Firetide mesh provides reliable and secure connectivity critical for bandwidth intensive applications and wireless networks. Firetide mesh uses proprietary protocols to communicate between the Firetide HotPort mesh nodes. This protocol is insusceptible to other Wi-Fi enabled devices. Hence, any device (including laptops, smartphones, tablets, and similar Wi-Fi devices) other than the Firetide HotPort mesh node cannot connect or communicate directly to the Mesh.

Moreover, Firetide mesh provides advanced security, including:

- Dual-layer of FIPS140-2 certifiable End-to-End 256-bit AES encryption
- Digitally signed firmware files – To stop any unauthorized firmware installation on nodes.

Figure A: Firetide Mesh does not allow access to any device to connect directly to the mesh network.
VLAN based access control lists

2. **Advanced Encryption Standard (AES)** is a widely adopted data encryption standard and is significant because the United States government has approved it. AES is already the choice of many commercial and government organizations internationally. There are many areas where AES is now in commercial use such as high-end VPN software from Checkpoint, Cisco, and Symantec. AES is also found in network appliances, VoIP services, to provide security for process control (SCADA) systems and hardware implementations that use both FPGAs and ASICs. *Firetide mesh* deploys the highest available 256 bits key size for the AES encryption.

3. **End-to-End Security**

256 bits key size for the AES encryption coupled with the End-to-End packet transmission provides a more secured solution. The benefit delivered by this End-to-End transmission is that it eliminates the need to open up packets into L3 between hops. Consequently, there is no need to check the IP address and route it at every hop. This eliminates any potential chances of sniffing data packets over hop making the whole process tightly secure and faster.

![Diagram showing data packets](image-url)
4. **Firetide issued certificate on nodes**

The HotView Pro network management system communicates, and shares network configuration only with nodes having authorized Firetide issued certificates. This blocks any rogue node to spoof as a Mesh node to join the network.

5. **Physical intrusion and Unknown nodes**

Firetide mesh deploys MAC based access control list. It also provides an option to block the ports completely on need-basis. Even though no unauthorized device can access the Firetide mesh network as explained in the features above, in order to detect any rogue node that is attempting to access the mesh network - the “High security” feature can be enabled. Once enabled, this secured mode creates a warning message for any new node that is discovered in the vicinity of the mesh network, thereby alerting the user.