



# Chapter 16: Advanced Security



## IT Essentials: PC Hardware and Software v4.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 16 Objectives

- 16.1 Outline security requirements based on customer needs
- 16.2 Select security components based on customer needs
- 16.3 Implement customer's security policy
- 16.4 Perform preventive maintenance on security
- 16.5 Troubleshoot security



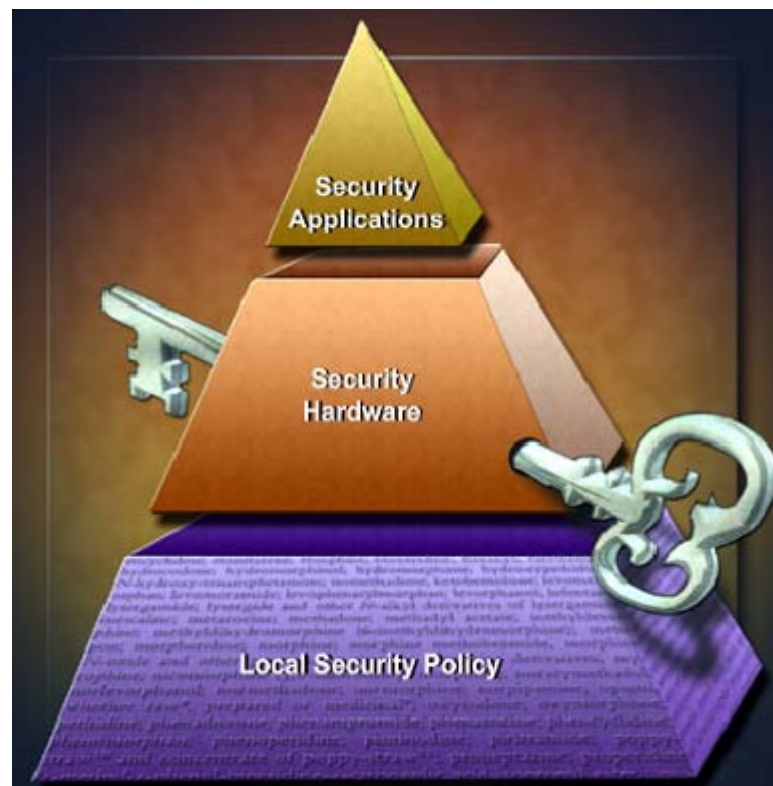
# Chapter 16 Worksheets, Activities, Labs

- 16.1.1 Worksheet: Security Policy
- 16.2.2 Activity: Security Devices
- 16.2.3 Worksheet: Firewalls
- 16.3.2 Lab: Windows XP Firewall
- 16.5.3 Lab: Fix a Security Problem
- 16.5.3 Remote Technician: Fix a Security Problem

# Outline Security Requirements

A security policy includes a comprehensive statement about the level of security required and how this security will be achieved.

- Is the computer located at a home or a business?
- Is there full-time Internet access?
- Is the computer a laptop?





# Outline a Security Policy

A collection of rules, guidelines, and checklists:

- Define an acceptable computer usage statement.
- Identify the people permitted to use the computer equipment.
- Identify devices that are permitted to be installed on a network, as well as the conditions of the installation.
- Define the requirements necessary for data to remain confidential on a network.
- Determine a process for employees to acquire access to equipment and data.



# Security Hardware

Identify hardware and equipment that can be used to prevent theft, vandalism, and data loss.

- To **restrict access** to premises, you might use biometrics, fences, and/or door locks.
- To **protect the network infrastructure**, you might secure telecom rooms, setup detection for unauthorized use of wireless, and/or setup hardware firewalls.
- To **protect individual computers**, you might use cable locks, laptop docking station locks and/or lockable cases.
- To **protect data**, you might use lockable HD carriers and/or USP security dongles.



# Security Applications

Security applications protect the operating system and software application data.

- Software Firewall
- Intrusion Detection Systems (IDS)
- Application and OS Patches
- Anti-virus software and anti-malware software

Compare the cost of data loss to the expense of security protection, and then determine what tradeoffs are acceptable.

# Selecting Security Components

Consider the following factors when deciding on security components:



- Advantages and disadvantages of a security component
- Overlapping features and functions
- Component setup and maintenance requirements
- Budget restrictions
- Real and perceived threats



# Security Techniques

Depending on the situation, more than one technique may be required.

- Use **encrypted passwords** to login to the network
- Monitor network activity through **logging and auditing**
- Set up **data encryption over wireless**

Encryption methods include:

- **Hash encoding** uses an algorithm to track tampering
- **Symmetric encryption** uses a key to encode/decode data
- **Asymmetric encryption** uses one key to encode and another key to decode
- **VPN** creates a virtual “secure tunnel”

# Access Control Devices

## Physical access control devices

- Lock
- Conduit
- Card key
- Video surveillance
- Guards

## Two-factor identification methods for access control

- Smart card
- Security key fob
- Biometric device





# Firewall Types

## Hardware Firewall

- Free-standing and uses dedicated hardware
- Initial cost for hardware and software updates can be costly
- Multiple computers can be protected
- Little impact on the computer performance

## Software Firewall

- Available as 3<sup>rd</sup> party software and cost varies
- Included in Windows XP operating system
- Typically protects only the computer it is installed on
- Uses the CPU, potentially slowing the computer

# Configure Security Settings

Two primary security settings include:

- Setting levels of **permissions on folders and files**
  - Use FAT or NTFS to configure folder sharing or folder-level permissions for users with network access
  - Use file-level permissions with NTFS to configure access to files
- **Securing wireless access points**



- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- MAC address filtering
- Unused wireless connections
- Service Set Identifier (SSID) Broadcasting
- Wireless antenna

# Configure Firewalls



- A restrictive firewall policy (open only the required ports)
- A permissive firewall policy (open all ports except those explicitly denied)
- Configure a software firewall manually or to run automatically.
- Configure a hardware firewall by indicating what is filtered by port type, port number, source address, and/or destination address.

# Protect Against Malware

Run software scanning programs to detect and remove the malicious software.

- Anti-virus, anti-spyware, anti-adware, and phishing programs

Phishing attacks trick the user into providing the personal information. A user's data can be sold and/or used fraudulently.



# Operating System Updates

Windows XP update options:

- **Automatic:**

Automatically downloads and installs without user intervention.

- **Only Download Updates:**

Download the updates automatically, but the user is required to install them.

- **Notify Me:**

Notify the user that updates are available and gives the user the option to download and install.

- **Turn off Automatic Updates:**

Prevents automatically checking for updates. Updates have to be discovered, downloaded and installed by the user.

# User Account Maintenance

- Group employees by job requirements to give access to files by setting up group permissions.
- When an employee leaves an organization, access to the network should be terminated immediately.
- Guests can be given access through a Guest account.





# Data Backups

	Description
<b>Full or Normal Backup</b>	Archives all selected files
<b>Incremental Backup</b>	Archives all selected files that have changed since last full or incremental backup. It marks files as having been backed up.
<b>Differential Backup</b>	Archives everything that has changed since last full backup. It does not mark files as having been backed up.
<b>Daily Backup</b>	Archives all selected files that have changed on the day of the backup
<b>Copy Backup</b>	Archives all selected files



# Troubleshooting Process

**Step 1** Gather data from the customer

**Step 2** Verify the obvious issues

**Step 3** Try quick solutions first

**Step 4** Gather data from the computer

**Step 5** Evaluate the problem and implement the solution

**Step 6** Close with the customer



# Level-one Technician Gathers Data

Description of problem by the level-one helpdesk technician:

- Customer is unable to connect to the network using wireless connection.
  - Customer cannot surf the Internet.
  - Customer cannot access any resources on the network.
  - Wireless does not seem to be working properly at the office.
  - The customer has checked all settings.
- The helpdesk technician was unable to resolve the problem, so the work order is escalated to a level-two technician.



## Open-Ended Questions

Here are some open-ended questions that a level-two technician might ask to gather more information from the customer in this scenario:

- Which specific network resources are you trying to access with your wireless system?
- Are there any network resources that you can access by wireless?
- When were you last able to access the network using wireless at the office?
- How does your computer perform using wireless at other locations?



## Level-two Technician Draws Conclusions

Based on the information given by the customer to the open-ended questions, these conclusions can be determined:

- In the office, no resources can be accessed.
- When operating away from the office, no problems are experienced.
- The problems started just after a new wireless router was installed.



## Closed-Ended Questions

Here are some closed-ended questions that a level-two technician might ask to gather more information from the customer in this scenario:

- Is your network cable plugged in?
- When you plug in your network cable, does everything work correctly?

From the answers to these questions, you determine that the customer is experiencing a wireless connection problem. Therefore, focus your efforts on **a problem with wireless connectivity in the office.**



# Verify the Obvious Issues

Examine the most obvious causes of a problem.

- Does the access point appear to be on?
- What lights on the access point are on or flashing?
- Does anyone else have this problem?
- Have you been able to connect to the Internet since the wireless router was upgraded?
- Does this problem occur only at your desk or at other areas of the office as well?
- Have you been able to connect through wireless at any other locations?



## Conclusions from Checking the Obvious

- The network login and password are valid.
- The wireless card in the user's computer operates normally.
- The problem is not interference with the wireless signal.
- There is probably a wireless configuration issue.



## Quick Solutions

- Check the wireless signal strength in various areas in the office.
- Try connecting using wireless connection with security settings turned off.

Results of quick solutions:

- The wireless signal strength seems normal.
- Wireless connection works with security turned off.

So the problem is probably a configuration issue.

- Check the configurations on the computer and on the access point.



# Gather Data from the Computer

Determine the MAC address of the computer:

1. Select **Start > Run**
2. Type **cmd** in the Run box. The Command Line interface should appear
3. Enter **ipconfig /all** at the command prompt.
4. Write down the MAC address of the wireless NIC and of the Ethernet NIC.

No resolution to the problem has been found at this point. The problem is most likely to be found in the configuration of the wireless access point security settings.



# Evaluate Problem & Implement Solution

## 1. What do you know now?

- Works using the Ethernet cable
- Works using wireless when the security is disabled
- Works using wireless at home
- No one else has the problem
- Doesn't work when connected to the office wireless access point

## 2. Determine possible solutions

- Might be incorrect wireless access point configuration settings

## 3. Implement the best solution

- The MAC address filter on the access point was incorrectly configured for this customer.
- Add the computer's MAC address to the wireless access point MAC address filter list.



## Close with the Customer

- Discuss with customer the solution implemented.
- Have customer verify problem is solved.
- Provide all paperwork to customer.
- Document steps of solution.
- Document components used in repair.
- Document time spent to resolve the problem.

# Common Problems and Solutions

Problem Symptom	Possible Solution
A customer reports that a backup that was started the night before is still going.	Advise the customer to implement a different type of backup that saves time.
A visiting consultant using a guest account cannot access needed files.	Grant access to the files for the duration of the visit. When the consultant leaves, disable the account.
A user refuses your request to e-mail you their student ID number and password.	Inform the user that there was no such request. Gather information and warn others against this phishing attack.
A user can locate a file on the server but cannot download it.	Change the user permissions on this file from read to read and execute.
A user cannot connect to the network using a wireless router even after the proper security key has been installed.	Verify that the user's MAC address is listed in the MAC address filter table.



## Fix a Security Problem

Now that you understand the troubleshooting process, it is time to apply your listening and diagnostic skills.

- Receive the work order
- Research the problem
- Take the customer through various steps to try and resolve the problem
- Document the problem and the resolution



# Chapter 16 Summary

## Advanced Security

- Security requirements for customers differ because of budget restraints, the type of equipment to secure, and the decision regarding hardware and software security.
- A security policy should be developed and used to determine the type of firewall to be installed.
- Hardware and software security tools are available to protect data on a network.
- Security policies should be followed by everyone in the organization.
- Preventive maintenance is an effective part of security.

# Additional Resources

- Linksys: Learning Center <http://www.linksys.com>
- Home PC Firewall Guide™ <http://www.firewallguide.com>
- HowStuffWorks: It's Good to Know  
<http://computer.howstuffworks.com/firewall.htm>
- United States Computer Emergency Readiness Team: Cyber Security Tip  
<http://www.us-cert.gov/cas/tips/ST04-004.html>
- Microsoft: Security at Home: Firewall FAQs  
<http://www.microsoft.com/athome/security/protect/firewall.mspix>
- ConsumerSearch: Firewalls Reviews, Best Firewalls  
<http://www.consumersearch.com/www/software/firewalls/index.html>
- Matousec: Comparison of Top Five Personal Firewalls  
<http://www.matousec.com/projects/windows-personal-firewall-analysis/top-five-comparison.php>
- Computer Shopper, PC PRO UK: Personal Firewalls  
<http://www.pcpro.co.uk/shopper/labs/222/software-labs-personal-firewalls/introduction.html>
- Information Week: Safety First: 5 Firewalls for Your Desktop PC  
<http://www.informationweek.com/software/showArticle.jhtml?articleID=192201247>



# Q and A



# Cisco | Networking Academy<sup>®</sup>

Mind Wide Open<sup>™</sup>