General Network Security

• **Security policy**
  – An organization’s set of rules regarding how to handle and protect sensitive data

• A security policy should include:
  – Physical security
  – Acceptable use of applications
  – Safeguarding data
  – Remote access to the network
  – Data center
  – Wireless security
General Network Security (continued)

• An effective security policy implements multiple layers of security
• A security policy should have three goals:
  – To prevent the hacker from getting access to critical data
  – To slow down the hacker enough to be caught
  – To frustrate the hacker enough to cause him or her to quit the hacking attempt
• When designing a security policy, take care to specify exactly what you are trying to protect
Protecting the Hardware

- The first level of security in any network is **physical security**
- Critical nodes of an organization should be separated from the general workforce
- The nodes should be kept in a central location where only a select group of people are allowed
- If office space is limited and nodes must be located near employees
  - The servers should at least be stored in a locked cabinet

*Figure 14-1  Server cabinet*
Protecting Software

• The primary threats against software are malware and hackers

• **Malware**
  – Refers to malicious programs that have many different capabilities

• Hackers are usually driven by greed, ego, and/or vengeance
  – They look to make personal gains through system vulnerabilities
Malware Prevention

• The most important elements of a prevention plan
  – Installing and maintaining virus prevention software,
  – Conducting virus awareness training for network users

• Types of malware
  – Virus
  – Worm
  – Macro Virus
  – Polymorphic Virus
  – Stealth Virus
Malware Prevention (continued)

- Types of malware (continued)
  - Boot-Sector Virus
  - Trojan or Trojan Horse
  - Logic Bomb

- Virus prevention software
  - Available for installation on entire networks
  - Usually includes a version that will run on clients as well as servers
  - Must be updated regularly to ensure your network is protected against all the latest malware threats
Malware Prevention (continued)

• User training
  – Users must be trained to update their antivirus software daily or, at a bare minimum, weekly
  – Users also must learn how viruses are transmitted between computers
  – Teach users to scan removable devices with the virus scanning software before using them
Firewalls

• **Firewall**
  – The primary method of keeping hackers out of a network
  – Normally placed between a private LAN and the public Internet, where they act like gatekeepers
  – Can be a hardware device or it can be software
  – Types: personal and enterprise

• All data packets entering or exiting the network have to pass through an enterprise-level firewall
  – Firewall filters (or analyzes) packets
Firewalls (continued)

• Four firewall topologies
  – Packet-filtering router
  – Single-homed bastion
  – Dual-homed bastion
  – Demilitarized zone (DMZ)
Figure 14-2  Packet-filtering router
All traffic is screened by the bastion host

**Figure 14-3** Single-homed bastion
Figure 14-4  Dual-homed bastion
Figure 14-5  Demilitarized zone
Firewalls (continued)

• **Intrusion Detection Systems (IDS)**
  – A security device that can detect a hacker’s attempts to gain access to the network
  – Can also detect virus outbreaks, worms, and distributed denial of service (DDoS) attacks

• **Intrusion Prevention Systems (IPS)**
  – Like an IDS, except that it is placed in line so all packets coming in or going out of the network pass through it
  – This allows an IPS to drop packets based on rules defined by the network administrator
Permissions, Encryption, and Authentication

• **Permission**
  – An official approval that allows a user to access a specific network resource

• **Encryption**
  – Often consists of using security algorithms to scramble and descramble data
  – Types of algorithms
    • Symmetric key
    • Asymmetric key
Permissions, Encryption, and Authentication (continued)

Figure 14-6  Symmetric key encryption
Permissions, Encryption, and Authentication (continued)

- Message is encrypted with user A’s Private key
- User B must have user A’s public key to decrypt the message

Figure 14-7  Asymmetric key encryption
Permissions, Encryption, and Authentication (continued)

• Secure Sockets Layer
  – A means of encrypting a session between two hosts through the use of digital certificates, which are based on asymmetric key encryption

• Authentication
  – The process by which users verify to a server that they are who they say they are
  – There are several types of authentication
    • Password authentication protocol (PAP)
    • Challenge handshake authentication protocol (CHAP)
Permissions, Encryption, and Authentication (continued)

• Additional authentication services supported by Cisco:
  – Remote Authentication Dial-in User Service (RADIUS)
  – Terminal Access Controller Access Control System Plus (TACACS+)

• These two common security protocols are based on the Authentication, Authorization, and Accounting (AAA) model
Mitigating Security Threats

• The three basic strategies for mitigating security threats are:
  – Using the SSH protocol to connect to your routers and switches rather than telnet
  – Turning off unnecessary services
  – Keeping up-to-date on security patches (software releases) with a patch management initiative
Secure Shell (SSH) Connections

• **Secure Shell (SSH) protocol**
  – Sends all data encrypted

• The two version of SSH are SSH Version 1 and SSH Version 2
  – SSH Version 2 is the recommended version

• Some SSH commands are mandatory and others are optional

• You must also generate an RSA key pair (asymmetric key encryption)
  – Which enables SSH
Secure Shell (SSH) Connections (continued)

• The preferred method is to implement SSH on all VTY lines
  – Which ensures that all remote IP sessions to the router will be protected in the SSH tunnel

• The command sequence for enabling SSH is:

  Router(config)#hostname SshRouter
  SshRouter(config)#ip domain-name sshtest.com
  SshRouter(config)#crypto key generate rsa

  The name of the keys will be:
  SshRouter.sshtest.com
Disabling Unnecessary Services

• You should disable the services unless your organization uses them

• Methods
  – Go through the CLI and enter a series of commands for each service
  – Use the Security Audit Wizard in the Cisco Security Device Manager (SDM)
Disabling Unnecessary Services (continued)

- The following services are unnecessary on most networks:
  (continued)
  - TCP Small Servers Service
  - UDP Small Servers Service
  - IP Bootp Server Service
  - Cisco Discovery Protocol (CDP)
  - IP Source Route
  - Maintenance Operations Protocol (MOP)
  - Directed Broadcast
  - ICMP Redirects
  - Proxy ARP
  - IDENT
  - IPv6
  - Finger Service
  - PAD Service
Patch Management

• Your organization’s patch management program should account for all software in the organization
  – Including commercial applications as well as applications developed in-house
• A patch management program should take into account the major software vendor’s patch release schedules
  – As well as your organization’s business goals and needs
• Not all patches released by vendors are flawless
Virtual Private Networks (VPNs)

- **Virtual Private Networks (VPNs)**
  - A popular technology for creating a connection between an external computer and a corporate site over the Internet

- To establish a VPN connection, you need VPN-capable components

- **Client-to-site VPN** (also known as remote user VPN)
  - A VPN that allows designated users to have access to the corporate network from remote locations
Virtual Private Networks (VPNs)

Figure 14-8  A client-to-site or a remote user VPN
Virtual Private Networks (VPNs)

- **Site-to-site VPN**
  - A VPN that allows multiple corporate sites to be connected over low-cost Internet connections
- **You can choose from several tunneling protocols to create secure, end-to-end tunnels**
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Generic Routing Encapsulation (GRE)
Virtual Private Networks (VPNs)

Figure 14-9  Site-to-site VPN
IPSec

• IPSec
  – A suite of protocols, accepted as an industry standard, which provides secure data transmission over layer 3 of the OSI model
  – An IP standard and will only encrypt IP-based data
• IPSec supports two modes of operation: transport mode and tunnel mode
IPSec (continued)

• **Transport mode**
  – Primarily geared toward encrypting data that is being sent host-to-host
  – Only encrypts and decrypts the individual data packets
    • Which results in quite a bit of overhead on the processor

• **Tunnel mode**
  – Encrypts all data in the tunnel and is the mode supported by Cisco components
IPSec Protocols

• Two IPSec protocols have been developed to provide packet-level security
• They include the following characteristics:
  – Authentication Header (AH)
  – Encapsulating Security Payload (ESP)
IPSec Authentication Algorithms

- Authentication algorithms use one of two **Hashed Message Authentication Codes (HMAC)**
  - **MD5** (message-digest algorithm 5)
  - **SHA-1** (secure hash algorithm)
- An HMAC is a secret key authentication algorithm that ensures data integrity and originality
  - Based on the distribution of the secret key
- Cryptographic software keys are exchanged between hosts using an HMAC
IPSec Encryption Algorithms

- For encryption, the two most popular algorithms on IPSec networks are **3DES** (tripleDES) and **AES**
  - These protocols are used solely with the IPSec ESP protocol
- Remember, AH does not support encryption
IPSec Key Management

• You need to pay attention to how keys are handed from node to node during IPSec authentication

• Two options are available
  – Deliver the secret keys to all parties involved via e-mail or on disk
  – Utilize a key management protocol

• Key management is defined by the Internet Security Association and Key Management Protocol (ISAKMP)
  – Governed by RFC 2407 and 2408
IPSec Transform Sets

• **A transform set**
  – A configuration value (or simply stated, a command) that allows you to establish an IPSEC VPN on a Cisco firewall

• You can create a transform set through the CLI or you can simply use the SDM GUI

• When creating an IPSec VPN you must specify a protocol, the algorithm, and the method of key management
Creating VPNs with the Security Device Manager (SDM)

- Cisco supports VPNs with several different devices
- VPNs can be created on firewalls, routers, computers
  - And even on a device specifically made for VPNs, called a VPN concentrator
- The following example focuses on using the Cisco Security Device Manager (SDM) Web utility to create a VPN on a Cisco router
Figure 14-10  SDM Flash Screen
Figure 14-11  SDM Home page
**Figure 14-12** VPN button selected in the Tasks pane
Site-to-Site VPN

This wizard will guide you through the necessary steps to configure one end of a site-to-site VPN tunnel on this router. The peer device must be configured with identical VPN configuration for the tunnel to work. Please select one of the following setup and click on the next button to begin.

- **Quick setup**
  Quick setup asks for minimal information and uses SDM defaults. This is recommended if you are creating a VPN tunnel between two Cisco routers using SDM.

- **Step by step wizard**
  Step by step wizard allows you to specify either the SDM default configuration or your own custom configuration.

**Figure 14-13** First page of the Site-to-Site VPN Wizard
Figure 14-14  Default VPN Settings
Figure 14-15  VPN Connection Information Screen
Figure 14-16  Summary of the Configuration
Figure 14-17  Commands Delivery Status dialog box
Figure 14-18  VPN Down
Cisco Security Audit Wizard

• You can use the Cisco SDM to conduct security audits

• The SDM’s Security Audit Wizard
  – Can be used to verify your router’s configuration
    • And determine what security settings have and have not been configured
  – Will also make recommendations as to which settings should be enabled
  – Provides an easy to use GUI that allows you to make those changes
Figure 14-19  SDM Security Audit Screen
Welcome to the security audit wizard

Security audit is a feature that examines your existing router configuration and then provides a list of recommended configuration changes in order to make your router and network more secure.

For a complete list of functions security audit checks for, see the On-line help topics.

Security audit will

- Check the router’s running config against a list of predefined security configuration settings.
- List identified problems then provide recommendations for fixing them.
- Allow the user to choose which identified problem(s) to fix then display the appropriate user interface for fixing them.
- Configures the router with user chosen security configuration.

To continue click next.

**Figure 14-20**  SDM Security Audit Wizard
Figure 14-21  Security Audit Results
### Security Audit Wizard

**Select an option:** Fix the Security problems

Check the "Fix-it" checkbox next to the settings you want to fix. Then, click "Next" to continue. You may be prompted for more information to fix certain settings.

<table>
<thead>
<tr>
<th>No.</th>
<th>Security Problems Identified</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PAD Service is enabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>2</td>
<td>IP bootp server Service is enabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>3</td>
<td>CDP is enabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>4</td>
<td>IP source route is enabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>5</td>
<td>Password encryption Service is disabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>6</td>
<td>TCP Keepalives for inbound telnet sessions is disabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>7</td>
<td>TCP Keepalives for outbound telnet sessions is disabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>8</td>
<td>Sequence Numbers and Time Stamps on Debugs are disabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>9</td>
<td>IP CEF is disabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>10</td>
<td>Minimum Password length is disabled or less than 6 characters</td>
<td>Fix it</td>
</tr>
<tr>
<td>11</td>
<td>Authentication Failure Rate is disabled or less than 3 retries</td>
<td>Fix it</td>
</tr>
<tr>
<td>12</td>
<td>Scheduler Interval is not set</td>
<td>Fix it</td>
</tr>
<tr>
<td>13</td>
<td>TCP Synwait time is not set</td>
<td>Fix it</td>
</tr>
<tr>
<td>14</td>
<td>Banner is not set</td>
<td>Fix it</td>
</tr>
<tr>
<td>15</td>
<td>Logging is not enabled</td>
<td>Fix it</td>
</tr>
<tr>
<td>16</td>
<td>Enable Secret Password is not set</td>
<td>Fix it</td>
</tr>
</tbody>
</table>

**Figure 14-22**   Fix the Security problems option

---


52
Figure 14-23  CDP check box
Figure 14-24 Summary Screen
Cisco Security Audit Wizard (continued)

![Commands Delivery Status Window]

**Figure 14-25** Commands Delivery Status
Summary

- Protecting the physical equipment where sensitive data resides is as important as protecting the data itself.
- When securing an organization’s network, you must be sure to protect it against external threats as well as internal threats.
- User training is a key element to protecting the network and the data within it.
- Using an SSH connection to a router is a much more secure method of connecting to a router than clear text telnet.
Summary (continued)

- Disabling unnecessary services increases a router’s security
- IPSec is an industry-standard suite of protocols and algorithms that allow for secure encrypted VPN tunnels
- Cisco’s SDM is a multifunction Web utility that allows you to create VPNs and complete a security audit