



**Certified Wireless Network Administrator (CWNA)
PW0-106**

Chapter 13
802.11 Network Security Architecture





Chapter 13 Overview

- 802.11 Security Basics
- Legacy 802.11 Security
- Robust Security
- Traffic Segmentation
- Infrastructure Security
- VPN Wireless Security

Certified Wireless Network Administrator: CWNA – PW0-106



2



802.11 Security Basics

- Data privacy
- AAA
Segmentation
- Monitoring
- Policy



Certified Wireless Network Administrator, CWNA – PW0-106 3



Data Privacy

- About the protection of data and the prevention of unauthorized access to it
- Uses encryption
 - RC4
 - AES



Certified Wireless Network Administrator, CWNA – PW0-106 4



AAA

- Authentication
 - Who are you?
 - What are you?
- Authorization
 - What can you do?
- Accounting
 - What did you do?



Certified Wireless Network Administrator, CWNA – PW0-106 5



Segmentation

- LANs
- WANs
- VLANs



Certified Wireless Network Administrator, CWNA – PW0-106 6



Policy

- Defines how computer systems must be implemented
 - Specific WiFi policies must be created
 - Traditional wired policies are not sufficient

Certified Wireless Network Administrator, CWNA – PW0-106 7



Legacy 802.11 Security

- Legacy authentication
 - Open System
 - Shared Key
- Static WEP encryption
- MAC filters
- SSID cloaking or hiding

Certified Wireless Network Administrator, CWNA – PW0-106 8

SYBEX **WILEY**

Static WEP

- Three main goals
 - Confidentiality The primary goal of confidentiality was to provide data privacy by encrypting the data before transmission.
 - Access Control WEP also provides access control, which is basically a crude form of authorization. Client stations that do not have the same matching static WEP key as an access point are refused access to network resources.
 - Data Integrity A data integrity checksum known as the integrity check value (ICV) is computed on data before encryption and used to prevent data from being modified.

Certified Wireless Network Administrator, CWNA – PW0-106 9

SYBEX **WILEY**

WEP Key and IV

64-bit WEP	24-bit IV	40-bit static key
128-bit WEP	24-bit IV	104-bit static key

Certified Wireless Network Administrator, CWNA – PW0-106 10

SYBEX **WILEY**

Transmission key

Static WEP Keys

Alphabet Set ?	Transmit Key	WEP Key Size
<input type="checkbox"/> WEP Key 1	01234567890123456789abcdef	40 128
<input type="checkbox"/> WEP Key 2		<input type="radio"/> <input type="radio"/>
<input type="checkbox"/> WEP Key 3		<input type="radio"/> <input type="radio"/>
<input type="checkbox"/> WEP Key 4		<input type="radio"/> <input type="radio"/>

Key Entry Method: Hexadecimal (0-9,A-F) ASCII Text

OK Cancel Help

Certified Wireless Network Administrator: CWNA – PW0-106 11

SYBEX **WILEY**

WEP encryption process

```
graph LR; IV[Initialization vector (IV)] --> Seed; WEP_key[WEP key] --> Seed; Seed --> RC4[RC4 algorithm]; RC4 --> Keystream; Plaintext --> XOR; Keystream --> XOR; XOR --> Encrypted_data[Encrypted data (ciphertext)]; Plaintext --> CRC32[CRC-32]; CRC32 --> ICV[Integrity check value (ICV)];
```



Initialization vector (IV) → Seed → RC4 algorithm → Keystream → XOR process → Encrypted data (ciphertext)

WEP key → Seed

Plaintext → XOR process

Plaintext → CRC-32 → Integrity check value (ICV)



Certified Wireless Network Administrator: CWNA – PW0-106 12



WEP attacks

- IV Collisions Attack
- Weak Key Attack
- Reinjection Attack
- Bit-Flipping Attack

Certified Wireless Network Administrator, CWNA – PW0-106 13



Other security measures

- MAC Filters
- SSID Cloaking
- In and of themselves these measures are not sufficient
- Can be a part of a layered approach



Certified Wireless Network Administrator, CWNA – PW0-106 14

802.11 standard	Wi-Fi Alliance certification	Authentication method	Encryption method	Cipher	Key generation
802.11 legacy		Open System or Shared Key	WEP	RC4	Static
	WPA-Personal	WPA Passphrase (also known as WPA PSK and WPA Preshared Key)	TKIP	RC4	Dynamic
	WPA-Enterprise	802.1X/EAP	TKIP	RC4	Dynamic
802.11-2007 (RSN)	WPA2-Personal	WPA2 Passphrase (also known as WPA2 PSK and WPA2 Pre-shared Key)	CCMP (mandatory) TKIP (optional)	AES (mandatory) RC4 (optional)	Dynamic
802.11-2007 (RSN)	WPA2-Enterprise	802.1X/EAP	CCMP (mandatory) TKIP (optional)	AES (mandatory) RC4 (optional)	Dynamic

Certified Wireless Network Administrator: CWNA – PW0-106 15

Robust Security Network (RSN)	
<ul style="list-style-type: none"> • 802.11-2012 defines an RSN <ul style="list-style-type: none"> – STAs must use the 4-way handshake – STAs must use CCMP or TKIP • Field known as the RSN Information Element (IE) may identify the cipher suite capabilities of each station • A transition security network (TSN) supports RSN-defined security, as well as legacy security such as WEP, within the same BSS, although most vendors do not support a TSN. 	



Certified Wireless Network Administrator: CWNA – PW0-106 16

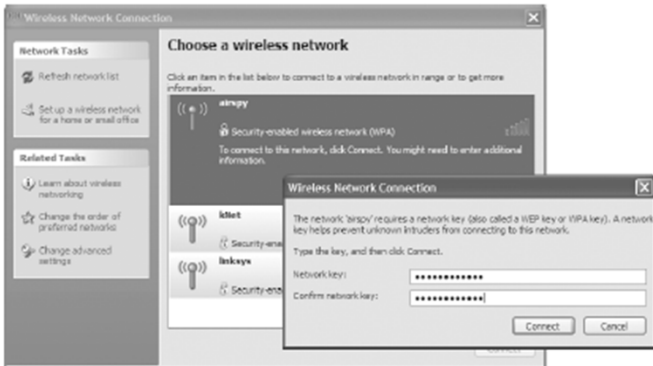
PSK Authentication

- Standard defines authentication and key management (AKM) services.
- An authentication and key management protocol (AKMP) can be either a preshared (PSK) or an EAP protocol used during 802.1X authentication
- WLAN vendors have many marketing names for PSK authentication, including WPA/WPA2-Passphrase, WPA/WPA2-PSK, and WPA/WPA2-Preshared Key.

Certified Wireless Network Administrator: CWNA – PW0-106
17

Client configured with static passphrase



The screenshot shows the Windows 'Wireless Network Connection' dialog box. The main window is titled 'Choose a wireless network' and lists several networks: 'hispq', 'hinet', and 'hiskays'. The 'hispq' network is selected and highlighted. A smaller dialog box is open over the 'hispq' network, titled 'Wireless Network Connection'. It contains the text: 'The network 'hispq' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network. Type the key, and then click Connect.' Below this text are two input fields: 'Network key:' and 'Confirm network key:', both containing masked characters (dots). There are 'Connect' and 'Cancel' buttons at the bottom of the dialog.

Certified Wireless Network Administrator: CWNA – PW0-106
18

SYBEX **WILEY**

Proprietary PSK Authentication

The diagram illustrates a wireless network setup for Proprietary PSK Authentication. On the left, three users are shown: User 1 (laptop), User 2 (laptop), and User 3 (mobile phone). Each user has a unique PSK and shares the same SSID, CWNA. On the right, a wireless router is shown with its configuration: SSID: CWNA, Authentication: WPA2-Personal, and three user-specific PSKs: User 1 - PSK: d6#S%^98f.., User 2 - PSK: 87fe@#S%a.., and User 3 - PSK: 90)356*&f.. Arrows point from the router to each user, indicating the authentication process.

User 1 SSID: CWNA
PSK : d6#S%^98f..

User 2 SSID: CWNA
PSK : 87fe@#S%a..

User 3 SSID: CWNA
PSK : 90)356*&f..

SSID: CWNA
Authentication: WPA2-Personal
User 1 - PSK : d6#S%^98f..
User 2 - PSK : 87fe@#S%a..
User 3 - PSK : 90)356*&f..

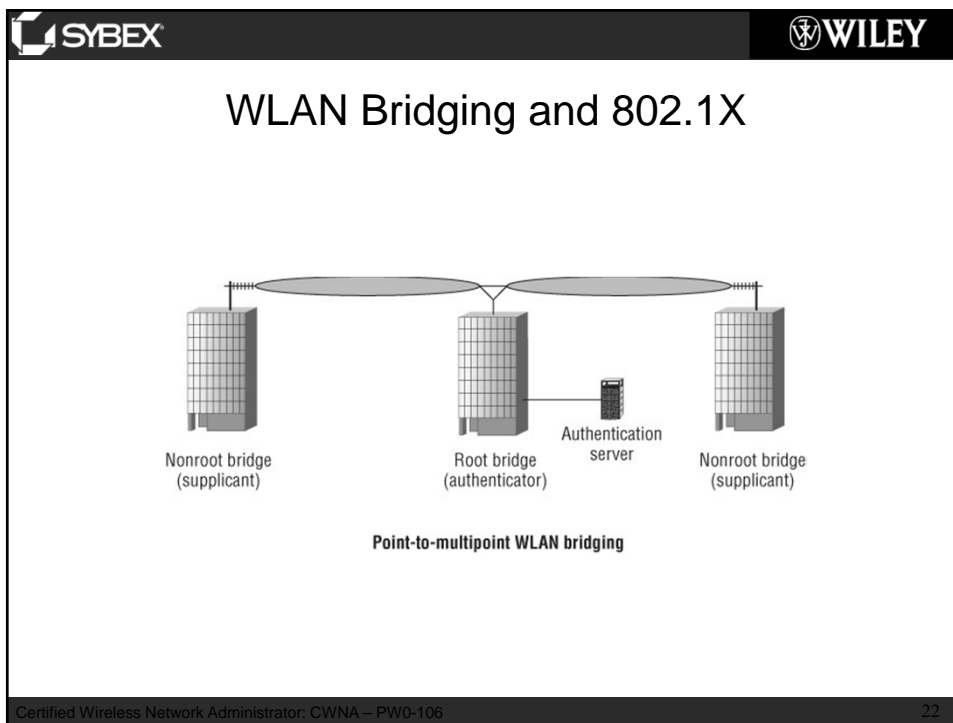
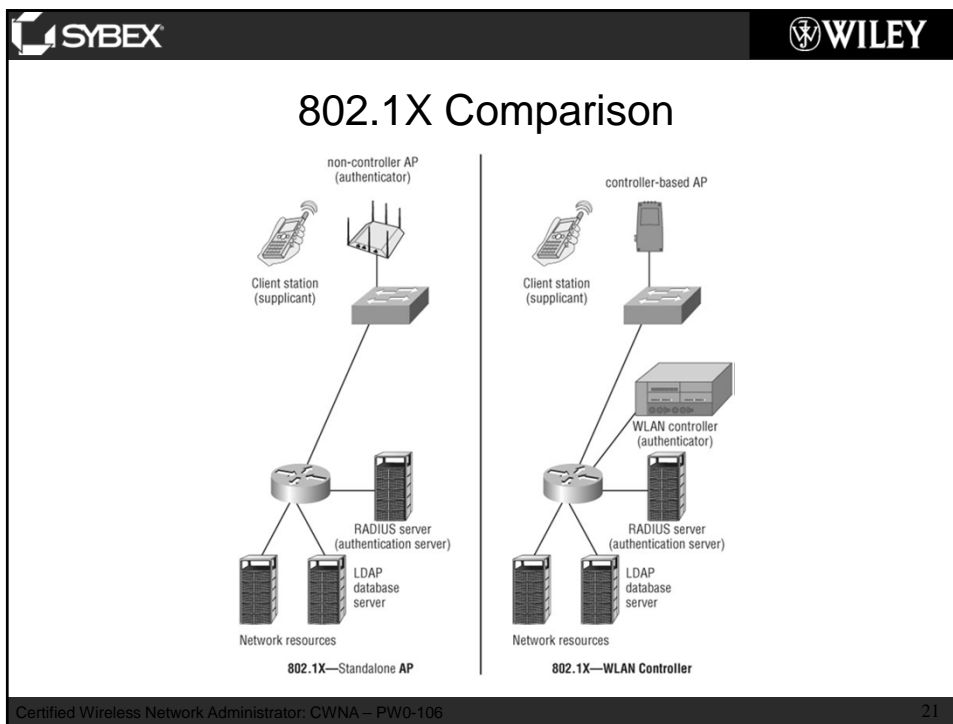
Certified Wireless Network Administrator: CWNA – PW0-106 19

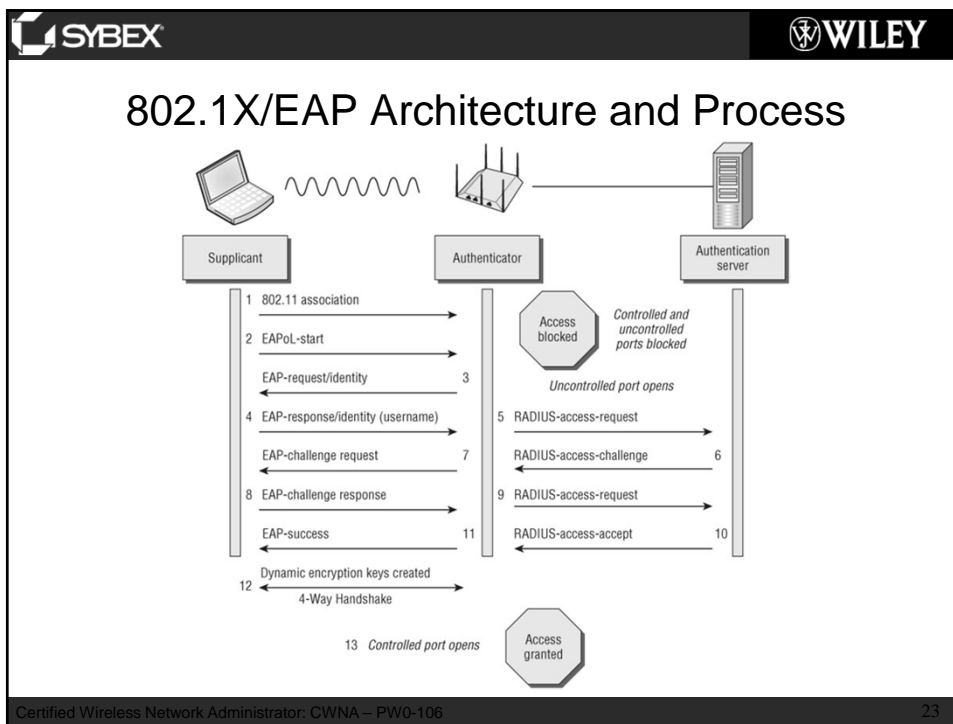
SYBEX **WILEY**

802.1X/EAP Framework

- Supplicant
- Authenticator
- Authentication Server (AS)

Certified Wireless Network Administrator: CWNA – PW0-106 20







EAP Types

TABLE 13.2 EAP comparison chart

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)	EAP-FAST
Security Solution	RFC-2284	Cisco proprietary	RFC-5216	RFC 5281	IETF draft	IETF draft	IETF draft	RFC 4851
Digital Certificates—Client	No	No	Yes	Optional	No	Yes	Optional	No
Digital Certificates—Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password Authentication	Yes	Yes	N/A	Yes	Yes	No	Yes	Yes
PACs—Client	No	No	No	No	No	No	No	Yes
PACs—Server	No	No	No	No	No	No	No	Yes
Credential Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption Key Management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Debatable	Yes	Yes	Yes	Yes	Yes	Yes
Tunnelled Authentication	No	No	Optional	Yes	Yes	Yes	Yes	Yes
Wi-Fi Alliance supported	No	No	Yes	Yes	Yes	No	Yes	Yes



Certified Wireless Network Administrator: CWNA – PW0-106 24



Dynamic Encryption-Key Generation

- EAP protocols that utilize mutual authentication provide “seeding material” that can be used to generate encryption keys dynamically
- Dynamic keys are generated per session per user



Certified Wireless Network Administrator, CWNA – PW0-106 25



4-Way Handshake

- Involves the creation of two master keys known as the Group Master Key (GMK) and the Pairwise Master Key (PMK)
- These master keys are the seeding material used to create the final dynamic keys that are used for encryption and decryption.
- Final encryption keys are known as the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK).



Certified Wireless Network Administrator, CWNA – PW0-106 26



WPA/WPA2-Personal

- Offers a simpler method of authentication using a PSK
- Matching passphrases on both the access point and all client stations
- Formula is run that converts the passphrase to a Pairwise Master Key (PMK) used with the 4-Way Handshake to create the final dynamic encryption keys



Certified Wireless Network Administrator: CWNA – PW0-106 27



TKIP Encryption

- An enhancement of WEP encryption
- Starts with a 128-bit temporal key that is combined with a 48-bit initialization vector (IV) and source and destination MAC addresses in a complicated process known as per-packet key mixing
- Uses a stronger data integrity check known as the message integrity check (MIC) to mitigate known bit-flipping attacks against WEP.



Certified Wireless Network Administrator: CWNA – PW0-106 28



CCMP Encryption

- Default encryption method defined under the 802.11i amendment
- Uses the Advanced Encryption Standard (AES) algorithm
- CCMP encryption keys are dynamically generated as a final result of the 4-Way Handshake.

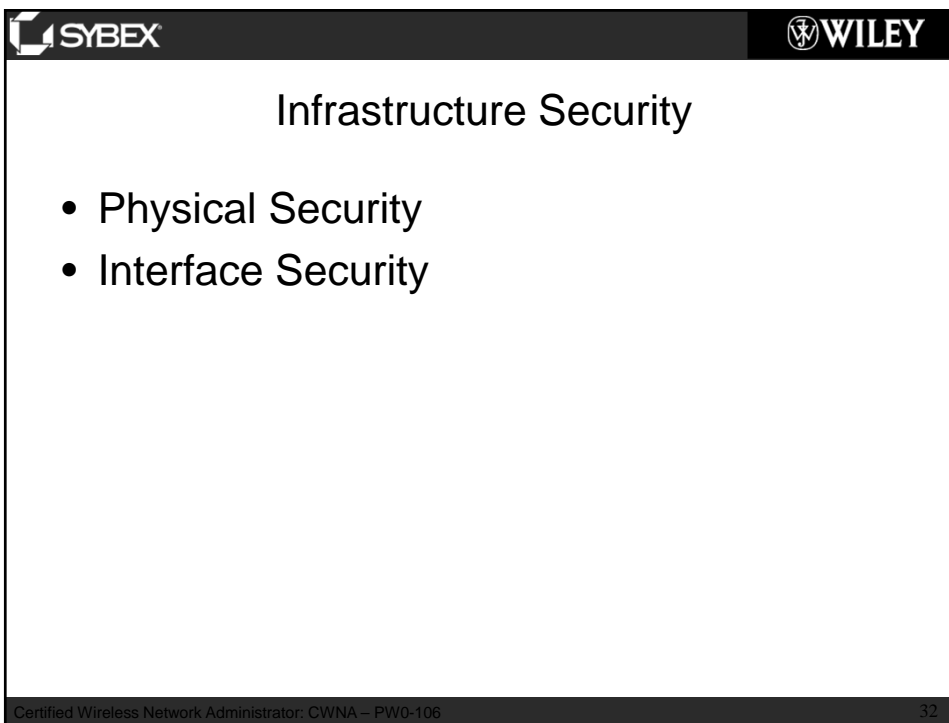
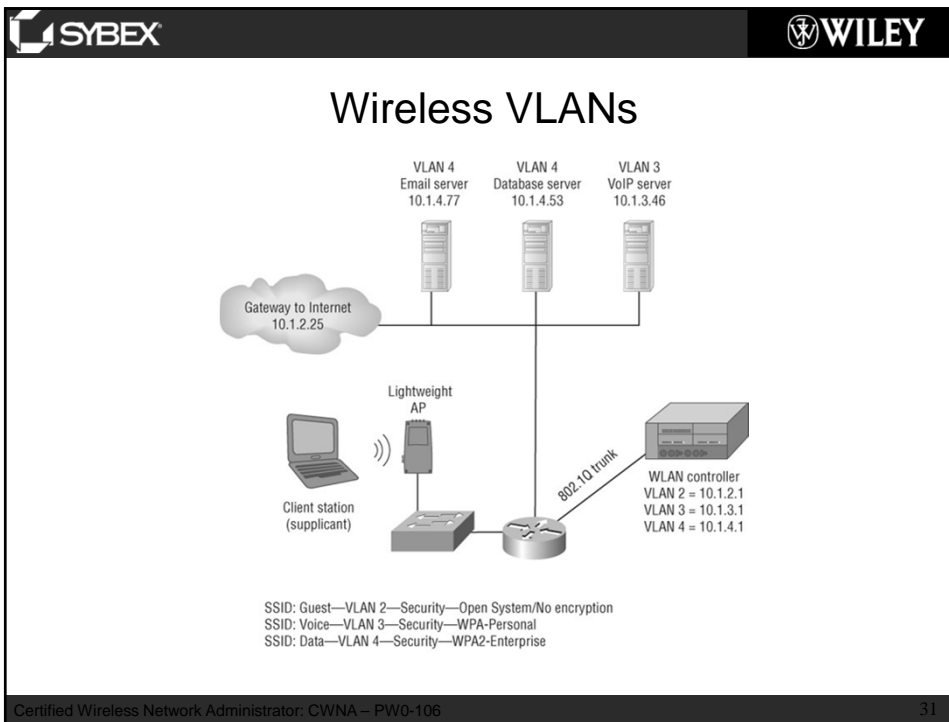
Certified Wireless Network Administrator: CWNA – PW0-106 29



Traffic Segmentation

- VLANs
 - Guest
 - Voice
 - Data
- RBAC

Certified Wireless Network Administrator: CWNA – PW0-106 30

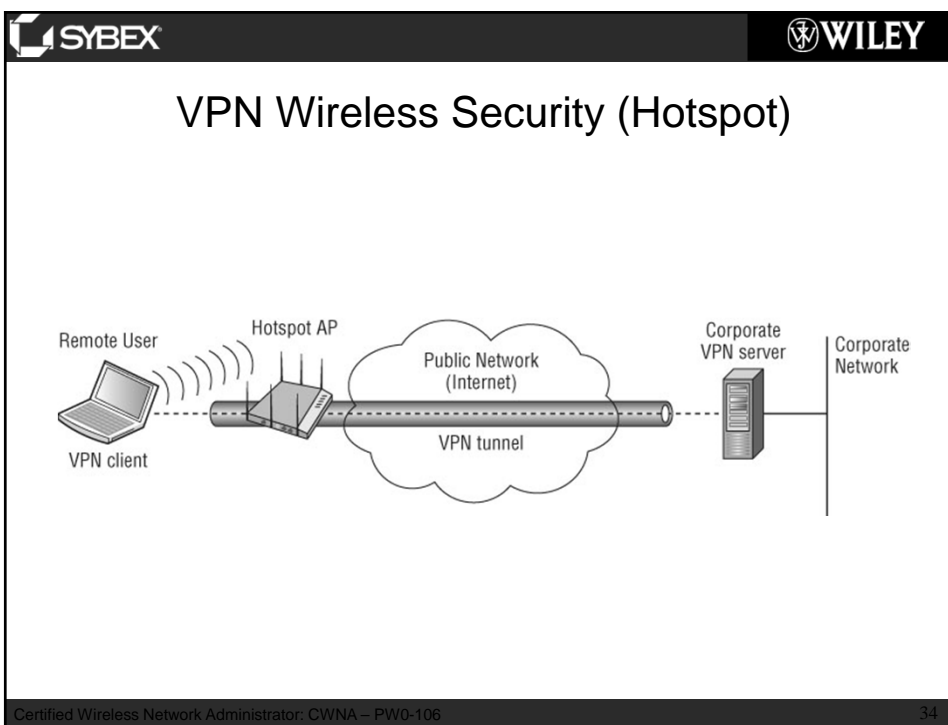


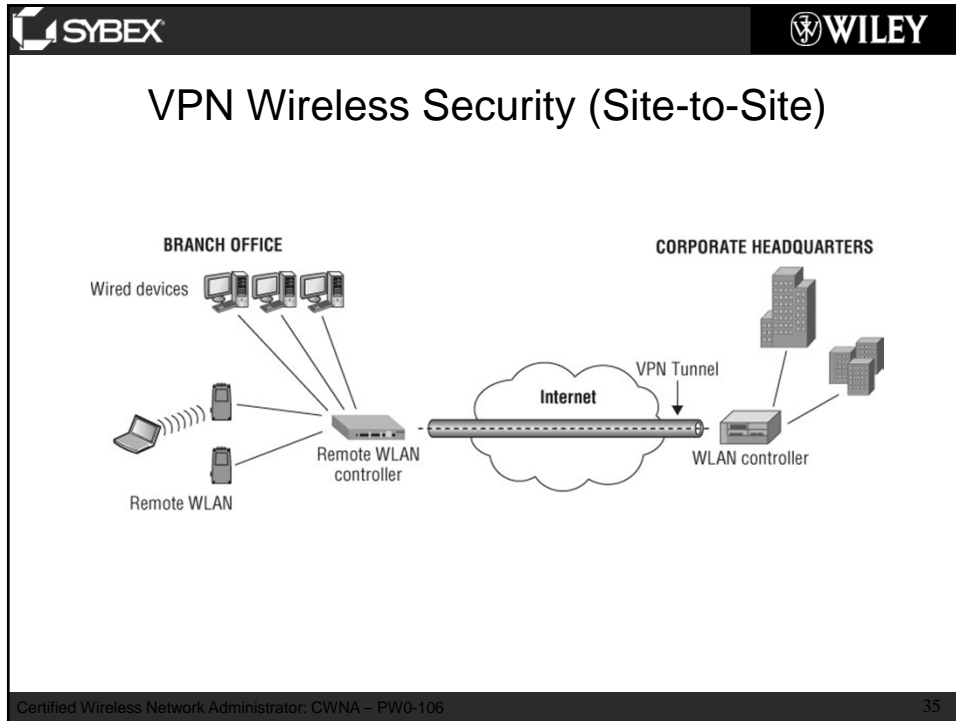
SYBEX **WILEY**

VPN Wireless Security

- Layer 3 VPNs
 - Most commonly used layer 3 VPN technology is Internet Protocol Security (IPsec).
- SSL VPN
 - Does not require the installation and configuration of client software on the end user's computer
 - User connects to a Secure Sockets Layer (SSL) VPN server via a web browser

Certified Wireless Network Administrator, CWNA – PW0-106 33





SYBEX **WILEY**

Logon section of captive web portals

Captive Web Portals > New

Save Cancel Export

Name* Captive_Portal (1-32 characters)

Registration Type User Authentication

Description Sybex Guest WLAN (0-64 characters)

Captive Web Portal Login Page Settings

Modify automatically-generated web pages Import custom web pages

Customize Login Page

Authentication Method CHAP

Captive Web Portal Success Page Settings

Captive Web Portal Failure Page Settings

Optional Advanced Configuration

Authenticated Network Access

User Name:

Password:

Submit

It may take up to 20 seconds for the registration process to complete.
Logging in includes you have read and accepted the Acceptable Use Policy

Certified Wireless Network Administrator, CWNA – PW0-106 37

SYBEX **WILEY**

Chapter 13 Summary

- 802.11 Security Basics
- Legacy 802.11 Security
- Robust Security
- Traffic Segmentation
- Infrastructure Security
- VPN Wireless Security

Certified Wireless Network Administrator, CWNA – PW0-106 38