Cambium Networks™

ENTERPRISE WI-FI SOLUTIONS

cnPilot™ Security Overview

INTRODUCTION

Cambium Networks' cnPilot™ Enterprise WLAN access points and cnMaestro™ end-to-end Cloud-based or on-premises wireless network manager work together to deliver a secure, scalable Wi-Fi solution for enterprise, hospitality, education, and public Wi-Fi deployments – at an attractive price point. The solution paper explains multiple facets of and best practices for cnPilot security capabilities.

SECURING THE CONNECTION

cnMaestro is specialized to ensure reliable, secure management of all Cambium Networks products.
The data connection between cnPilot solutions and cnMaestro is secured using standard SSL (HTTPS) for privacy and authentication. The cnPilot APs validate the certificate from cnMaestro to ensure protection from spoofing attacks.

All connections are initiated from the APs towards cnMaestro over standard Web ports and protocols, ensuring seamless connectivity without the need to modify firewalls to open ports.

During onboarding to a cnMaestro account, the cnPilot APs will either use a Cambium ID and password that has been configured by the administrator, or present a partly randomized serial number that works to prevent brute-force serial number attacks.

- Secure Cloud-based device onboarding
- Secure tunneling – SSL (HTTPS)
- Individual AP level admin protection
- ACL – MAC blacklist
- URL – blacklist and whitelist
- RADIUS-based user authentication

Cambium Networks support and engineering staff provide backend automated monitoring. Beyond the architectural security measures, Cambium Networks' physical data centers are under 24x7 video surveillance with UPS power supply and multi-zoned to ensure continuous service in the event that any one center experiences technical difficulties.

AP SECURITY

Securing configuration and firmware The access point stores sensitive information such as configuration files containing passwords, shared RADIUS secrets, etc – all of which are encrypted in the AP's configuration file. This encryption ensures that anyone other than the administrator who might view the configuration overview, or who is given temporary access to the system, will not be able to view these sensitive parameters to gain unauthorized access to data.

The access point firmware is signed using a Cambium Networks certificate and when the firmware on the device is to be updated, the signature of the new image is validated. This prevents malicious firmware to be loaded onto APs.

The configuration interfaces of the AP (CLI and GUI) have been hardened, with careful scrutiny and sanitization of all inputs to prevent malicious attacks.

Securing Administrative interfaces cnPilot access points support secure interfaces for configuration and monitoring including HTTPS for the GUI, SSH for the CLI, and V3 for SNMP. While more traditional interfaces such as Telnet and SNMP v1 are available if desired, these can be disabled and the device can be set up to be managed only over secure connections that provide data privacy and confidentiality.

- Secure SSIDs: WPA/WPA2 security with AES-CCM encryption
- Built-in basic firewall
- Automatic encryption of stored passwords and sensitive data
- Cambium Networks certificate signed AP firmware

CLIENT SECURITY

Securing User Traffic The access point bridges traffic from wireless clients to the wired network, and there are multiple stages along this path where security is important. Traffic over the air can be intercepted by packet capture tools run by users in the vicinity of the network, but that can be prevented by configuring the WLAN with WPA2 security, which uses AES-CCM based encryption. Per-session encryption keys are derived between the AP and the wireless client, based on either pre-share security keys (WPA2-Pre-Shared) or RADIUS/802.1x authentication (WPA2-Enterprise). This will encrypt all traffic on the air, both to and from the AP.

The use of WPA2 is recommended, but WPA2-Enterprise is preferred because it provides strong mutual authentication in addition to encryption.

cnPilot access points also support the IEEE 802.11w standard, which specifies mechanisms to protect management frames. While WPA2 encryption provides privacy and authentication for data traffic, it still leaves the client connection susceptible to attacks that can cause disconnects and denials of service. 802.11w protects connections between cnPilot access points and clients supporting this standard.

- Per session encryption keys: (WPA2-pre-shared) or RADIUS/802.1x auth
- MAC based access control lists (ACLs)
- Wired network traffic controls by IP address, port numbers, and subnets

cnPilot APs also support MAC based access control lists, which can be configured on the access point or maintained centrally on a RADIUS server and allow the AP to scan the server for access permission per device. Though MAC addresses can be spoofed, when used in conjunction with WPA2, MAC authentication can provide an additional layer of security.

Securing access to wired network In addition to securing traffic, it is also important to ensure that traffic is bridged out appropriately to the wired side. On cnPilot APs, this includes the mapping of VLAN to each WLAN, and user traffic is only bridged out to the appropriate VLAN. This ensures separation of traffic on both wired and wireless sides, allowing use of guest and corporate networks together on the same AP.

In addition, access to/from the wired network can also be controlled using access control lists, which are per-SSID lists of IP addresses, port numbers, and subnets that the administrator can configure. The AP will then only allow traffic that matches these rules. One example of ACL management is to allow access only for web browsing (TCP ports 80, 443) while blocking other services such as SMTP.

cnPilot enterprise APs also include a firewall that provides protection from some basic network denial of service attacks from malformed or spoofed packets.