Meetinghouse Firewall Overview

READ

- Print

Last Updated: 23 September 2019 at 11:38

The meetinghouse firewall is the most important component for secure, filtered meetinghouse internet. The firewall blocks malicious users on the internet from accessing meetinghouse computers. It also prevents users from accessing inappropriate sites on the internet. Church policy states that meetinghouse internet must be filtered through an **approved meetinghouse firewall**.
Facilities management groups are responsible for ordering and installing meetinghouse firewalls correctly. Installation may be delegated to technology specialists.

Technology specialists are responsible for making sure that the meetinghouse firewall remains in place, remains properly configured, and does not get bypassed. It is recommended that firewalls be checked at least quarterly.

Proper firewall function can be checked by following the steps on the "Meetinghouse Internet Filter Check" article.
Back to Top

Meetinghouse Firewall Features

The Meraki MX64 is the only approved firewall for meetinghouses worldwide. Any other firewall deployed in meetinghouses should be replaced with the Meraki. Available features associated with this firewall include:

Network Features:

1. Simplified **self-activation** through Technology Manager (tm.ChurchofJesusChrist.org).
2. **Facilities zone** for internet-enabled appliances (click here for details).
3. **Special-purpose zone** for family history centers and other non-meetinghouse applications.
4. Church-approved **internet content filtering**.
5. Advanced **troubleshooting resources and tools** for the Global Service Center.
6. Improved **network management and reporting tools**.

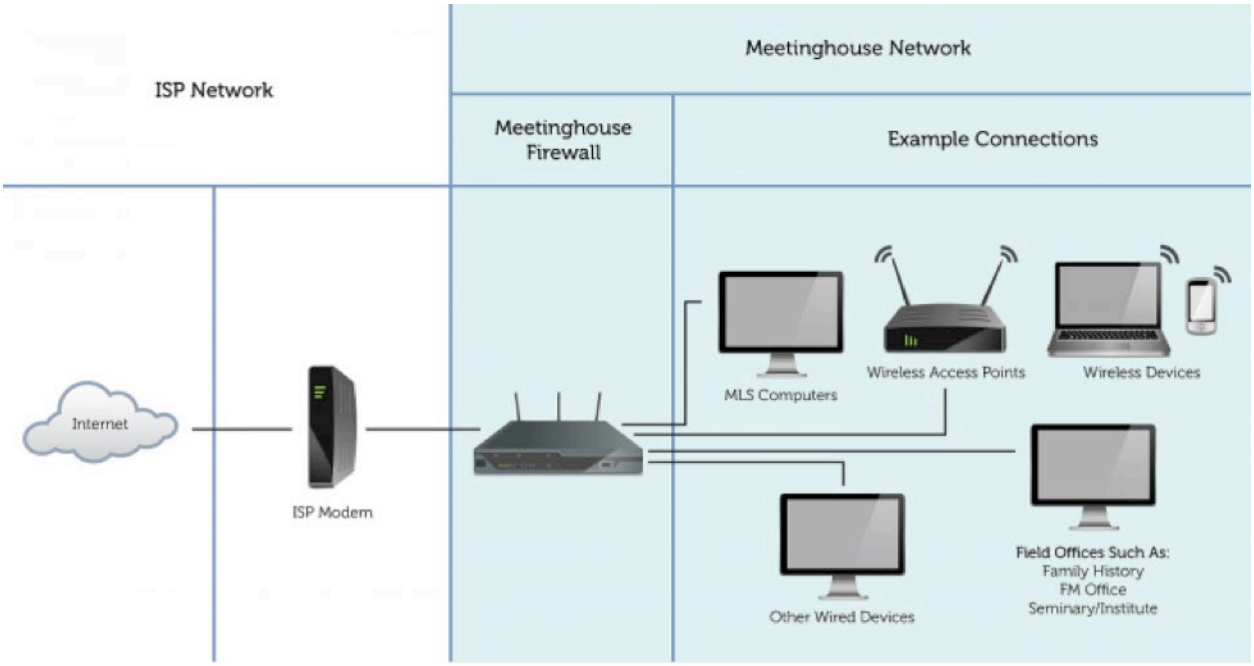
Meraki MX64 Hardware Features:

1. **Gigabit** ethernet LAN interfaces.
2. **Increased** maximum internet throughput up to 250 Mbps.
3. **Cellular** USB WAN interface.

Note: The standard meetinghouse firewall should not be installed in PCI-compliant locations where credit cards are used.

Placement of the Meetinghouse Firewall

The meetinghouse firewall must be situated between the internet service provider (ISP) modem and all devices on the meetinghouse network. No device other than the meetinghouse firewall should ever connect directly to the ISP modem. Wireless capabilities on ISP modems must be disabled.



Facilities managers make the final decisions regarding placement of meetinghouse firewalls. The following should be considered in determining where to place the firewall:

- **Secure Location:** Firewalls and ISP modems should be placed in secure areas that do not get a lot of traffic. Avoid locations where people have easy access to bypass the firewall. Attics, drop ceilings, and lockable closets are preferred (unless the attic gets too hot).

- **Good Operating Environment:** Avoid locations that restrict airflow or that reach temperatures outside of the operating range of the firewall (32°F to 104°F / 0°C to 40°C).

- **Port Accessibility:** The ports and the status lights on the ISP modem and the firewall should be easy to access and view so the stake technology specialist and facilities management group can troubleshoot problems and verify connections.

- **Close to ISP:** The meetinghouse firewall is usually placed near the ISP termination point (the demarcation point) and where the network is distributed to the rest of the building. The meetinghouse firewall can be placed on a shelf or surface-mounted to a wall or ceiling.

Firewall Configuration before a Meraki Switch is installed

The Meraki MX64 firewall has five network ports on the back of the device. Each port is configured as follows:

- **Ports 1, 2, and 3*—Public Zone:** These ports provide "public" internet access. Examples of devices that should be connected to these ports include clerk or MLS PCs, ward or stake printers, webcast equipment, and wireless access points.
- **Port 4—FAC Zone:** This port is reserved for internet-enabled appliances and should not be used for any other purpose. Only the facilities manager should connect devices to this port. This port should not have any public devices connected to it.

- **Internet Port:** The cable coming out of the ISP modem should go directly into this port.

Firewall Configuration after the Meraki Switch is installed

The Meraki MX64 firewall has five network ports on the back of the device. Each port is configured as follows:

- **Port 1 -** Connects to SFP9 on a Meraki 8 Port switch, SFP25 on a Meraki 24 Port Switch, and SPF49 on a Meraki 48 Port switch.
- **Port 2 -** Public Zone: This port provides "public" internet access. This port should only be used to access TM during the switch installation. This port will be empty after the Meraki switch is installed.
- **Ports 3 and 4 -** These ports will be disabled and empty after the Meraki Switch is installed.
- **Internet Port:** The cable coming out of the ISP modem should go directly into this port.

Back to Top

Extending Meetinghouse Internet

Once a meetinghouse has internet service and a firewall, the challenge becomes extending internet access to the rest of the building. “Networking Overview” for the meetinghouse includes information on doing this.

Back to Top