Fortinet Wireless

Course #203

Course Overview

Through this 1-day training participants learn a comprehensive overview of the Fortinet Wireless solution and sufficient knowledge to provision wireless LANs based on this solution in the field. Students will become familiar with the core standards and technologies of the wireless solution. The student should have the level of FortiGate knowledge equivalent to that form attending the 301 course prior to attending this course.

The training consists of the following modules:

- Wireless technology essentials
- Wireless controller
- Device identification
- Advanced authentication
- Custom AP profiles
- Putting it all together

The knowledge gained from the training and labs is assessed in the wireless accreditation which is part of this course.

Course Objectives

At the conclusion of this course, a student should be able to:

- Explain at a high-level the various radio frequency fundamentals used in Wi-Fi technology
- Identify the 2.4 GHz and 5 GHz frequencies used in Wi-Fi technology
- Describe at a high-level the 802.11 Wireless LAN standards
- Describe the MIMO system
- Identify key WFA, IEEE and IETF standards
- Describe at a high-level CAPWAP and thin AP architecture and how they are used in wireless
- Describe wireless planning site survey best-practices and use FortiPlanner as a wireless planning tool
- Describe the fast roaming feature
- List the components and advantages of the FortiGate integrated wireless controller and the wireless solution
- Identify the key configuration requirements of an SSID
- Describe the purpose of the Virtual Access Point in the FortiOS configuration
- Describe the configuration of security and authentication settings for a wireless LAN
- Identify the purpose of MAC filtering
- Identify the managed AP topologies
- Identify the goals and describe the main phases of the CAPWAP protocol
- Describe the basic access point configuration settings for a simple wireless LAN deployment.

- Perform a wireless network deployment using equipment in a hands-on lab
- Identify the device Identification features of FortiOS and describe device identification techniques
- Describe how to apply device identification features to a VAP interface
- Configure to control access of wireless clients based on device type in a hands-on lab
- Identify wireless authentication methods and describe WPA2 Enterprise authentication
- Explain 802.1X and EAP standards and their usage in wireless networks
- Identify the capabilities of wireless Single Sign On (SSO)
- Describe the usage and configuration of the captive portal
- Describe the guest access capability
- Introduce FortiAuthenticator usage in the wireless solution
- Configure enterprise authentication using 802.1X in a hands-on lab
- Identify the requirement for custom AP profiles and the features that can be configured using custom profiles
- Describe rogue AP detection feature and the protection provided
- Describe wireless IDS techniques and protection provided
- Describe the usage of client load balancing mechanisms and the options available
- Perform a configuration to enable rouge AP detection in the hands-on lab
- Configure a full-mesh wireless network
- Configure WPA Enterprise authentication using FortiAuthenticator as the authentication server.