PELICAN

NETWORK SECURITY BRIEF

Security, intelligent by design.

Customer protection is paramount at Pelican Wireless. The solution is by all accounts a fundamental approach to Internet security; start with a design that eliminates risk.

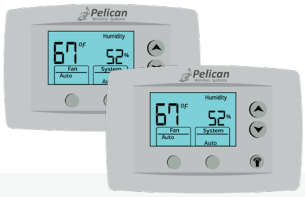
By utilizing advanced mesh network technology (not WiFi) Pelican is able to keep thermostat communication separate from your business network. So, no cross communication is even possible. And with only a single Pelican Gateway per site, your IT department can retain the integrity of your business network, without requiring any complex or unique configurations.

PELICAN MANAGED SERVERS

Each Pelican installation gets assigned a specific cloud server for its data. All Pelican cloud servers are maintained, updated and managed for free by Pelican.

PELICAN GATEWAY

Each Pelican site gets a gateway (GW400). No live data is stored at the gateway. The gateway is tasked with forwarding messages between the Pelican servers and the thermostats. The gateway has a standard Ethernet connector and uses TCP/IP messaging to communicate across the Internet to the Pelican server.



PELICAN THERMOSTATS

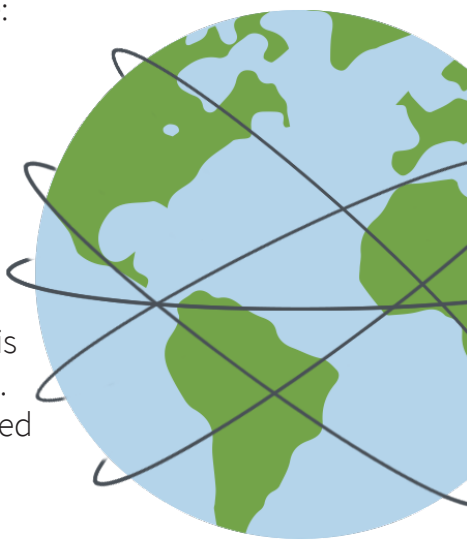
Pelican thermostats wirelessly communicate between each other and the Pelican gateway. Communication is over Pelican's encrypted wireless mesh network technology. Thermostats do NOT require IP addresses or WiFi connections.

Internet communication

Each installation site is assigned a specific server for its data. From time-to-time, site databases are migrated from one server to another to allow us to manage load and keep performance high.

Each site is assigned a unique domain name (i.e., MyFacilityName.OfficeClimateControl.net). The specific DNS/IP destination that the Gateway uses will match the IP address of the unique domain.

The Pelican Wireless Gateway establishes a single TCP/IP connection over its Ethernet port to it's designated Pelican Server. The Gateway can be configured to obtain it's initial IP settings using DHCP (default) or using a static configuration. At a minimum it requires a local IP address, a netmask, and a gateway address. Once it has a valid local IP address the Gateway will establish outbound connections using three ports. They are:



UDP/514 – This port is for diagnostic and troubleshooting information.

TCP/9742 – This port will be used from time to time to verify which Pelican
Server it should use for it's primary data connection.

TCP/9800-11000 – Each site will be assigned a single outbound port in this range for connections to the primary server. This is dynamically assigned. However, upon request, Pelican Technical Support can assign a single fixed port to be used by the Gateway.

The Gateway does not require any Firewall inbound connections and can be placed outside of the customer's Firewall on an isolated network since it's only communication is out to the Internet servers. The Gateway uses Advanced Encryption Standard (AES) to maintain a secure connection with the Pelican Servers. The Gateway maintains constant connectivity. This allows for real time communications to the Pelican thermostats.

Wireless communication

Pelican utilizes the IEEE 802.15.4 wireless standard seen in the diagram on the next page. This standard was designed to be compatible and coexist with the WiFi standard IEEE 802.11. Because of the design, they can coexist in the same frequency channels; however, the IEEE 802.15.4 standard allows for two extra narrow channels which are not utilized by WiFi due to potential WiFi crossover. Pelican's products are capable of operating in any of the defined channels, but by default they operate in channel 26 (2.480 MHZ) which means that Pelican is completely unnoticed and has no effect in environments where there is WiFi installed.

Wireless Spectrum Comparison