resources using network access control, such as physical separation of networks, restrictive firewalls, and VLANs.
* Limiting access to files and objects using operating system-based access controls, such as UNIX host security and Windows domain security.
* Limiting users’ access to data by using application-level controls, such as different user profiles for different roles.
* Using cryptography to protect data outside the application. Examples include encryption to provide confidentiality, and secure fingerprints or digital signatures to provide data authenticity and integrity.

### **Network Security Policy and Process**

Network security is a continuous process, built around a security policy. Business needs (organizational requirements) and risk analyses are inputs to the development of a security policy. Regardless of the security implications, business needs must come first; if the business cannot function because of security constraints, the organization will have a major problem.

The following are the key areas to consider when designing a secure network:

* **Business needs:** What the organization wants to do with the network
* **Risk analysis:** The risk-versus-cost balance
* **Security policy:** The policies, standards, and guidelines that address business needs and risk
* **Industry-recommended practices:** The reliable, well-understood, and recommended security practices in the industry
* **Security operations:** The process for incident response, monitoring, maintenance, and compliance auditing of the system

#### **Security Policy**

A *security policy* is a set of objectives, the rules of behavior for users and administrators, and the requirements for system and management that collectively are designed to ensure the security of computer systems in an organization.

#### **Network Security Process**

A security policy should be considered a living document, continuously updated as technology and organizational requirements change. **A process consisting of the following four steps helps maintain the security policy:**

* **Secure**: A security solution is implemented to stop or prevent unauthorized access or activities and to protect information and assets. Securing the network might include implementing filtering and stateful inspection, identity authentication, encryption, virtual private networks (VPN), vulnerability patching, and other countermeasures to implement the security policy.
* **Monitor**: Monitoring the security solution is required to detect violations of the security policy; monitoring might include system auditing, real-time intrusion detection and response, and content-based detection and response.
* **Test**: The effectiveness of the security policy and the implemented security solution is validated by regular system auditing and assessment, and vulnerability scanning. Any applications installed and patches applied to software must be verified against the security policy.
* **Improve**: The information gathered from monitoring and testing the security solution, including event and data analysis and reporting, is used to make improvements to the security implementation. The security policy might have to be adjusted as new security vulnerabilities and risks are identified, and as network security intelligence improves.

## Cisco Self-Defending Network

### **The Cisco Self-Defending Network Framework**

To prevent information theft, organizations must implement precautions such as establishing formal organizational security policies, enforcing access rights to authenticated users, and securing the transport of data and voice communications. Security must be fully integrated into all aspects of the network to proactively recognize potential suspicious activity, identify threats, react adaptively, and facilitate a coordinated response to attacks. Cisco has defined the Self-Defending Network to take advantage of the intelligence in network resources and to protect organizations by identifying, preventing, and adapting to threats from both internal and external sources.

**The Self-Defending Network’s integrated network security incorporates the following three critical elements:**

* **Trust and identity management:** To protect critical assets by allowing access based on privilege level
* **Threat defense:** To minimize and mitigate outbreaks
* **Secure connectivity:** To ensure privacy and confidentiality of communications

#### **Cisco Self-Defending Network Phases**

The Cisco Self-Defending Network contains three characteristic that together provide continuous, intelligent, future-proofed security, from the network through to the application layer:

* **Integrated security:** Security defense technologies are incorporated across all network elements, including routing, switching, wireless, and security platforms so that every point in the network can defend itself. These security features include firewalls, VPNs, and trust and identity capabilities. An example is the use of the Cisco Security Agent, which provides endpoint server and desktop protection against new and emerging threats stemming from malicious network activity.
* **Collaborative security systems:** The secure network components work together as a security system that adheres to and responds to an organization’s security policies. An example of this collaborative characteristic is NAC, implemented in devices from multiple vendors.
* **Adaptive threat defense:** The secure network uses several tools to defend against new security threats and changing network conditions. Application awareness defends against security threats entering the network from within Internet-enabled applications. Behavioral recognition defends against worms, viruses, spyware, DDoS attacks, and other threats. Network control intelligently monitors and manages the security infrastructure and provides tools for IT managers to audit, control, and correlate.

### **Trust and Identity Management**

Businesses need to effectively and securely manage who and what can access the network, as well as when, where, and how that access can occur.

**Trust and identity management** is critical for organizations. It underpins the creation of any secure network or system by providing or denying access to business applications and networked resources based on a user’s specific privileges and rights.

Trust and identity management solutions provide secure network access and admission at any point in the network and isolate and control infected or unpatched devices that attempt to access the network. The three aspects of trust and identity management are trust, identity, and access control,

**Trust** defines the relationship in which two or more network entities are allowed to communicate. Security policy decisions are based on **trust**.

Trusted entities are allowed to communicate freely; communication with untrusted entities needs to be carefully managed and controlled because of its higher risk. Trust and risk are opposites; security is used to limit risk by enforcing limitations on trust relationships.

* + - 1. **Implementing Strong Password Policies**

On a Windows host, it is possible to implement password complexity rules to force users to choose strong passwords, which are more difficult for hackers to determine. Some characteristics of a strong password include the following:

* It is a minimum of ten characters
* It is a mixture of uppercase and lowercase letters
* It contains at least one numeric character (0–9) or nonalphanumeric character (for example, !#@&)
* It has at least one special character within the password—not at the beginning or end
* It is not a form of the user’s name or user ID
* It is a word that is not found in a dictionary (domestic or foreign)

#### **Access Control**

Trust and identity management is also supported by access control. **Access control** is the ability to enforce a policy that states which entities (such as users, servers, and applications) can access which network resources.

Network access control mechanisms are classified in the following ways:

* **Authentication mechanisms**, which establish the subject’s identity.
* **Authorization mechanisms**, which define what a subject can do in a network and thus limit access to a network. The granularity of access, such as read-only or write, may also be defined.
* **Accounting mechanisms**, such as an audit trail, which provides evidence and accounting of the subject’s actions, and real-time monitoring, which provides security services such as intrusion detection.

#### **Trust and Identity Management Technologies**

Some of the many technologies used for trust and identity management include the following:

* **ACLs:** Lists maintained by network devices such as routers, switches, and firewalls to control access through the device. An example is an ACL on a router that specifies which clients, based on their IP addresses, can connect to a critical server in the data center.
* **Firewall:** A device designed to permit or deny network traffic based on certain characteristics, such as source address, destination address, protocol, port number, and application. The firewall enforces the access and authorization policy in the network by specifying which connections are permitted or denied between security perimeters.
* **NAC:** A set of technologies and solutions that uses the network infrastructure to enforce security policy compliance on all devices trying to access network computing resources, thereby limiting damage from emerging security threats.
* **IEEE 802.1X:** An IEEE standard for media-level access control, providing the ability to permit or deny network connectivity, control VLAN access, and apply traffic policy based on user or device identity.
* **Cisco Identity-Based Networking Services (IBNS):** An integrated solution combining several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources.

## Network Security Solutions

### **Integrated Security within Network Devices**

The section explains the security features integrated in Cisco network devices. To design and implement a secure network, it is necessary to integrate security in every part of the network environment. Cisco network devices supporting integrated security include the following:

* Cisco IOS routers (cisco internetwork operating system): is a software used on most cisco system router and current cisco network switches. Earlier switches run “**Catos**”. IOS is a package of routing, switching, internetworking and telecommunication functions integrated in to a multitasking operating system.
* Security appliances, including
  + VPN concentrators
  + Cisco PIX security appliances: is a security mechanism that delivers enterprise class security for small office and enterprise teleworker environment.
* Catalyst services modules
* Endpoint security solutions

### **Securing the Enterprise Network**

Securing the enterprise network involves deploying technologies that support identity and access control, threat defense and infrastructure protection, and security management. This section reviews the locations at which security devices and solutions might be deployed within the Enterprise network of a sample organization.

### **Deploying Security in the Enterprise Campus**

Consider an organization that has experienced several incidents in which laptop users on the campus network have brought in viruses from home, some users have attempted to intercept network traffic, and some interns have tried to hack the network infrastructure. To manage the risks, the organization implements identity and access control solutions, threat detection and mitigation solutions, infrastructure protection, and security management.

Identity and access control technologies include the following:

* IEEE 802.1X is port securitythat provides an authentication mechanism to device that attach to LAN or WAN
* NAC(network Access control list) appliances: is a computer security to end point security technology such as antivirus, host intrusion preventionand user or system authentication,
* ACLs on Cisco IOS devices
* Firewalls (for example, Cisco FWSM) provide stateful inspection and application inspection

Threat detection and mitigation technologies include the following:

* Net Flow
* Syslog
* SNMPv3
* HIPS (for example, the Cisco Security Agent)
* NIPS
* Cisco Security MARS
* Cisco Security Manager
* **Netflow :** is a network protocol developed by cisco for collecting IP traffic information as it enters or exit as interface and monitoring network traffic. network administrators can determine things such as the source and destination of traffic and class of service .
* **Syslog**: is a way for network devices to send event messages to a logging server that is known as a syslog server .routers and switches can send syslog messages.
* **IDS (intrusion detection system):** it inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or a system attack from someone attempting to break into the system.
* **NIPS(network based intrusion prevention system):** is a system used to monitor a network as well as protect the confidentiality ,integrity and availability of a network .and also its main functions is protecting the network from threats such as DOS attack and unauthorized usage.
* **SNMPv3:** is a protocol that describes how to configure the security mechanism to handle SNMP packets. SNMPV3 includes three important service such as authentication, privacy and access control.
* **Cisco Security monitoring analysis and response system (MARS):**is a security monitoring tool for network device and control of the existing security .
* **HIPS(host intrusion prevention system )**:is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Infrastructure protection technologies include the following:

* AAA
* SSH
* SNMPv3
* IGP or EGP MD5 routing protocol security
* Layer 2 security feature
* **AAA**: means authentication, authorization and accounting
* **IGP(Interior gateway protocol)**:is a type of protocol used for exchanging routing information between gateways (host with routers) within an autonomous system (e.g . LAN).
* **SSH(secure shell):** is a UNIX-based command interface and protocol for securely getting access to a remote computer.it is widely used by network administrator to control web And other kinds of servers remotely .

#### **Deploying Security in the Enterprise Data Center**

The organization’s data center hosts servers for the main campus network and branch offices. These servers contain the enterprise’s most sensitive information and are available to a large number of users. Network performance is a critically important issue, which sometimes limits the choice of protection mechanisms. Some specific risks in the data center include direct compromise of exposed applications and unauthorized access to data, and compromise of other hosts from compromised servers in this module.

To provide security, the organization implements identity and access control solutions, threat detection and mitigation solutions, infrastructure protection, and security management.

Identity and access control technologies include the following:

* 802.1X port security
* ACLs on Cisco IOS devices
* Firewalls (for example, Cisco FWSM)

Threat detection and mitigation technologies include the following:

* NetFlow
* Syslog
* SNMPv3
* HIPS (for example, the Cisco Security Agent)
* IDS (for example, the Cisco IDSM-2)
* NIPS
* Cisco Security MARS

Infrastructure protection technologies include the following:

* AAA
* SSH
* SNMPv3
* IGP routing protocol security

#### **Deploying Security in the Enterprise Edge**

The enterprise edge modules provide WAN connectivity among various parts of the enterprise network. Security is important whenever data is transferred between locations. For example, some specific risks in the WAN module include the following:

* Data transmission confidentiality and integrity violations, in which an attacker who obtains physical access to the network media or to a service provider WAN switch can intercept WAN traffic and might eavesdrop or change data in transit.
* Accidental or deliberate misconfiguration of the WAN network, which can result in the interconnection of different enterprises. Some WAN protocols might establish automatic peering, and unwanted connectivity could become possible.

To provide security, the organization implements identity and access control solutions, threat detection and mitigation solutions, infrastructure protection, and security management.

Identity and access control technologies include the following:

* ACLs on Cisco IOS devices
* Firewalls (such as Cisco PIX Security appliances)
* IPsec or SSL VPN (used to provide layer 2 tunneling protocol packets by providing confidentiality,authentication,and integrity.
* Network access control(NAC) appliances
* adaptive security (AS) appliances

Threat detection and mitigation technologies include the following:

* NetFlow
* Syslog
* SNMPv3
* HIPS (for example, the Cisco Security Agent)
* NIPS
* Cisco Security MARS

Infrastructure protection technologies include the following:

* AAA
* SSH
* SNMPv3
* IGP or EGP MD5 routing protocol security