



# Instructor Materials Chapter 7 Network Security



## Networking Essentials

Cisco | Networking Academy®  
Mind Wide Open™



## Chapter 7: Network Security



## Networking Essentials

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 7 - Sections & Objectives

- 7.1 Am I at Risk?
  - Explain network security threats.
- 7.2 Methods of Attack
  - Explain other types of network security threats.
- 7.3 How Can I Protect My Network?
  - Explain how software tools can mitigate network security threats.
- 7.4 How Do Firewalls Protect Networks?
  - Configure a firewall to control network traffic.



## 7.1 Am I at Risk?



Cisco | Networking Academy®  
| Mind Wide Open™



## Am I at Risk?

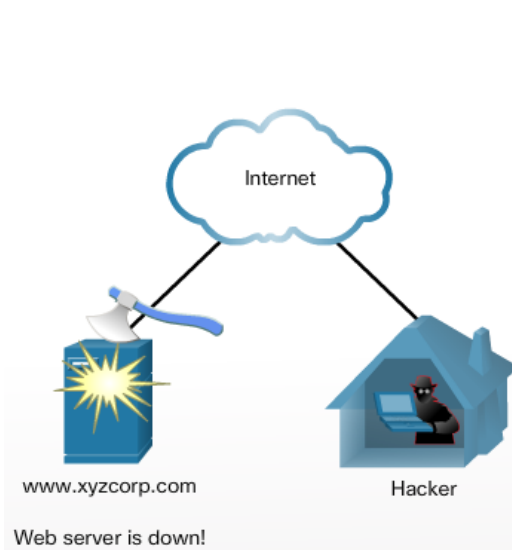
# Hackers and Intruders

- What Do They Want?
- When the hacker gains access to the network, four types of threat may arise: Information theft, Identity theft, Data loss / manipulation, and Disruption of service

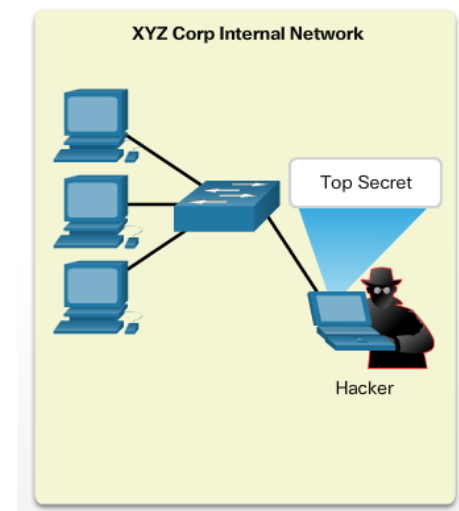
- Where Do They Come From?

- External threats arise from individuals working outside of an organization.
- Internal threats occur when someone has authorized access to the network through a user account or has physical access to the network equipment.

External Attack



Internal Attack





Am I at Risk?

# Social Engineering Attacks

## ■ Social Engineering

- In the context of computer and network security, social engineering refers to a collection of techniques used to deceive internal users into performing specific actions or revealing confidential information.



## ■ Types of Social Engineering

- Three of the most common methods hackers use to obtain information directly from authorized users go by unusual names: pretexting, phishing, and vishing.

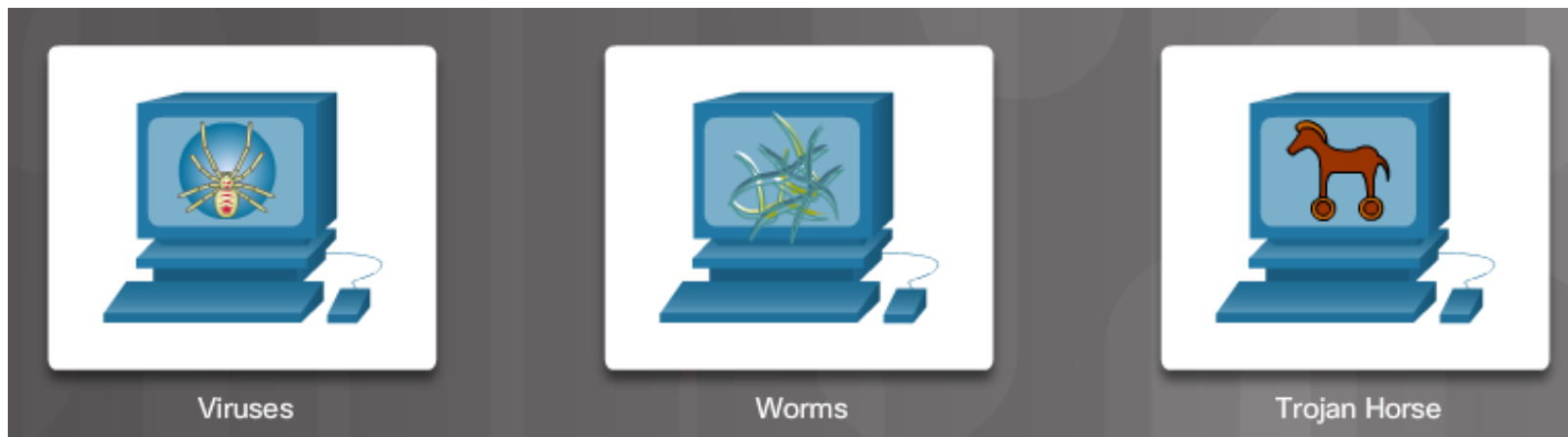


Am I at Risk?

# Virus, Worms, and Trojan Horses

## ■ Other Types of Attacks

- Malicious software can damage a system, destroy data, as well as deny access to networks, systems, or services. They can also forward data and personal details from unsuspecting PC users to criminals.



A virus is a program that spreads by modifying other programs or files.

A worm is similar to a virus, but unlike a virus does not need to attach itself to an existing program.

A Trojan horse is a program that is written to appear like a legitimate program, when in fact it is an attack tool.





## 7.2 Methods of Attack



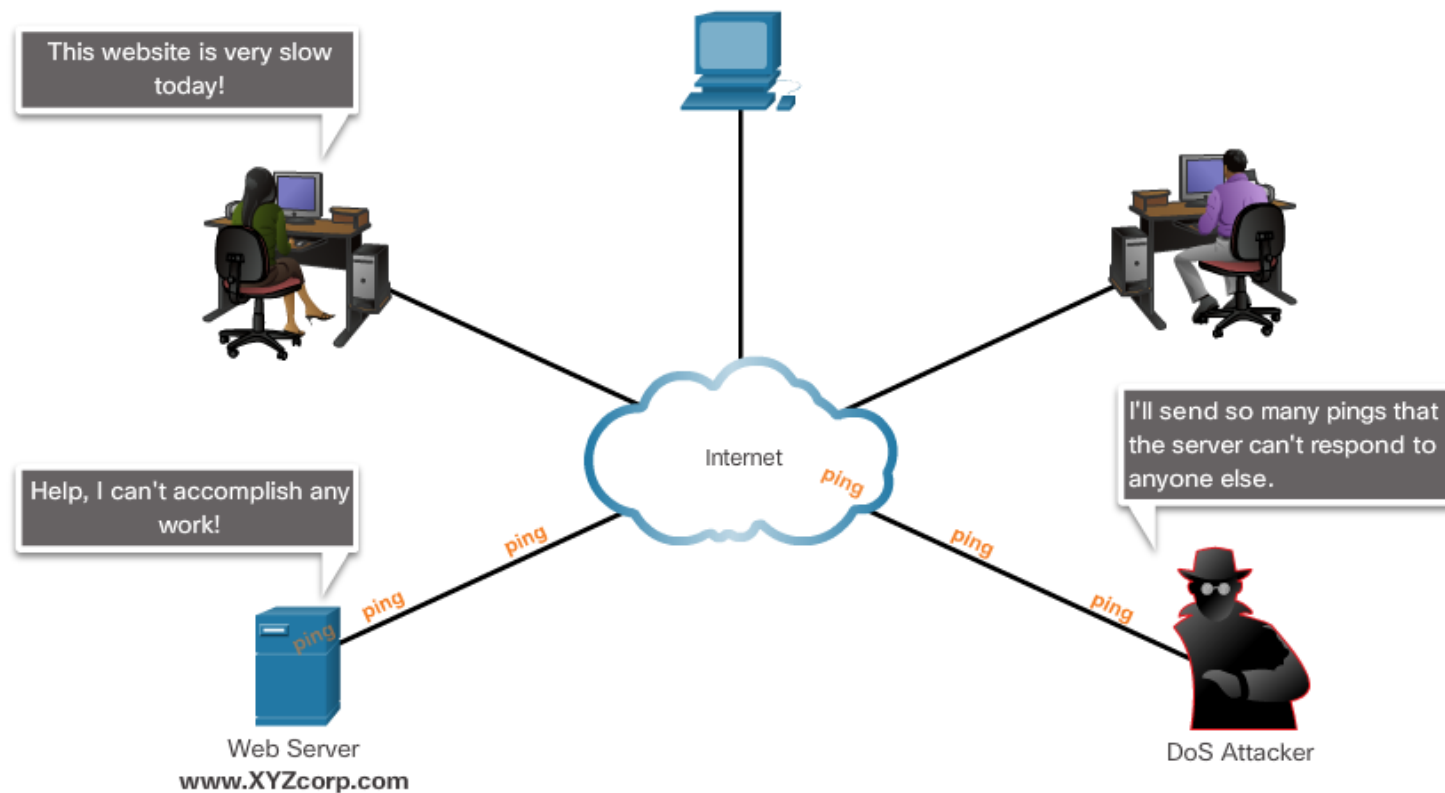


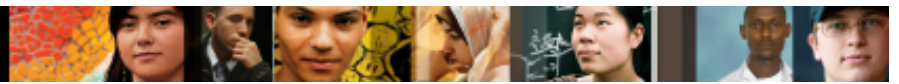


## Methods of Attack

# Denial of Service and Brute Force Attacks

- An attacker uses a DoS attack to perform these functions:
  - Flood a system or network with traffic to prevent legitimate network traffic from flowing
  - Disrupt connections between a client and server to prevent access to a service





## Methods of Attack

# Denial of Service and Brute Force Attacks (Cont.)

### ■ DDoS

- DDoS is a more sophisticated and potentially damaging form of the DoS attack. It is designed to saturate and overwhelm network links with useless data.

### ■ Brute Force

- With brute force attacks, a fast computer is used to try to guess passwords or to decipher an encryption code. The attacker tries a large number of possibilities in rapid succession to gain access or crack the code.



## Methods of Attack

# Other Types of Malware

### ■ Spyware

- Spyware is any program that gathers personal information from your computer without your permission or knowledge. This information is sent to advertisers or others on the Internet and can include passwords and account numbers.

### ■ Adware

- Adware is a form of spyware used to collect information about a user based on websites the user visits. That information is then used for targeted advertising.



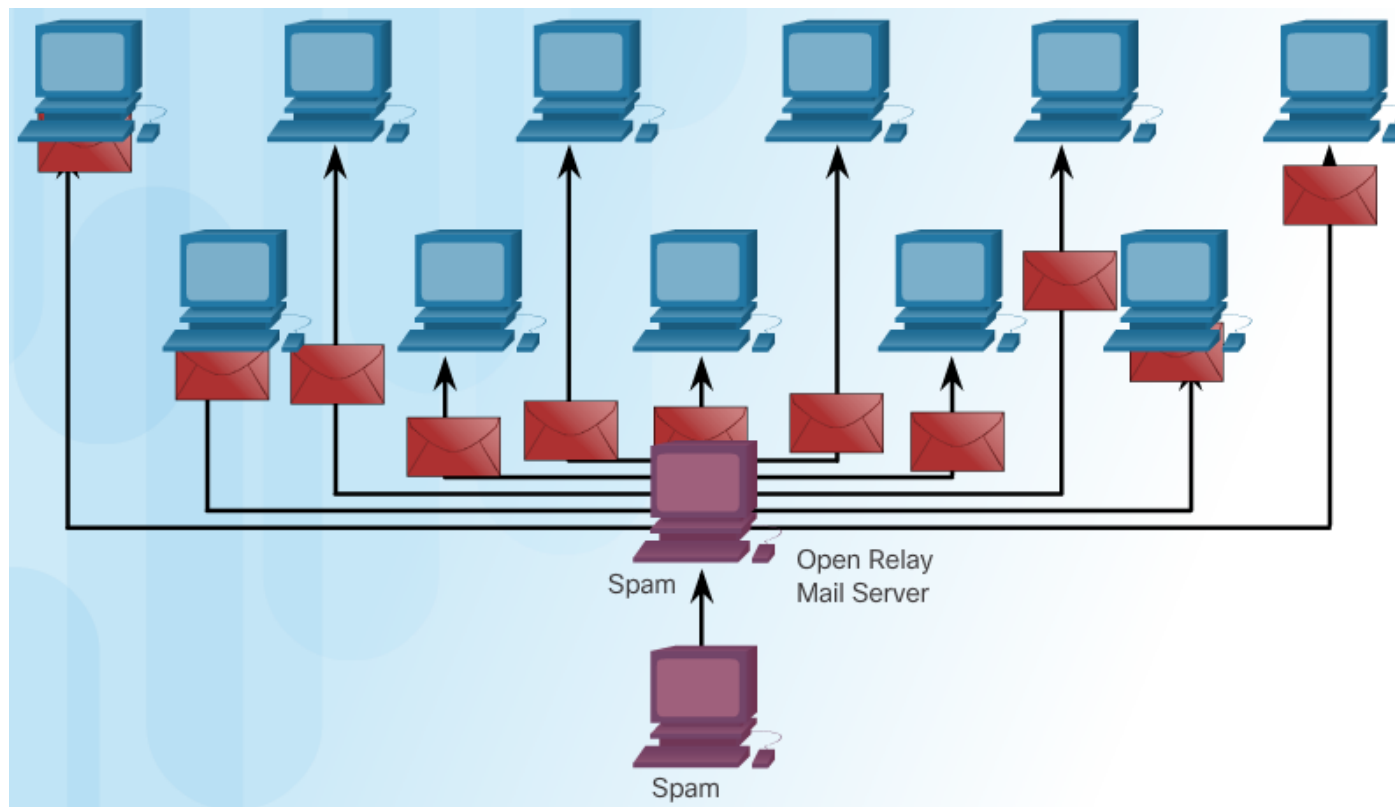


## Methods of Attack

# Other Types of Malware (Cont.)

### ■ Botnets and Zombies

- When infected, the “zombie” computer contacts servers managed by the botnet creator. These servers act as a command and control (C&C) center for an entire network of compromised devices, or "botnet."





## 7.3 How Can I Protect My Network?



Cisco | Networking Academy®  
Mind Wide Open™



## How Can I Protect My Network?

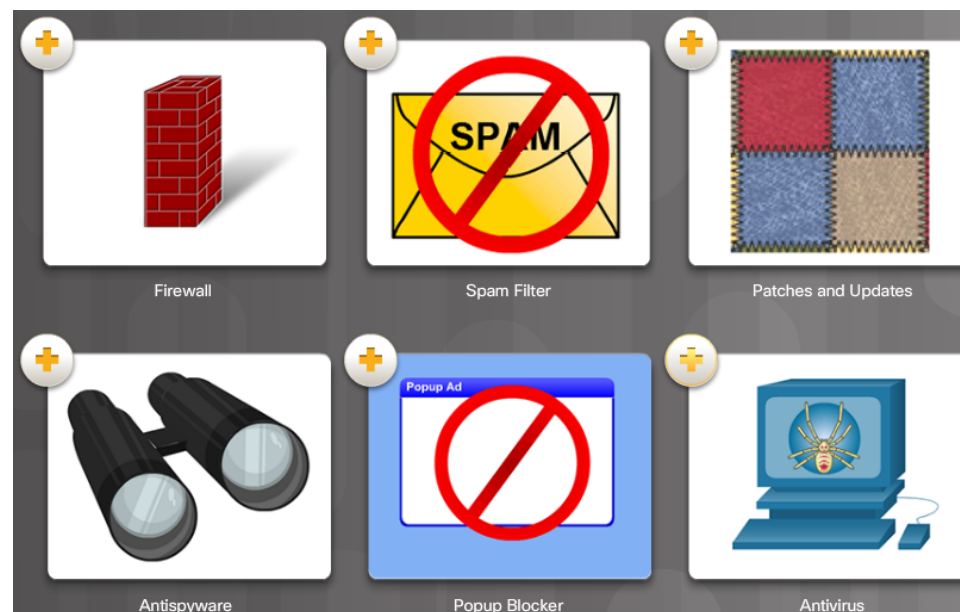
# Security Tools

### ■ Security Practices

- Security procedures can range from simple, inexpensive tasks such as maintaining up-to-date software releases, to complex implementations of firewalls and intrusion detection systems.

### ■ Security Tools

- Many tools are available to network users to protect the devices from attacks and to help remove malicious software from infected machines.



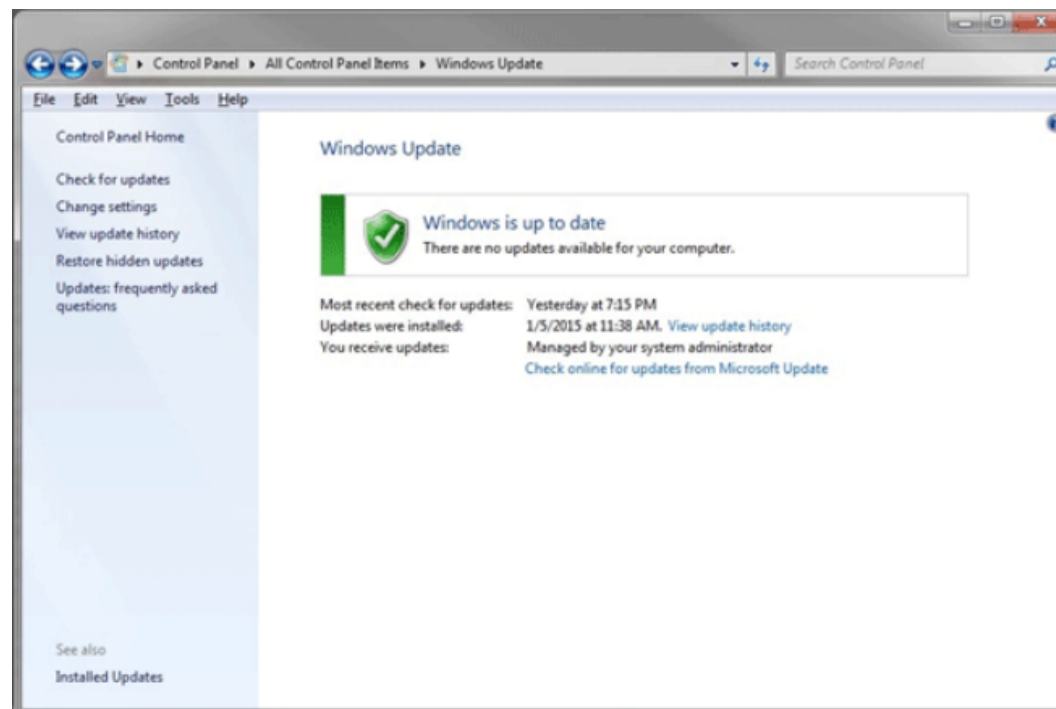


# How Can I Protect My Network?

## Security Tools (Cont.)

### ■ Patches and Updates

- A patch is a small piece of code that fixes a specific problem. An update, on the other hand, may include additional functionality to the software package as well as patches for specific issues.





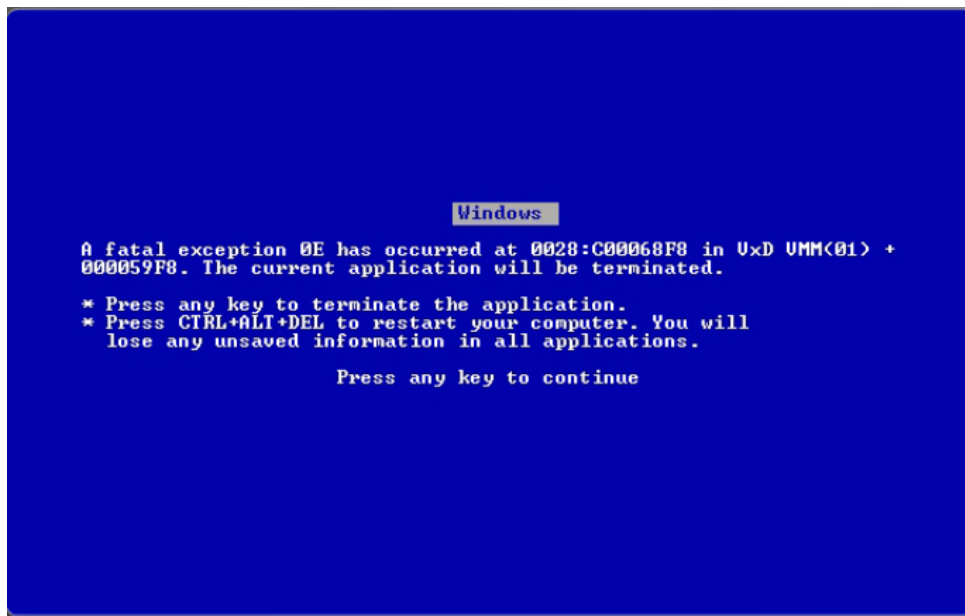


# How Can I Protect My Network?

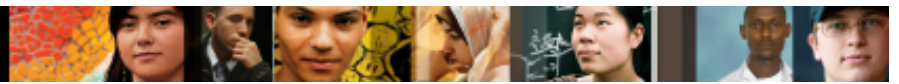
## Antivirus Software

### ■ Infection Detection

- Any device that is connected to a network is susceptible to viruses, worms and Trojan horses. So how do you know if your computer has been infected?



- Computer starts acting abnormally
- Program does not respond to mouse and keystrokes
- Programs starting or shutting down on their own
- Email program begins sending out large quantities of email
- CPU usage is very high
- There are unidentifiable, or a large number of processes running
- Computer slows down significantly or crashes



## How Can I Protect My Network?

# Antivirus Software (Cont.)

### ■ Antivirus Software

- Antivirus software relies on known “virus signatures” in order to find and prevent new viruses from infecting the computer.

### ■ Antispam Software

- Protects hosts by identifying spam and performing an action, such as placing it into a junk folder or deleting it.

### ■ Additional Safeguards

- Before forwarding virus warning emails, check a trusted source to see if the virus is a hoax.

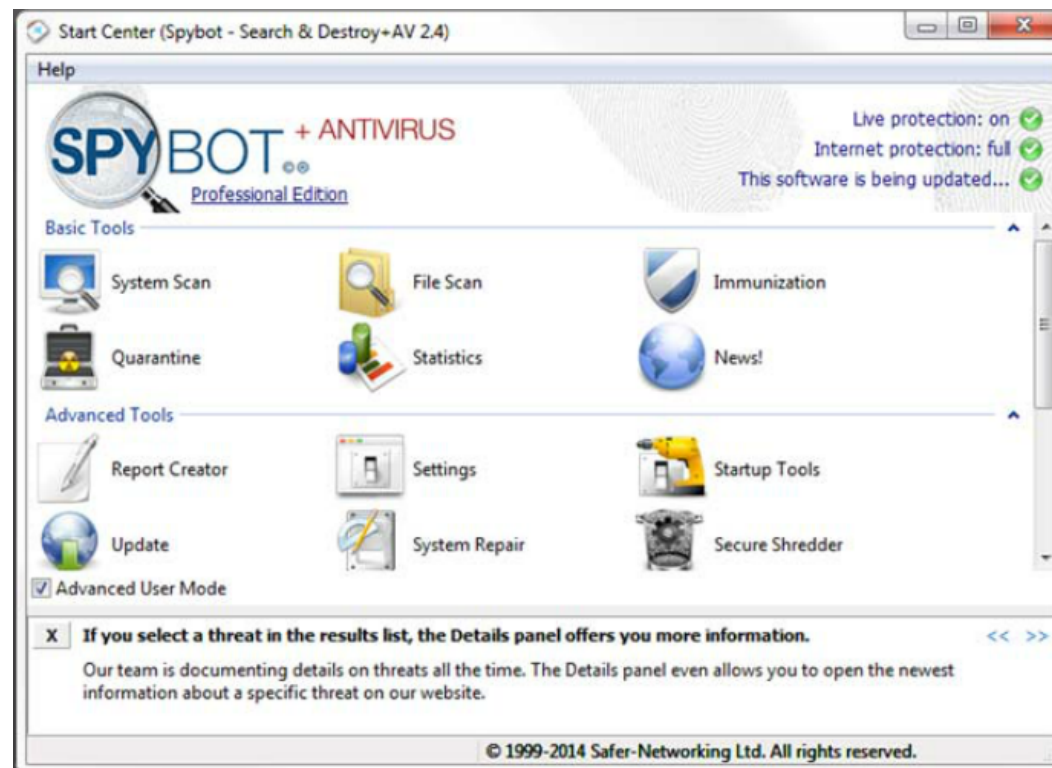




## How Can I Protect My Network?

# Removing Spyware

- Antispyware, Adware, and Popup Blockers
  - Antispyware detects and deletes spyware applications. Many antispyware applications also include detection and deletion of cookies and adware. Popup blocking software can be installed to prevent popups and pop-up-unders.





## 7.4 How Do Firewalls Protect Networks?



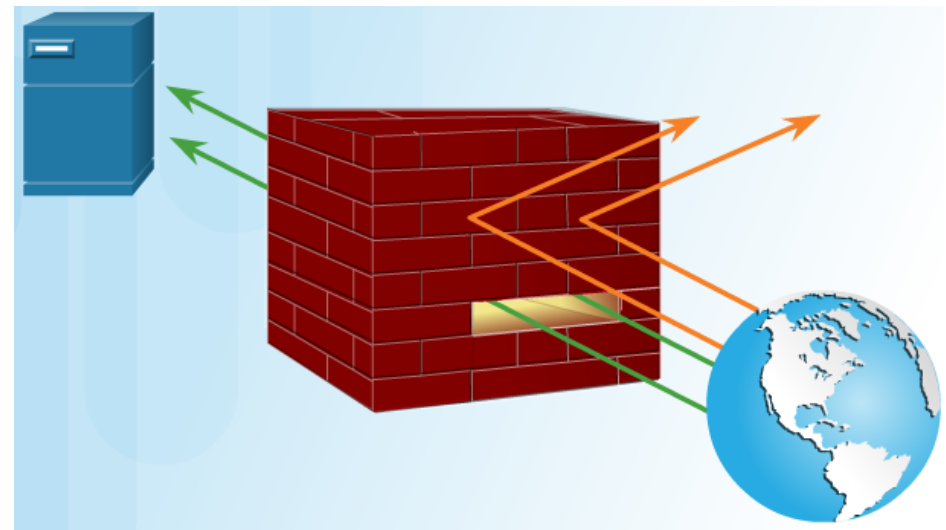


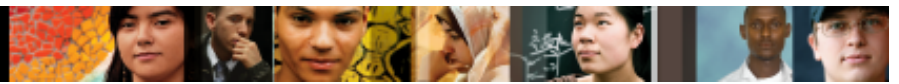
## How Do Firewalls Protect Networks?

# Firewall Basics

### ■ What is a Firewall?

- A firewall prevents undesirable traffic from entering protected areas of the network. A firewall is usually installed between two or more networks and controls the traffic between them as well as helps prevent unauthorized access.
- Firewalls can be implemented in software. Firewalls may also be hardware devices.
- A hardware firewall is a freestanding unit.
- Firewalls often perform Network Address Translation.





## How Do Firewalls Protect Networks?

# Firewall Basics (Cont.)

### ■ DMZ

- In computer networking, a DMZ refers to an area of the network that is accessible to both internal and external users.
- With the wireless router, a simple DMZ can be set up that allows an internal server to be accessible by outside hosts.
- The wireless router isolates traffic destined to the IP address specified. This traffic is then forwarded only to the switch port where the server is connected.





# How Do Firewalls Protect Networks?

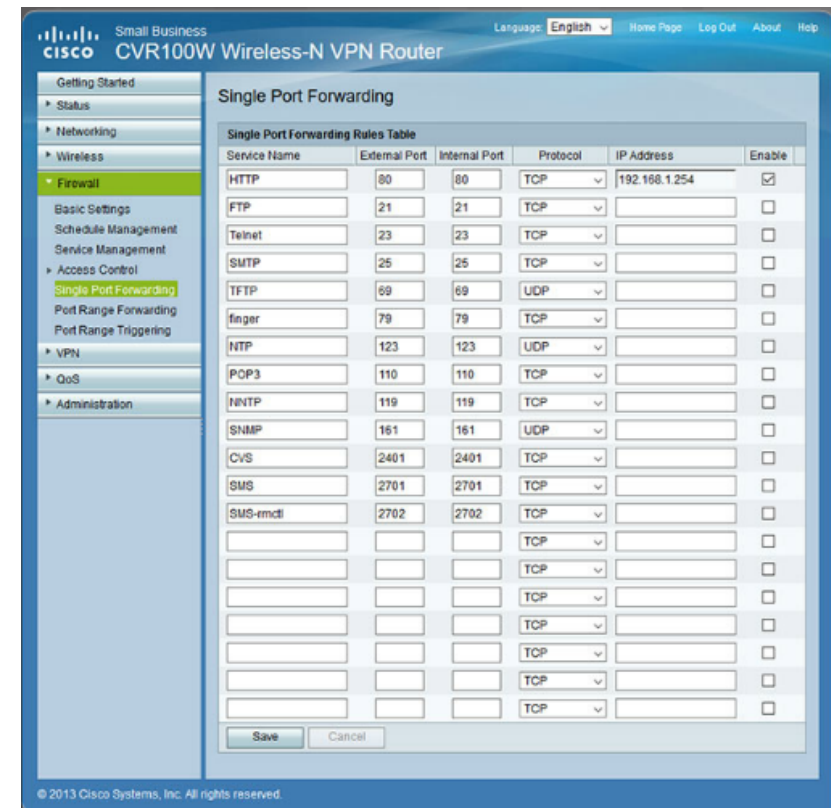
## Configuring Firewalls

### ■ Port Forwarding

- Port forwarding is a rule-based method of directing traffic between devices on separate networks. This method of exposing your devices to the Internet is much safer than using a DMZ.
- The rules that you configure in the firewall settings determine which traffic is permitted on to the LAN.

### ■ Port Triggering

- Port triggering allows the router to temporarily forward data through inbound TCP or UDP ports to a specific device. You can use port triggering to forward data to a computer only when a designated port range is used to make an outbound request.



The screenshot shows the configuration interface for a Cisco CVR100W Wireless-N VPN Router. The left sidebar contains a navigation menu with options like Getting Started, Status, Networking, Wireless, Firewall (selected), Basic Settings, Schedule Management, Service Management, Access Control, Single Port Forwarding (highlighted), Port Range Forwarding, Port Range Triggering, VPN, QoS, and Administration. The main content area is titled 'Single Port Forwarding' and contains a 'Single Port Forwarding Rules Table'.

Service Name	External Port	Internal Port	Protocol	IP Address	Enable
HTTP	80	80	TCP	192.168.1.254	<input checked="" type="checkbox"/>
FTP	21	21	TCP		<input type="checkbox"/>
Telnet	23	23	TCP		<input type="checkbox"/>
SMTP	25	25	TCP		<input type="checkbox"/>
TFTP	69	69	UDP		<input type="checkbox"/>
finger	79	79	TCP		<input type="checkbox"/>
NTP	123	123	UDP		<input type="checkbox"/>
POP3	110	110	TCP		<input type="checkbox"/>
NNTP	119	119	TCP		<input type="checkbox"/>
SNMP	161	161	UDP		<input type="checkbox"/>
CvS	2401	2401	TCP		<input type="checkbox"/>
SMS	2701	2701	TCP		<input type="checkbox"/>
SMS-rmcll	2702	2702	TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>
			TCP		<input type="checkbox"/>

At the bottom of the table are 'Save' and 'Cancel' buttons. The footer of the page reads '© 2013 Cisco Systems, Inc. All rights reserved.'



