CompTIA A+ Core 2 Exam 220-1102

Lesson 16

Configuring SOHO Network Security

Objectives

- Explain attacks, threats, and vulnerabilities
- Compare wireless security protocols
- Configure SOHO router security
- Summarize security measures

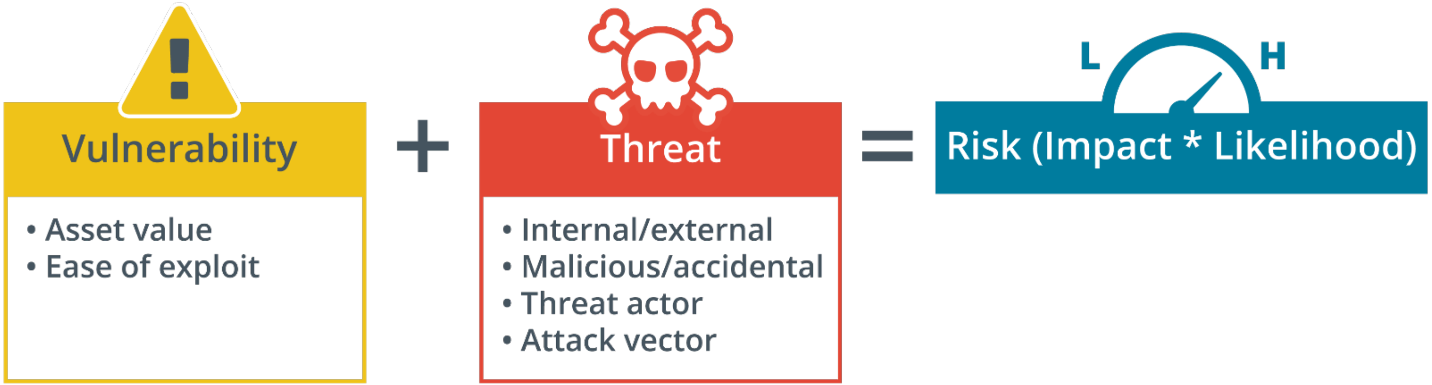
Lesson 16

Topic 16A

Explain Attacks, Threats, and Vulnerabilities

Information Security

- Information security CIA triad
  - Confidentiality, integrity, availability
- Cybersecurity
- Security assessments



Vulnerability
- Asset value
- Ease of exploit

+

Threat
- Internal/external
- Malicious/accidental
- Threat actor
- Attack vector

=

Risk (Impact * Likelihood)

Vulnerabilities

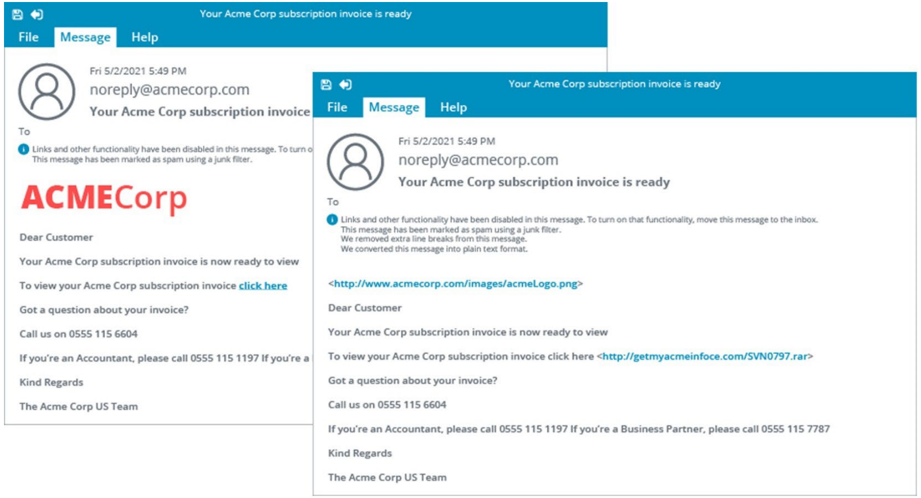
- Non-compliant systems
  - Configuration baselines and hardening
  - Vulnerability scanning
- Unprotected systems
  - Missing or misconfigured antivirus or firewall security controls
- Software and zero-day vulnerabilities
- Unpatched and end of life (EOL) operating systems
- Bring your own device (BYOD) vulnerabilities

Social Engineering

- Impersonation
  - Gain physical or network access/privileges
  - Pretexting
- Dumpster diving
  - Obtain information to develop attacks
- Shoulder surfing
  - Observe passwords and confidential information
- Tailgating and piggybacking
  - Gain physical access

Photo by Uros Jovicic on Unsplash

Phishing and Evil Twins



Fri 5/2/2021 5:49 PM

noreply@acmecorp.com

Your Acme Corp subscription invoice

To

Links and other functionality have been disabled in this message. To turn o
This message has been marked as spam using a junk filter.

ACMECorp

Dear Customer

Your Acme Corp subscription invoice is now ready to view

To view your Acme Corp subscription invoice click here

Got a question about your invoice?

Call us on 0555 115 6604

If you're an Accountant, please call 0555 115 1197 If you're a

Kind Regards

The Acme Corp US Team

Fri 5/2/2021 5:49 PM

noreply@acmecorp.com

Your Acme Corp subscription invoice is ready

To

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the inbox.
This message has been marked as spam using a junk filter.
We removed extra line breaks from this message.
We converted this message into plain text format.

<http://www.acmecorp.com/images/acmeLogo.png>

Dear Customer

Your Acme Corp subscription invoice is now ready to view

To view your Acme Corp subscription invoice click here <http://getmyacmeinfoce.com/SVN0797.rar>

Got a question about your invoice?

Call us on 0555 115 6604

If you're an Accountant, please call 0555 115 1197 If you're a Business Partner, please call 0555 115 7787

Kind Regards

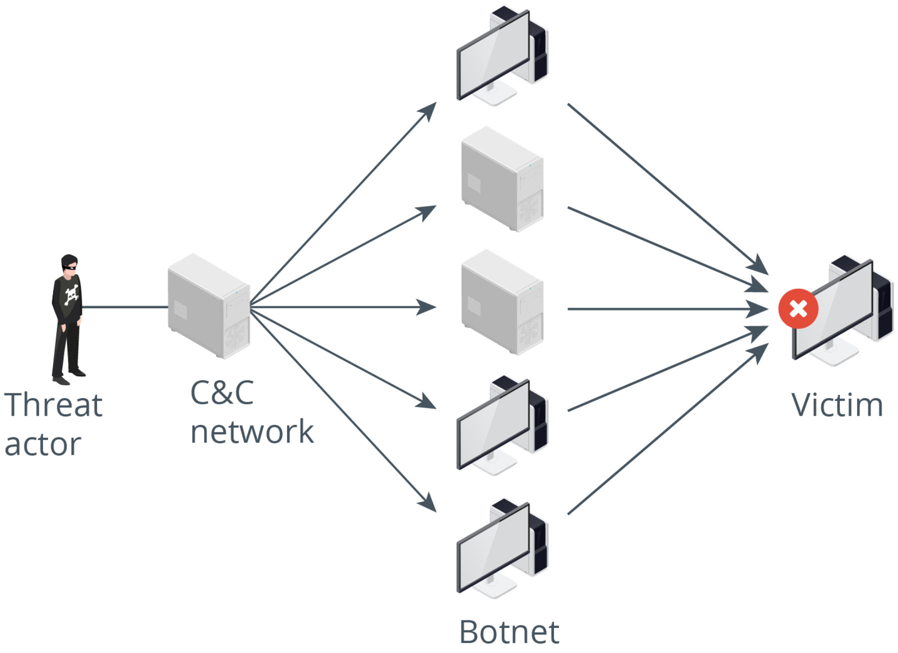
The Acme Corp US Team

Screenshot courtesy of CompTIA

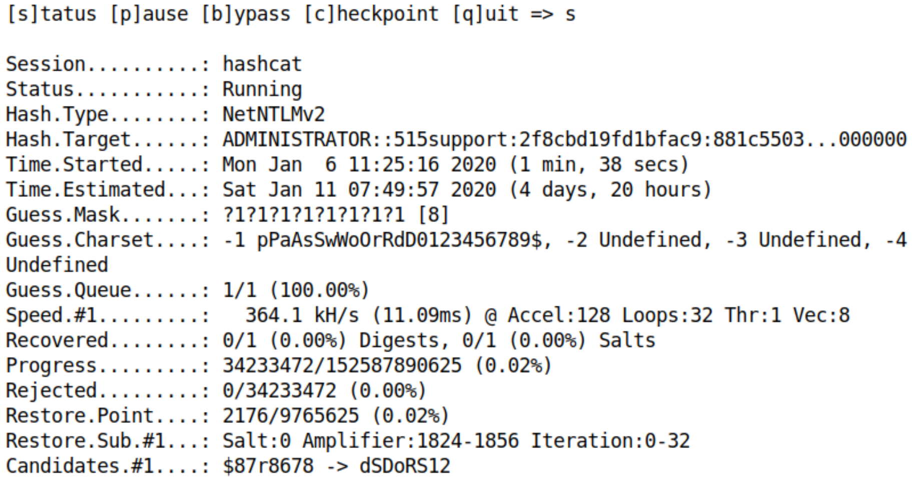
- Phishing
  - Social engineering via spoofed messaging
  - Spear phishing
  - Whaling
  - Vishing
- Evil twin
  - Spoofed access point

Threat Types

- External versus internal threats
- Footprinting threats
- Spoofing threats
- On-path attacks
- Denial of service (DoS) attacks
- Distributed denial of service (DDoS) and botnets



Password Attacks



```
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Type........: NetNTLMv2
Hash.Target......: ADMINISTRATOR::515support:2f8cbd19fd1bfac9:881c5503...000000
Time.Started.....: Mon Jan  6 11:25:16 2020 (1 min, 38 secs)
Time.Estimated...: Sat Jan 11 07:49:57 2020 (4 days, 20 hours)
Guess.Mask.......: ?1?1?1?1?1?1?1?1 [8]
Guess.Charset....: -1 pPaAsSwWoOrRdD0123456789$, -2 Undefined, -3 Undefined, -4
Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   364.1 kH/s (11.09ms) @ Accel:128 Loops:32 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 34233472/152587890625 (0.02%)
Rejected.........: 0/34233472 (0.00%)
Restore.Point....: 2176/9765625 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:1824-1856 Iteration:0-32
Candidates.#1....: $87r8678 -> dSDoRS12
```

- Plaintext passwords
- Password hashes
  - Hashed password files/database
  - Hashes captured in network traffic
- Password hash cracking
  - Dictionary
  - Brute force

Cross-site Scripting Attacks

- Web application vulnerabilities
  - Server-side versus client-side code
  - Input validation
- Cross-site scripting (XSS)
  - Attacker exploits input validation vulnerability to inject code into trusted site/web app
  - Non-persistent versus persistent
  - Arbitrary code could deface site, steal cookies, intercept form data, or install malware

SQL Injection Attacks

- Structured Query Language (SQL)
  - Statements to update and retrieve database records
  - SELECT, INSERT, DELETE, UPDATE
- Threat actor exploits faulty input validation to run arbitrary SQL statements
  - SELECT … FROM … WHERE
- Add or return information in the database without authorization

Hashing and Encryption Concepts

- Hashing
  - Non-reversible conversion of arbitrary length plaintext to fixed length hash
  - Hashes can be compared to prove integrity
- Symmetric encryption
  - Reversible conversion of plaintext to ciphertext
  - Ciphertext can only be deciphered with key, providing confidentiality
- Asymmetric encryption
  - Private and public key pair

Digital Signatures and Key Exchange

- Digital signatures
  - Use hashing and key pair to validate a message or certificate
  - Private key encrypts a hash of the message/certificate
  - Public key decrypts hash
- Key exchange
  - Use key pair to protect exchange of bulk encryption secret key
  - Public key encrypts secret session key
  - Private key decrypts session key

Review Activity: Attacks, Threats, and Vulnerabilities

- Information Security and Vulnerabilities
- Social Engineering, Phishing, and Evil Twins
- Threat Types
- Password Attacks
- Cross-site Scripting and SQL Injection Attacks
- Hashing and Encryption Concepts
- Digital Signatures and Key Exchange

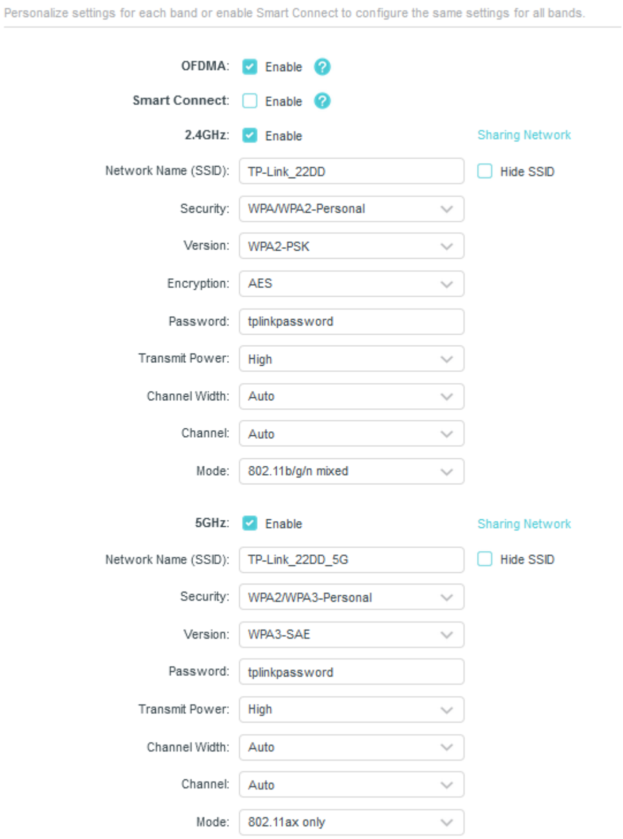
Lesson 16

Topic 16B

Compare Wireless Security Protocols

Wi-Fi Protected Access

- WPA
  - Temporal Key Integrity Protocol (TKIP) with RC4 cipher
  - Stop-gap attempt to fix flaws in earlier Wired Equivalent Privacy (WEP) standard
- WPA2
  - Uses stronger Advanced Encryption Standard (AES) cipher
- WPA3
  - Replaces 4-way handshake with Simultaneous Authentication of Equals (SAE)
  - Management frame protection and Wi-Fi Enhanced Open



Personalize settings for each band or enable Smart Connect to configure the same settings for all bands.

OFDMA: ☑ Enable

Smart Connect: ☐ Enable

2.4GHz: ☑ Enable — Sharing Network

Network Name (SSID): TP-Link_22DD ☐ Hide SSID

Security: WPA/WPA2-Personal

Version: WPA2-PSK

Encryption: AES

Password: tplinkpassword

Transmit Power: High

Channel Width: Auto

Channel: Auto

Mode: 802.11b/g/n mixed

5GHz: ☑ Enable — Sharing Network

Network Name (SSID): TP-Link_22DD_5G ☐ Hide SSID

Security: WPA2/WPA3-Personal

Version: WPA3-SAE

Password: tplinkpassword

Transmit Power: High

Channel Width: Auto

Channel: Auto

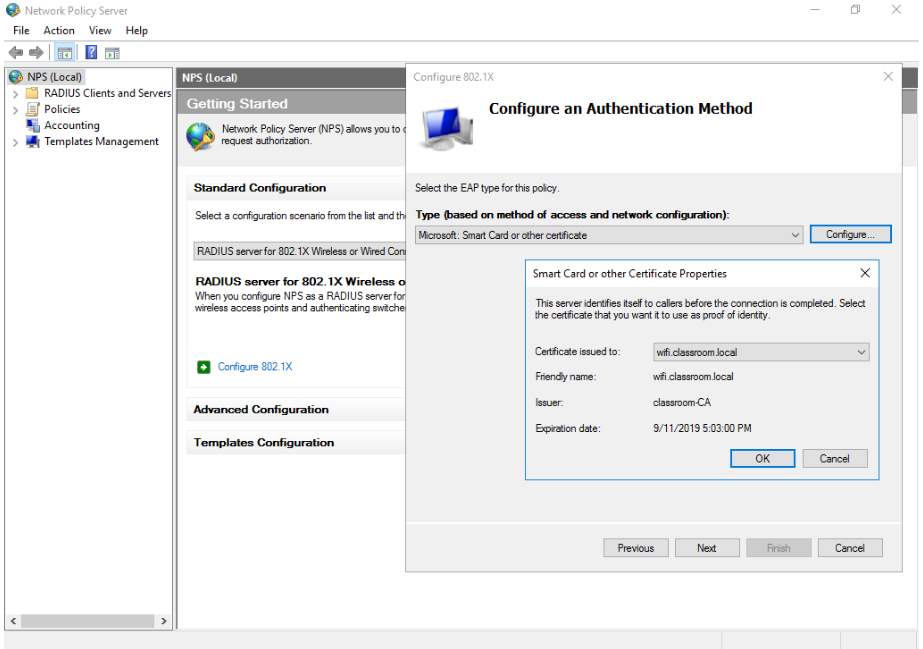
Mode: 802.11ax only

Screenshot courtesy of TP-Link

Wi-Fi Authentication Methods

- Open, personal, and enterprise authentication methods
- WPA2 pre-shared key authentication
  - Passphrase authentication credential is used to generate a master key
  - Station and access point exchange hashed messages derived from master key to establish trust
  - Master key is used in the generation of a transit key to encrypt data messages
  - 4-way handshake vulnerable to key recovery attacks
- WPA3 personal authentication
  - Still uses passphrase but replaces 4-way handshake with more secure key agreement process

Enterprise Authentication Protocols



Network Policy Server (NPS) allows you to c
request authorization.

Select a configuration scenario from the list and th

RADIUS server for 802.1X Wireless or Wired Con

RADIUS server for 802.1X Wireless o

When you configure NPS as a RADIUS server for
wireless access points and authenticating switche

Select the EAP type for this policy.

Type (based on method of access and network configuration):

Microsoft: Smart Card or other certificate

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued to: wifi.classroom.local

Friendly name: wifi.classroom.local

Issuer: classroom-CA

Expiration date: 9/11/2019 5:03:00 PM

Screenshot courtesy of Microsoft

- 802.1X
  - Network directory holds account details and permissions
  - Access point shuttles Extensible Authentication Protocol (EAP) traffic between station and authentication server/directory
- EAP supports multifactor authentication methods
  - EAP with Transport Layer Security (EAP-TLS)

RADIUS, TACACS+, and Kerberos

- Remote Authentication Dial-In User Service (RADIUS)
  - Access point is client of RADIUS server
  - Configured with IP address and shared secret
- Terminal Access Controller Access-Control System (TACACS+)
  - Often used to authenticate and authorize appliance administrators rather than end-users
- Kerberos authentication and authorization for SSO

Review Activity: Wireless Security Protocols

- Wi-Fi Protected Access
- Wi-Fi Authentication Methods
- Enterprise Authentication Protocols
- RADIUS, TACACS+, and Kerberos

Lesson 16

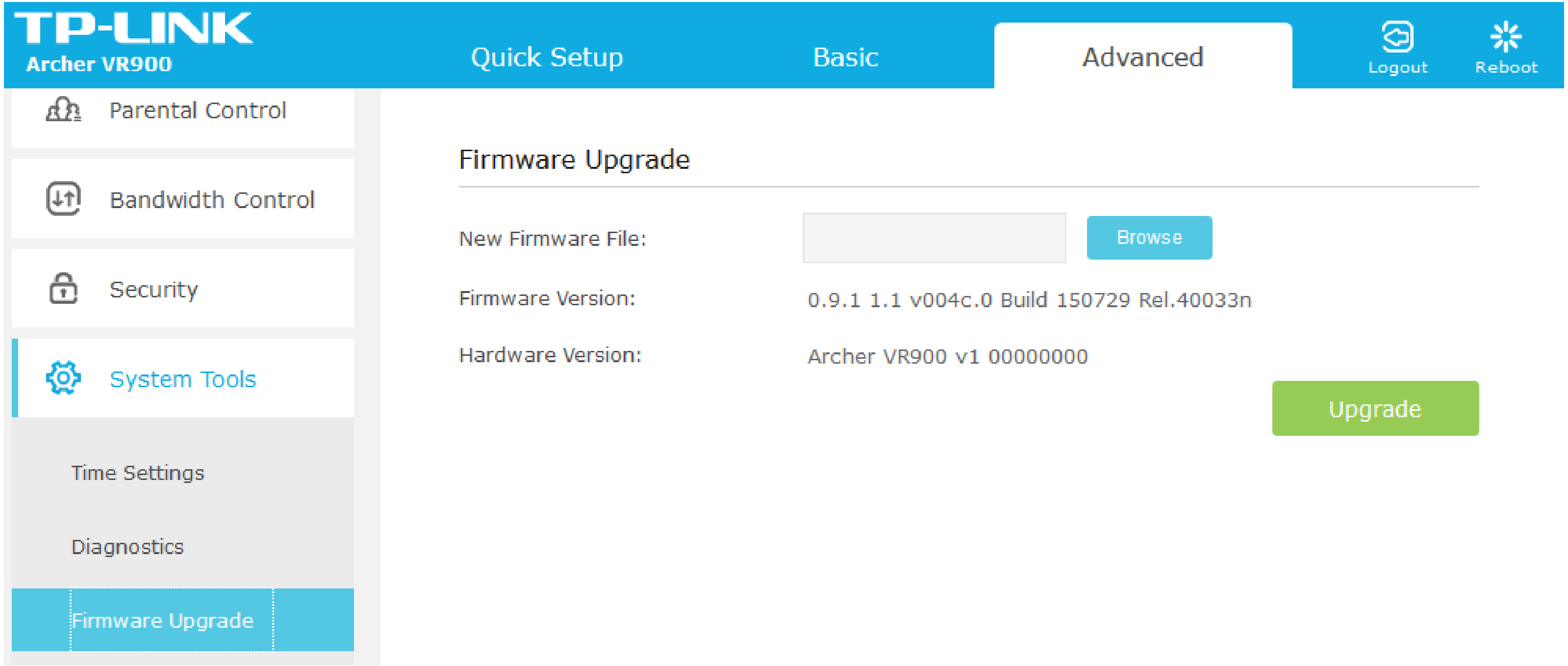
Topic 16C

Configure SOHO Router Security

Home Router Setup

- Physical placement/secure locations
- Setup process
  - Management IP/address
  - Change default passwords
- Internet access and static wide-area network (WAN) IP

Firmware Update



Firmware Upgrade

New Firmware File: Browse

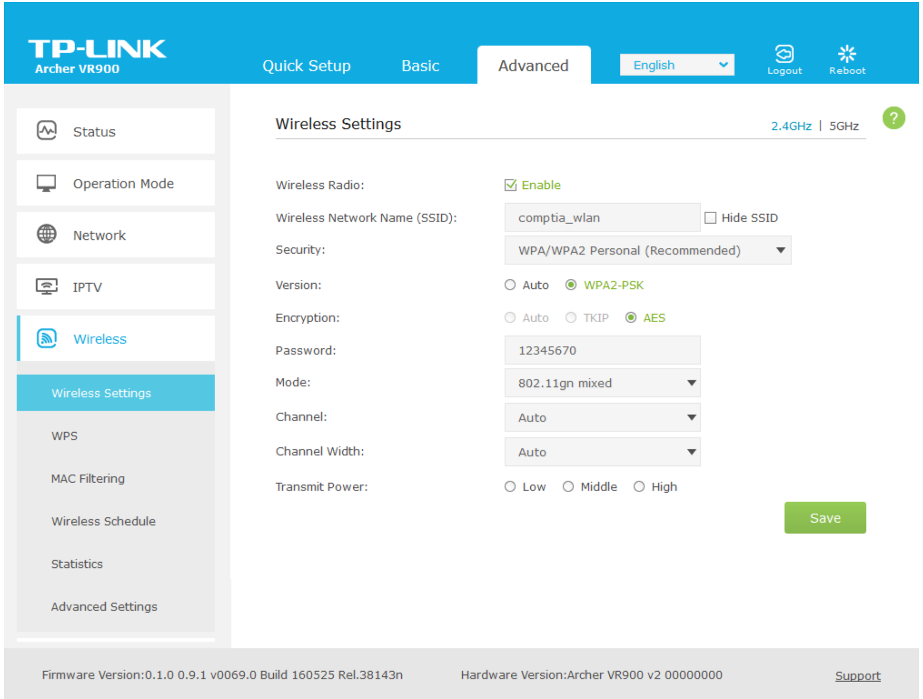
Firmware Version: 0.9.1 1.1 v004c.0 Build 150729 Rel.40033n

Hardware Version: Archer VR900 v1 00000000

Upgrade

Screenshot courtesy of TP-Link

Home Router LAN and WLAN Configuration



Wireless Settings — 2.4GHz | 5GHz

Wireless Radio: ☑ Enable

Wireless Network Name (SSID): comptia_wlan ☐ Hide SSID

Security: WPA/WPA2 Personal (Recommended)

Version: ○ Auto ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

Password: 12345670

Mode: 802.11gn mixed

Channel: Auto

Channel Width: Auto

Transmit Power: ○ Low ○ Middle ○ High

Save

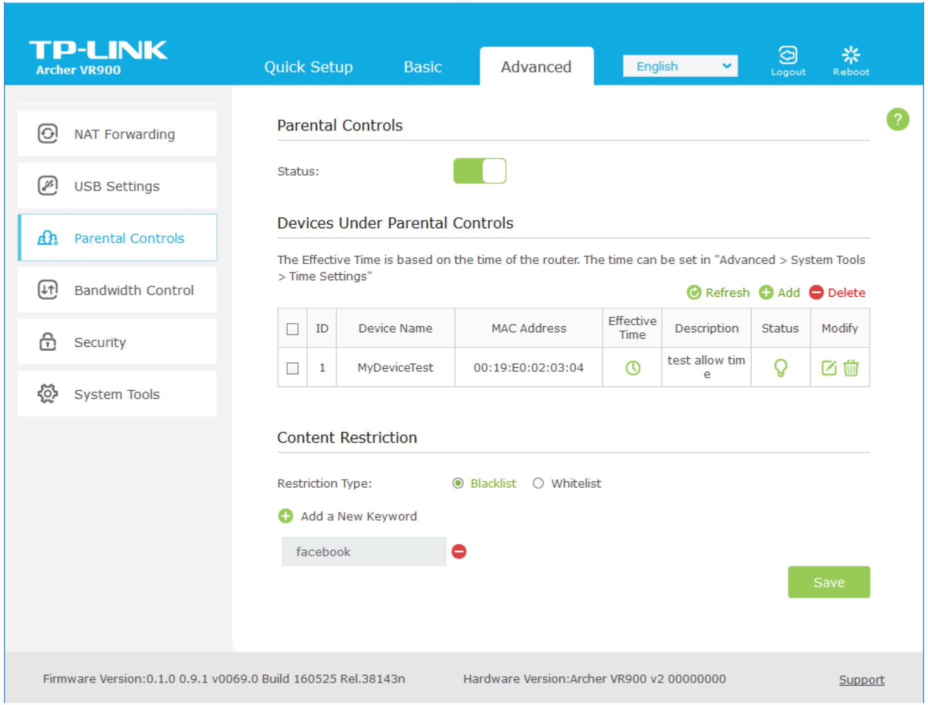
Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n Hardware Version:Archer VR900 v2 00000000 Support

Screenshot courtesy of TP-Link

- Service set identifier (SSID)
  - Choosing a non-default name
  - Disabling broadcast
- Encryption settings
  - WPA mode and compatibility
  - Authentication type
- Disabling guest access
- Changing channels

Home Router Firewall Configuration

- Inbound filtering
  - Block by default and configure port forwarding exceptions
- Outbound filtering
  - Allow by default and configure content filtering
- IP address filtering
- Content filtering
  - Blocklists and reputation databases



Parental Controls

Status: ●

Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings"

□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
□	1	MyDeviceTest	00:19:E0:02:03:04	🕓	test allow time	💡	✎ 🗑

Content Restriction

Restriction Type: ● Blacklist ○ Whitelist

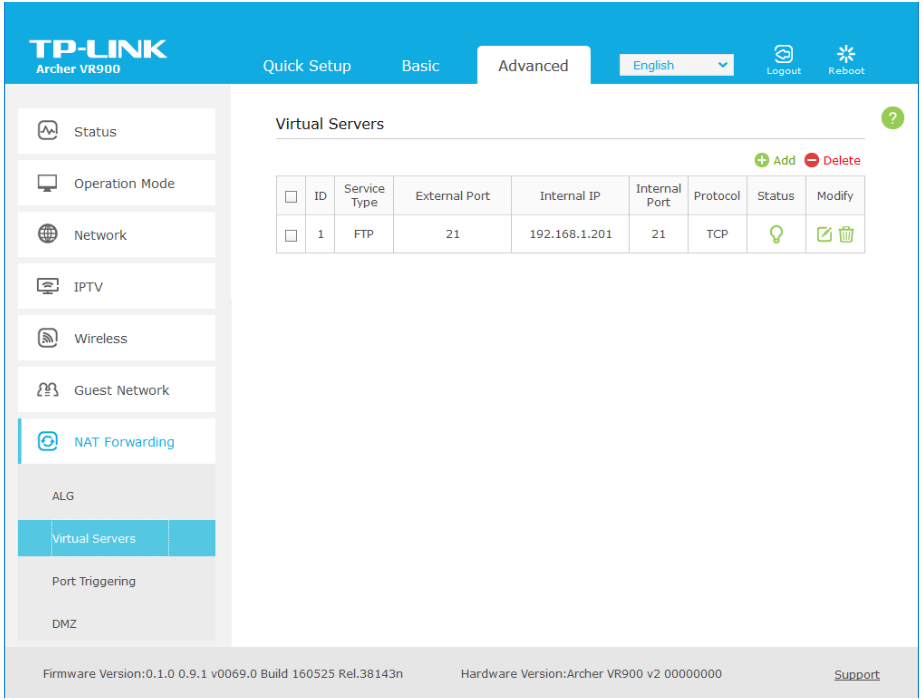
Add a New Keyword

facebook

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n   Hardware Version:Archer VR900 v2 00000000

Screenshot courtesy of TP-Link

Home Router Port Forwarding Configuration



Virtual Servers

□	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
□	1	FTP	21	192.168.1.201	21	TCP		

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n

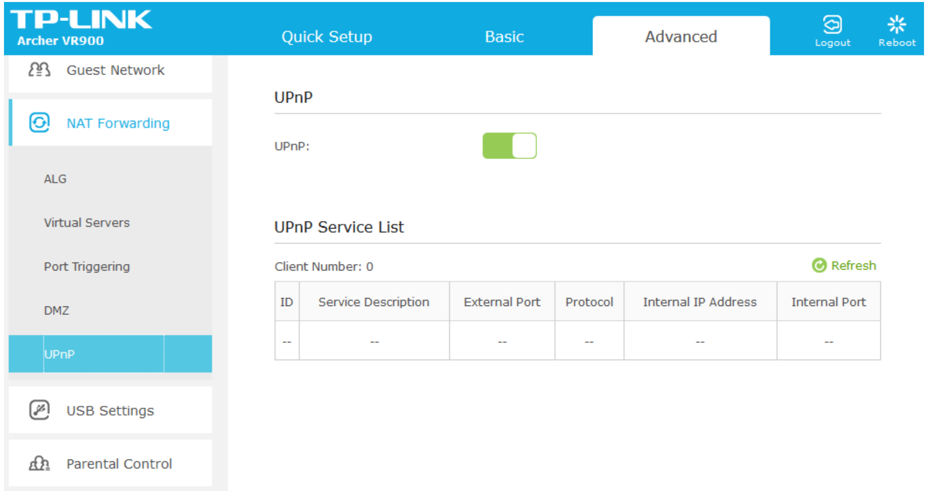
Hardware Version:Archer VR900 v2 00000000

Screenshot courtesy of TP-Link

- Allow incoming traffic to reach a designated LAN IP address and port
- Static IP address and DHCP reservations
- Configuring port forwarding and port triggering rules
  - Forward inbound request for port to same port on LAN host
  - Map to different port on LAN host
- Disabling unused ports

Universal Plug-and-Play

- Allows LAN devices and apps to autoconfigure port forwarding rules
- Associated with many vulnerabilities



UPnP

UPnP:

UPnP Service List

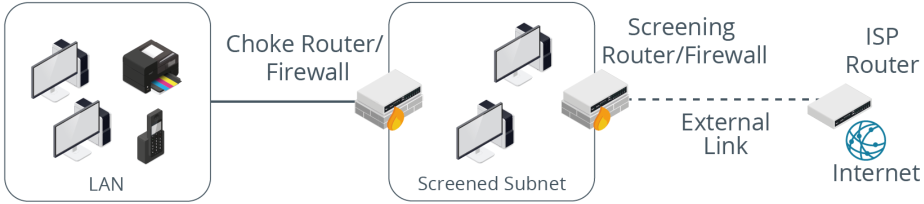
Client Number: 0

Refresh

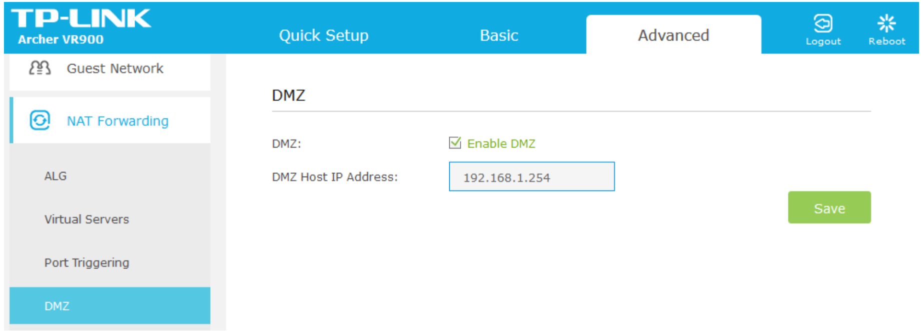
ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
--	--	--	--	--	--

Screenshot courtesy of TP-Link

Screened Subnets



Images © 123RF.com



DMZ

DMZ: ☑ Enable DMZ

DMZ Host IP Address: 192.168.1.254

Screenshot courtesy of TP-Link

- Enterprise screened subnet or demilitarized zone (DMZ)
  - Compromised server can expose LAN to attacks
  - Enterprise networks use segment-based screened subnets
  - Different firewall rules apply between each segment
- “DMZ host” or “SOHO DMZ” is a LAN host left open to access from the Internet

Review Activity: SOHO Router Security

- Home Router Setup
- Firmware Updates
- Home Router LAN and WLAN Configuration
- Home Router Firewall and Port Forwarding Configuration
- Universal Plug-and-Play
- Screened Subnets

Lab Activity

- Assisted Lab: Configure SOHO Router Security
  - Configure a secure wireless network and apply a port forwarding configuration to a home router

Lesson 16

Topic 16D

Summarize Security Measures

Physical Access Control

- Site/premises security systems
- Perimeter security
  - Fences and bollards
- Access control vestibules
  - Ensure only one person enters at a time
- Magnetometers
  - Metal detector to prevent unauthorized items
- Security guards
  - Enforce and monitor security systems and support users

Lock Types

Image by Bunlue Nantaprom © 123RF.com

- Door locks
  - Keys operated
  - Electronic
  - Badge reader
    - Magnetic swipe cards
    - Smart cards and key fobs
  - Biometric scanner (fingerprint/palmprint/retina)
- Equipment locks

Alarms and Surveillance

- Alarm systems
  - Circuit, motion, proximity, and duress
- Video surveillance
  - Closed circuit television (CCTV) or IP camera
  - Motion detection and facial recognition
- Lighting
  - Personal safety
  - Facilitate surveillance

Review Activity: Security Measures

- Physical Access Control
- Lock Types
- Alarms and Surveillance

CompTIA A+ Core 2 Exam 220-1102

Lesson 16

Summary