Module 16: Configure Network and Device Security

Networking Essentials (NETESS)

Module Objective

Module Title: Configure Network and Device Security
Module Objective: Configure Network and Device Security

Topic Title	Topic Objective
Wireless Security Measures	Describe basic ways to address wireless security vulnerabilities.
Implement Wireless Security	Configure user authentication.
Configure a Firewall	Configure firewall settings.

16.1 Wireless Security Measures

Wireless Vulnerabilities

- Wireless networking provides ease and convenience of connecting devices.
- Unfortunately, that ease of connectivity and the fact that the information is transmitted through the air also makes the wireless network vulnerable to interception and attacks, such as war-driving.
- **War-driving** is the process of driving around and searching for wireless networks. When a wireless network is found, the location of the WLAN is logged and shared.
- When the access to a WLAN is compromised, an attacker can access the network from any location the wireless signal reaches.
- Special security features and implementation methods are required to help protect a WLAN from attacks.

A Comprehensive Security Plan

Security measures should be planned and configured before connecting the home wireless router to the network, including:

- **Basic Wireless Setting** – Change the default SSID and disable SSID broadcast.
- **Wireless Security** – Set the security profile for each band to use WPA2 Personal, AES and passphrase.
- **MAC Address Filtering** – Configure the specific MAC addresses to prevent or permit on the WLAN.
- **Port Forwarding** – Configure the ports that should be forwarded to a specific device, such as a web server in the demilitarized zone (DMZ).
- **Demilitarized Zone (DMZ)** – Configure the IPv4 address for the server in the DMZ.

Wireless Security Measures

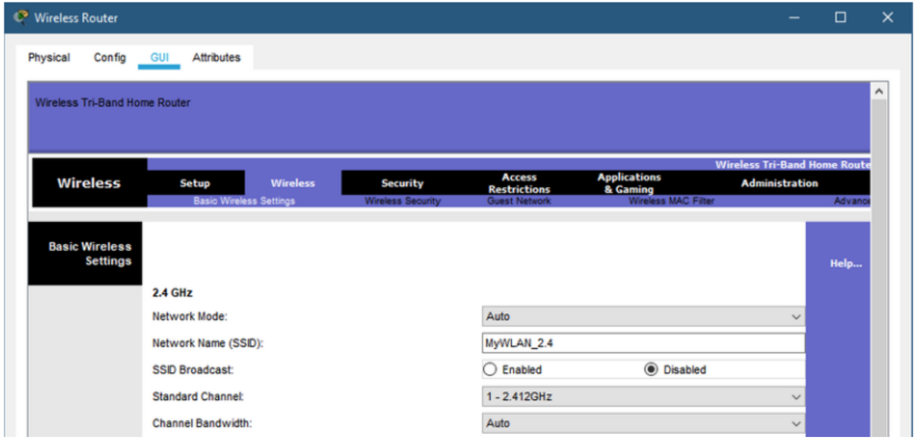
Video - Secure a Wireless Home Network

Wireless Security Measures

SSID Broadcasts

- One easy way to gain entry to a wireless network is through the network name, or SSID.
- By default, wireless routers and access points broadcast SSIDs to all computers within the wireless range.
- With SSID broadcast activated, any wireless client can connect to it, if no other security features are configured.

- The SSID broadcast feature can be turned off. When it is turned off, the wireless network is no longer made public.
- Any client must already know the SSID to join the network.
- Note, turning off SSID broadcast alone does not protect the wireless network from experienced threat actors.



2.4 GHz

Network Mode: Auto

Network Name (SSID): MyWLAN_2.4

SSID Broadcast: ○ Enabled ● Disabled

Standard Channel: 1 - 2.412GHz

Channel Bandwidth: Auto

Changing Default Settings

- Most wireless access points and routers are preconfigured with settings such as SSIDs, administrator passwords, and IP addresses. These default settings are well-known.
- Changing the default settings on a wireless router will not protect the wireless network by itself. For example, SSIDs are transmitted in plaintext. Even with SSID broadcast turned off and default values changed, attackers can learn the name of a wireless network through the use of devices that intercept wireless signals.
- Other security measures should also be implemented to help protect the network, such as authentication and encryption.

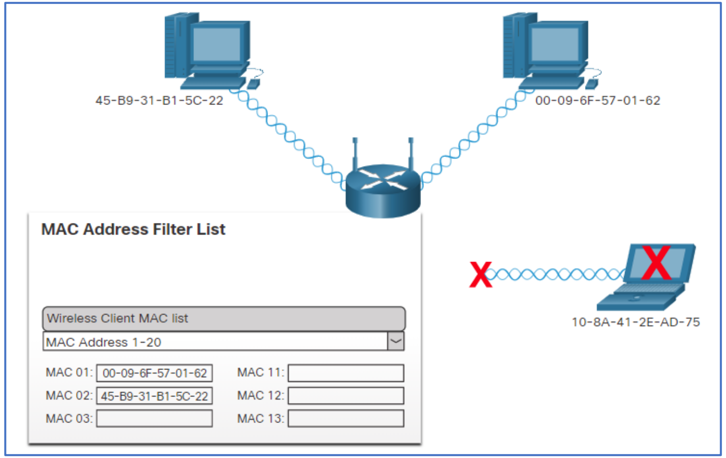
Wireless Security Measures

MAC Address Filtering

- One way to limit access to the wireless network is to control exactly which devices are allowed or not allowed by filtering MAC addresses.

- If MAC address filtering is configured, when a wireless client attempts to connect, or associate, with an AP, the wireless router or AP will look up the MAC address of the connecting client and permit or deny the device onto the wireless network based on the configuration.

- Some issues are with this configuration. The person setting up the wireless router/AP will have to enter MAC addresses manually, so this measure does not scale well.



MAC Address Filter List

Wireless Client MAC list

MAC Address 1-20

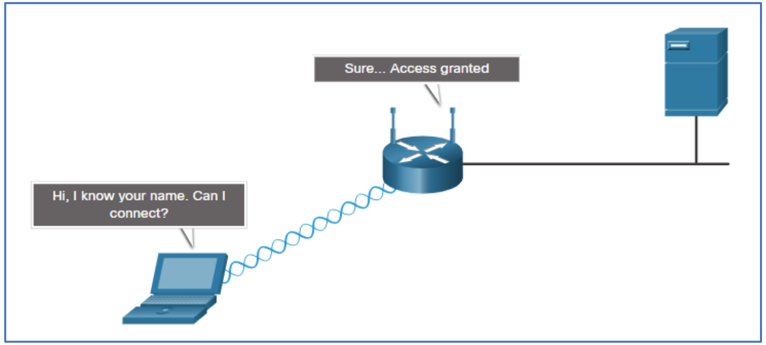
MAC 01:	00-09-6F-57-01-62	MAC 11:	
MAC 02:	45-B9-31-B1-5C-22	MAC 12:	
MAC 03:		MAC 13:	

16.2 Implement Wireless Security

Open Authentication

- Another way to control who can connect to the network is to implement authentication.
- Authentication is the process of permitting entry to a network based on a set of credentials.
- It is used to verify that the device that is attempting to connect to the network is trusted.

- The use of a username and password is a most common form of authentication.
- In a wireless environment, authentication, if enabled, must occur before the client can connect to the WLAN.
- There are different types of wireless authentication methods including open authentication, PSK, EAP, and SAE.
- By default, wireless devices do not require authentication. This is referred to as open authentication.
- Open authentication should only be used on public wireless networks or on networks where authentication will be done by other means.



Authentication and Association

- **Authentication** is to verify that the device that is attempting to connect to the network is trusted.
- **Association** is for a client to successfully connect to the AP and carry data communication.

- After authentication is enabled, regardless of the method used, the client must successfully pass authentication before it can associate with the AP and join the network. If both authentication and MAC address filtering are enabled, authentication occurs first.

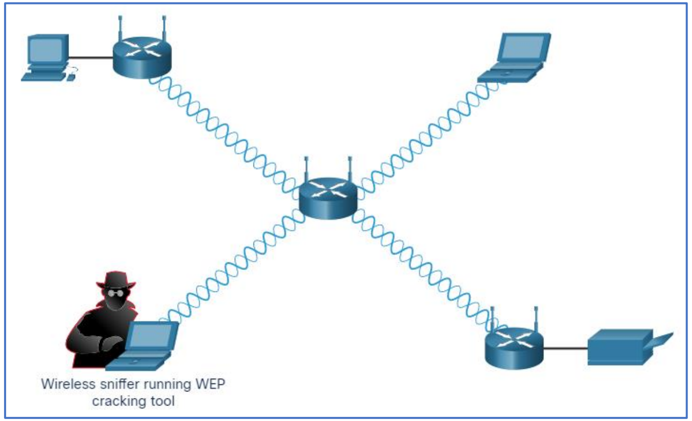
- When authentication is successful, the AP will then check the MAC address against the MAC address table. After verification, the AP adds the host MAC address into its host table. The client is then said to be associated with the AP and can connect to the network.

Implement Wireless Security

Authentication Protocols

- Early wireless routers used an encryption protocol known as Wired Equivalency Protocol (WEP) to secure wireless transmissions between clients and access points.
- WEP uses pre-configured keys to encrypt and decrypt data. A WEP key is entered as a string of numbers and letters and is generally 64 bits or 128 bits long and in some cases, 256 bits long.
- However, there are weaknesses within WEP, including the use of a static key on all WEP-enabled devices on the wireless LAN.

- One way to overcome this vulnerability is to change the key frequently.
- Another way is to use a more advanced and secure form of encryption known as Wi-Fi Protected Access (WPA).
- WPA2 uses encryption keys from 64 bits up to 256 bits.
- WPA2, generates new, dynamic keys each time a client establishes a connection with the AP.
- The version of WPA2 designed for home networks is designated as WPA2-PSK.



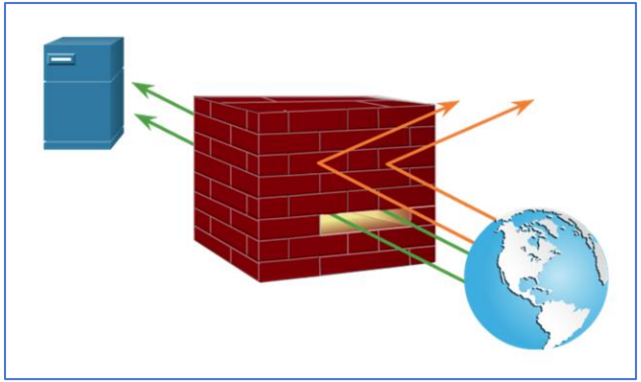
Packet Tracer - Configure Basic Wireless Security

In this activity, you will configure wireless security using WPA2 Personal.

16.3 Configure a Firewall

Firewall Overview

- A firewall prevents undesirable traffic from entering protected areas of the network.
- A firewall is one of the most effective security tools available for protecting internal network users from external threats.
- A firewall is usually installed between two or more networks and controls the traffic between them, as well as helping to prevent unauthorized access.
- Firewall products use various techniques for determining what is permitted or denied access to a network.



Firewall Operation

- Firewalls can be implemented in software which is to be loaded onto PCs, networking devices, or servers.

- Firewalls may also be hardware devices for the single purpose of protecting areas within the network.

- A firewall can be configured to block multiple individual external devices by IP address, to permit or deny packets matching the range of TCP or UDP ports.

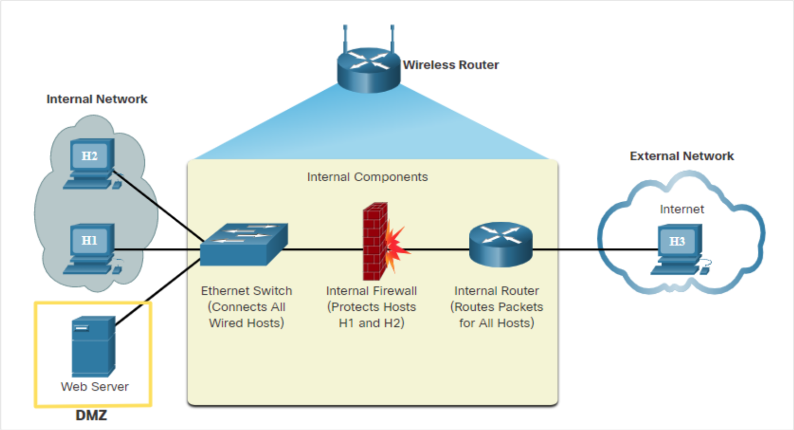
- Typically a firewall passes two different types of traffic into a network:
  - Responses to traffic that originates from inside the network
  - Traffic that originated from outside the organization that is destined for a port that you have intentionally permitted, such as a server located in DMZ

- Additionally, firewalls often perform Network Address Translation (NAT).

Configure a Firewall

The DMZ

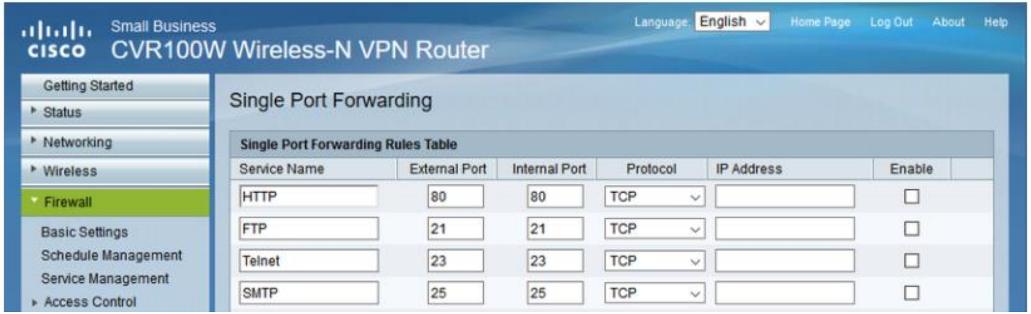
- Many home network devices support demilitarized zone (DMZ) capabilities.
- A DMZ refers to an area of the network that is accessible and controlled for both internal and external users.
- It is more secure than the external network but not as secure as the internal network.
- With the wireless router, a simple DMZ can be set up that allows an internal server to be accessible by outside hosts.
- The server requires a static IP address that must be specified in the DMZ configuration.
- 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.


Wireless Router
Internal Network
H2
H1
Internal Components
External Network
Internet
H3
Ethernet Switch (Connects All Wired Hosts)
Internal Firewall (Protects Hosts H1 and H2)
Internal Router (Routes Packets for All Hosts)
Web Server
DMZ

Configure a Firewall

Port Forwarding

- One way to permit other users to reach devices inside the network through the internet is by port forwarding.
- Port forwarding is a rule-based method of directing traffic between devices on separate networks.
- This method of exposing internal devices to the internet is safer than using a DMZ.
- When incoming traffic from the internet reaches the router, the firewall in the router determines if the traffic should be forwarded to a certain device based on the port number found with the traffic.
- Port numbers are associated with specific services, such as FTP, HTTP, HTTPS, and POP3.
- The port forward rules configured in the firewall settings determine which traffic is permitted on to the inside LAN.



Single Port Forwarding

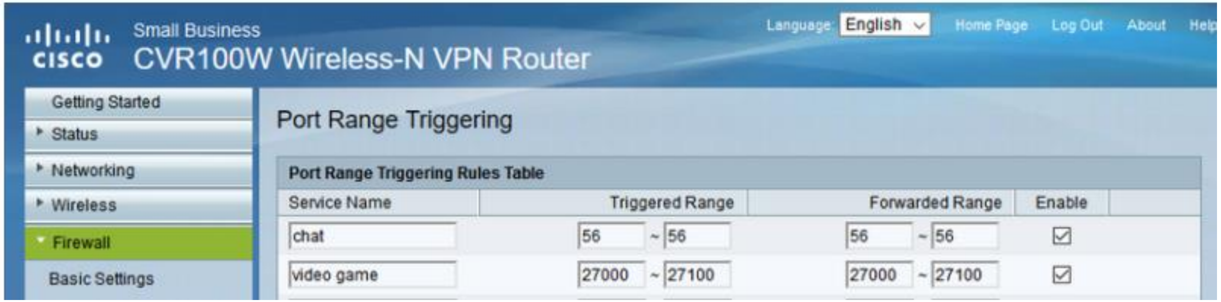
Single Port Forwarding Rules Table

Service Name	External Port	Internal Port	Protocol	IP Address	Enable
HTTP	80	80	TCP		□
FTP	21	21	TCP		□
Telnet	23	23	TCP		□
SMTP	25	25	TCP		□

Configure a Firewall

Port Triggering

- Port triggering allows the router to temporarily forward data through inbound TCP or UDP ports to a specific device.
- Port triggering can be used to forward data to a computer only when a designated port range is used to make an outbound request.
- One usage for port triggering is multiplayer games where a number of TCP and UDP connections could exist between the players while the game is active.
- Port triggering should be configured carefully because leaving a large number of ports open to the internet can represent a security risk.



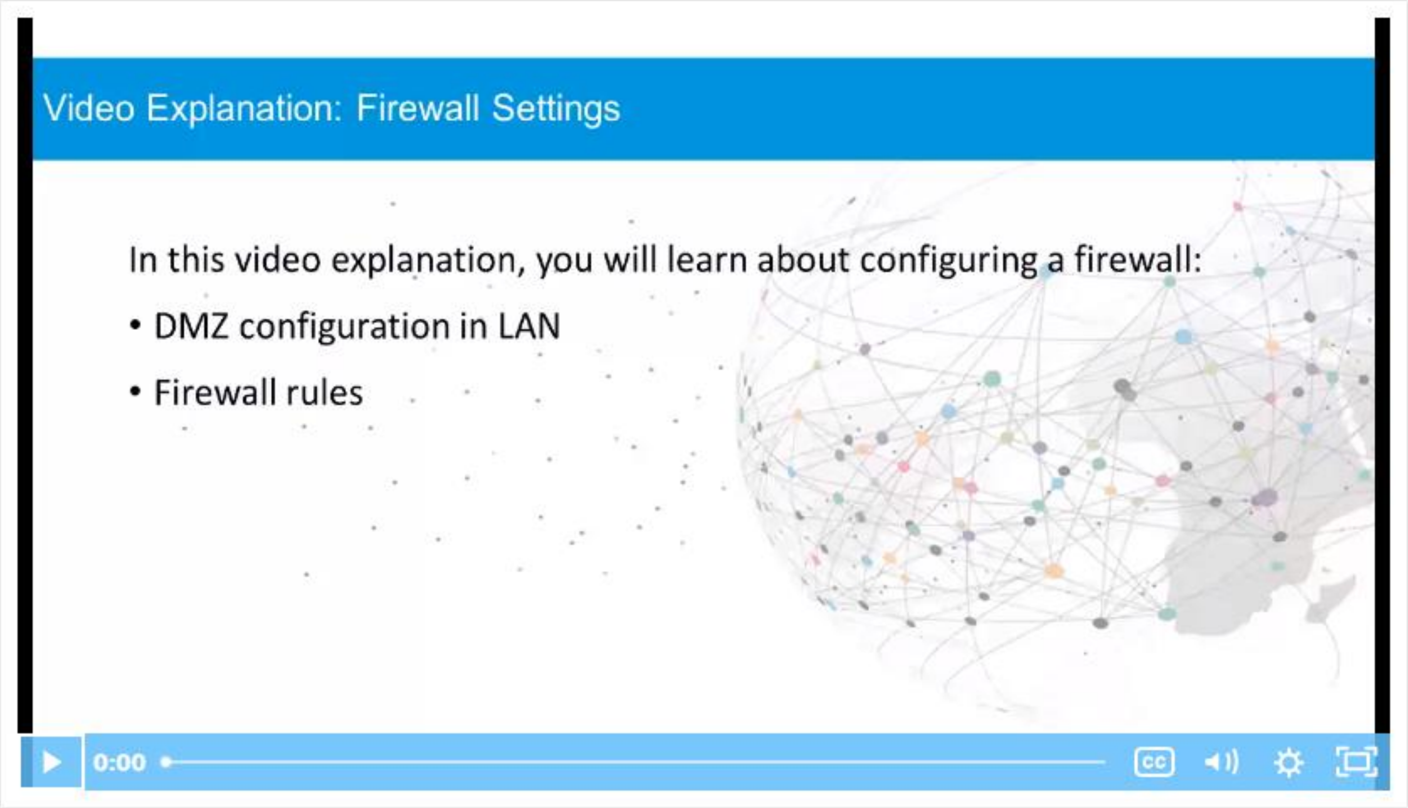
Port Range Triggering

Port Range Triggering Rules Table

Service Name	Triggered Range	Forwarded Range	Enable
chat	56 ~ 56	56 ~ 56	☑
video game	27000 ~ 27100	27000 ~ 27100	☑

Configure a Firewall

Video - Firewall Settings on a Wireless Router



Video Explanation: Firewall Settings

In this video explanation, you will learn about configuring a firewall:

- DMZ configuration in LAN
- Firewall rules

Configure a Firewall

Video - Firewall Settings on a Windows PC

Lab - Configure Windows Firewall Settings

In this lab, you will complete the following objectives:

- Access Windows Firewall settings to add a new firewall rule.
- Create a firewall rule to permit ping requests.
- Remove the new firewall rule to return the settings to their previous state.

16.4 Configure Network and Device Security Summary

What Did I Learn in this Module?

- With wireless connectivity, threat actors can tune into signals from wireless network.
- When wireless access is compromised, threat actors can use your internet services for free, as well as access computers on the network.
- Special security features and implementation methods should be used to help protect the WLAN.
- Default settings on a wireless router should be changed to be more secure and unique.
- MAC address filtering builds a MAC address database that is used to determine whether the devices are allowed or denied to connect to the wireless network.
- Applying a username and password is the most common form of authentication.
- WPA2 uses encryption keys from 64 bits up to 256 bits.
- WPA2 generates new, dynamic keys each time a client establishes a connection with the AP.
- The version of WPA2 designed for home networks is designated as WPA2-PSK.
- Firewall products use techniques for determining what is permitted or denied access to a network.
- Port forwarding is a rule-based method of directing traffic between devices on separate networks.
- Port triggering allows the router to temporarily forward data through inbound TCP or UDP ports to a specific device.

Module 16 - Dynamic Addressing with DHCP

New Terms and Commands

- War Driving
- War Walking
- War Chalking
- WPA2-PSK
- MAC Address Filtering
- Firewall
- Demilitarized Zone (DMZ)
- Port forwarding
- Port triggering