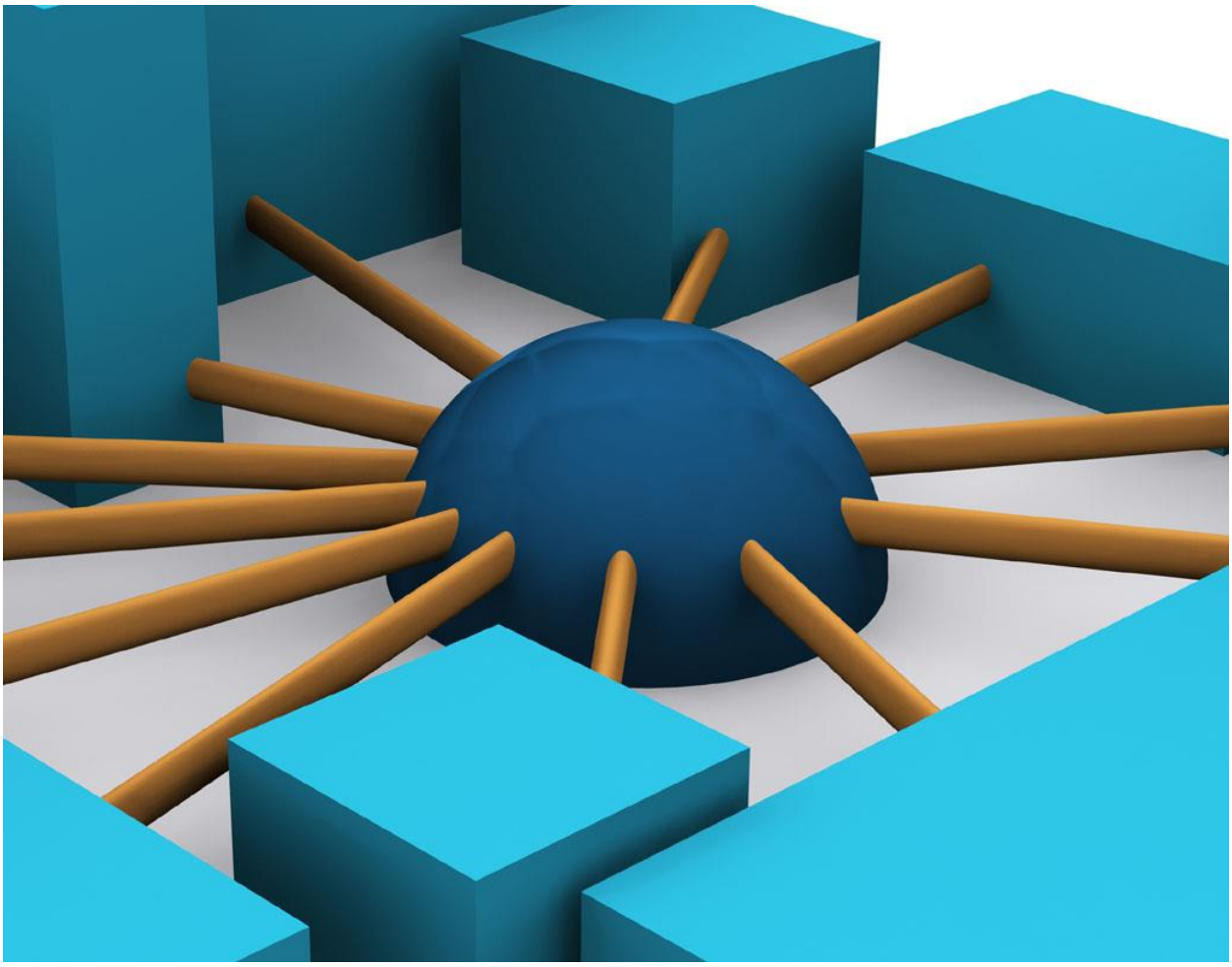
BACnet Secure Connect

A Secure Infrastructure for Building Automation

David Fisher
Bernhard Isler
Michael Osborne
SSPC 135 IT Working Group



Contents

Disclaimer

The information contained in this document represents the current view of the ASHRAE SSPC-135 IT Working Group (IT-WG) regarding the issues discussed as of the date of publication. Because BACnet is under continuous maintenance, this document should not be interpreted as a commitment on the part of ASHRAE or the SSPC-135. The IT-WG cannot guarantee the accuracy of any information presented after the date of publication.

ASHRAE MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Executive Summary

BACnet, an international standard, has been in widespread use in building automation (BA) systems since its publication in 1995. Decades of use, and deployment of more than 25 million devices worldwide, has generated a wealth of knowledge about the benefits and issues related this technology. During this period, information technology (IT) professionals have had increasing exposure to BACnet. The confluence of accepted best practices in the IT world and in BACnet has exposed opportunities for improvement. To this end, SSPC-135 IT-WG has worked over the past five years to define new mechanisms for BACnet that mesh more naturally with evolving IT best practices.

A key concern among all parties is network and information security and infrastructure integrity. With a sharply increasing interest in cloud-based applications, owners, managers, BA, and IT professionals have a strong desire to create BA infrastructures that provide very high levels of security. At the same time, on the IT side there is a mature set of best practices for implementing and managing secure communications infrastructure. Previous attempts by BACnet to address these concerns went in a different direction than the IT community, ultimately frustrating efforts to gain acceptance.

Recognizing these concerns, the IT-WG has developed a new proposal centered on secure communications exclusively using accepted IT best practices. The new technology is called “BACnet Secure Connect (BACnet/SC)” and is the subject of this white paper. Simply put, BACnet/SC provides the means to create secure communications connections between BA devices both across the cloud, and within facilities. BACnet/SC uses the latest techniques for security and integrates easily with IT infrastructure. At the same time, BACnet/SC preserves 100% of the capabilities and is backward-compatible with all existing BACnet deployments and devices. Aligning BACnet/SC with existing IT standards and best practices allows your organization to create very secure BA infrastructure and unlock new cloud-based applications. It will also future-proof your organization's investment in BA as new security innovations become available.

Introduction

BACnet today provides all the capabilities to interconnect BACnet devices within a BA system, including:

- Widespread interoperability among over 1000 vendors
- Support for multiple application domains including HVAC, lighting, access control, elevators, and more
- Backwards compatibility between older and newer versions of BACnet
- System scalability from low-cost devices to advanced devices and workstations
- An open and free-to-use standard that continues to evolve to meet the changing needs of BA systems

BA systems are becoming increasingly more sophisticated and often need to be integrated with other IT infrastructures. Owners are demanding more information about building operations and costs, resulting in Facility Managers tasking the BA system to provide more data more often from more devices on the network. IT departments, already burdened with regular IT infrastructure work, have little capacity to learn and manage BA systems that have nonstandard requirements.

BACnet Secure Connect (BACnet/SC) provides BA infrastructure that uses standard internet protocol and standard, widely used security methods, eliminating much of the concern and work for an IT department. Because BACnet/SC is capable of traversing the entire network, it provides the Facility Manager with a secure and efficient path to obtain the data the Owner needs.

Why is BACnet/SC needed? In simple terms, there are some aspects of existing BACnet systems that are sometimes problematic because they deviate from common IT policies and practices, although these vary from one situation to another. From an IT perspective, BACnet/SC solves many common problems:

- BACnet/SC provides a sophisticated network security solution that uses standards widely accepted by the IT community.
- BACnet/SC eliminates the need for static IP addresses, reducing the burden on IT groups, and may decrease lease costs to users.
- BACnet/SC is not dependent on broadcast messaging.
- BACnet/SC eliminates BACnet/IP Broadcast Management Devices (BBMDs) and their configuration and is tolerant of changes in network topology.
- BACnet/SC works easily with firewall devices that are common in IT infrastructure.

BACnet Secure Connect

BACnet/SC is a new BACnet datalink that eliminates many of the concerns Owners, Facility Managers, and IT professionals have with BACnet today. It is based on standard TLS 1.2 security with options for 128-bit and 256-bit elliptic curve cryptography. It eliminates the need for static IP addresses and network broadcasts. It simplifies configuration by eliminating BBMD devices along with the need to keep them configured to match the network topology.

The BACnet/SC proposal extends beyond these key features to support other capabilities, including:

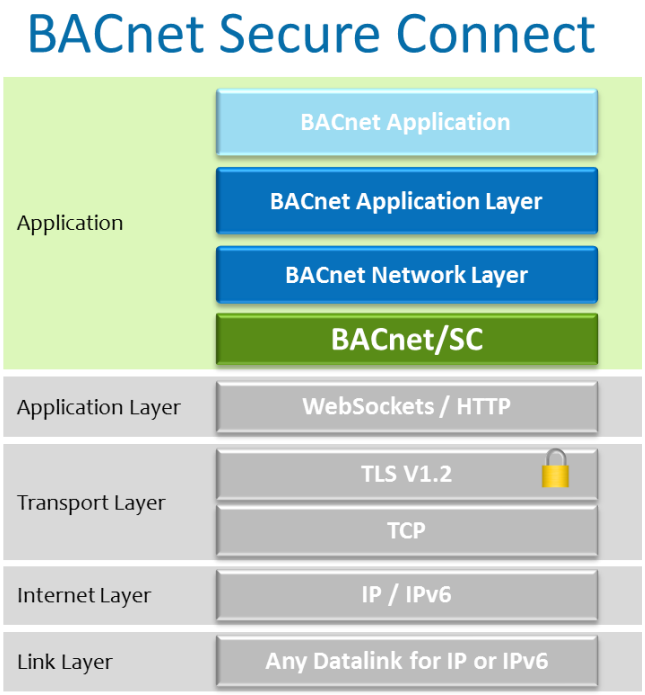
- Using shared IP networks with no virtual private network (VPN) setup required
- Allowing seamless traversal of simple-to-complex and local-to-global IP network configurations without compromising the existing security mechanisms, such as firewalls and supporting NATs
- Provides secure message transport using the standard IP application protocol, Secure WebSockets, which is an extension to HTTPS and runs over Transport Layer Security (TLS)
- Allowing communications independent of the network's configuration, including IPv4, IPv6, WiFi, and cellular
- Full compatibility with all existing BACnet systems and devices through normal BACnet routing

BACnet/SC provides a secure mechanism to allow a device to be authenticated and authorized to use the network.

BACnet Secure Connect
Virtual Datalink

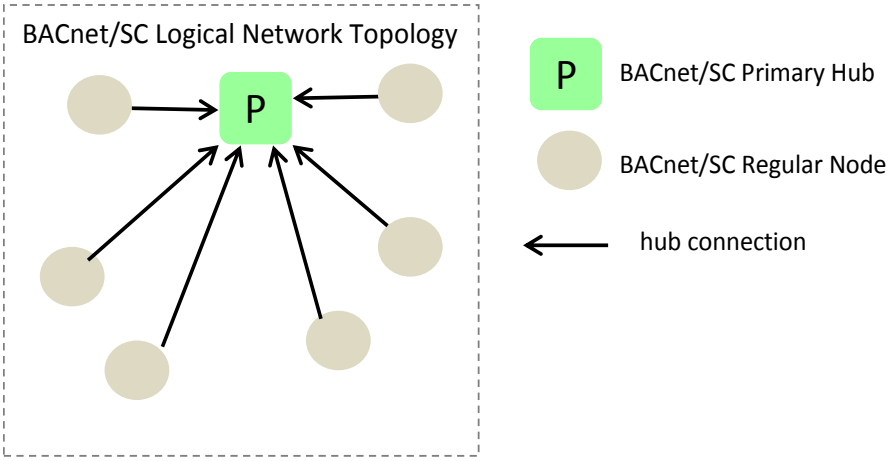
IP Centric View:

- All of BACnet is an "Application", including the BACnet/SC BACnet Datalink
- WebSockets are the "Application Layer"
- TLS & TCP build the "Transport Layer"
- IP or IPv6 is the "Internet Layer"
- At "Link Layer", any datalink technology possible that supports IP or IPv6: Ethernet, WLAN, 4G/5G, ...

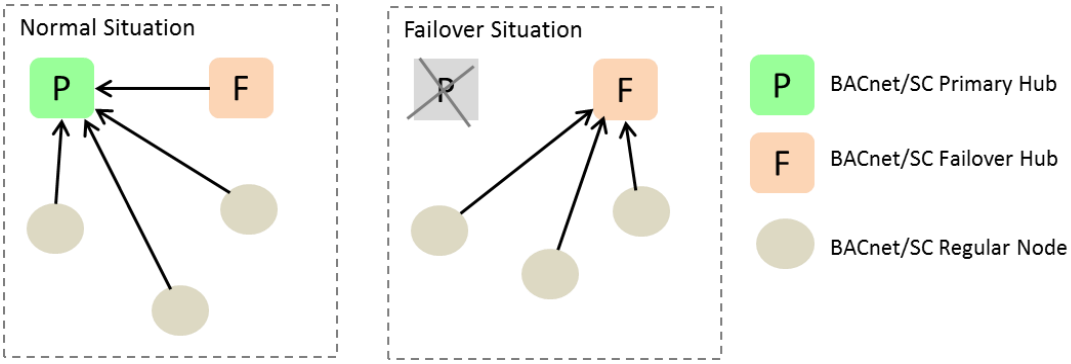


Topology

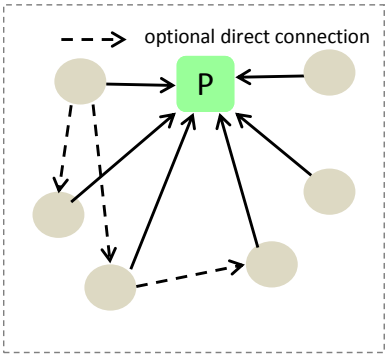
BACnet/SC uses a hub-and-spoke topology where a single central hub device directs traffic between any number of node devices. The hub analyses the traffic to determine whether it should be directed to another node or forwarded to all connected nodes. A node can be a simple device, such as a thermostat, or a more sophisticated device that routes to an existing BACnet system, or it could be the main workstation for the entire facility.



Because a hub is single point of failure, BACnet/SC includes a detailed failover mechanism to ensure the system remains viable if the hub fails or is taken offline for maintenance or upgrade. All BACnet/SC nodes are mandated to support reconnecting to the BACnet/SC failover hub.



Regular nodes have the option of performing direct connections to other regular nodes in addition to going through a hub.



Implementation Scenarios

There are many ways BACnet/SC could be deployed. Below are a few of the possible scenarios.

Scenario #1

A building with an existing BACnet system where the Facilities Manager needs to access the system remotely across the public Internet and cannot allow inbound connections through the building network's firewall

In this case, a single BACnet/SC node that includes a BACnet router for routing to the legacy BACnet system is added to the building, a cloud-based BACnet/SC hub is deployed, and BACnet/SC node workstation software is used. The building BACnet/SC node initiates a connection to the BACnet/SC hub in the cloud, and because the building node is initiating the connection from inside the building, no specific configuration is required in the building's firewall except for outbound HTTPS connections, which are typically already enabled. The facility manager uses the workstation software to initiate a connection to the hub in the cloud, and, once connected, is able to manage the building's system.

New Equipment

- BACnet router that supports BACnet/SC
- BACnet/SC hub ("P" in Figure 1) outside of the facility
- (Optional) BACnet/SC failover hub ("F" in Figure 1) also outside of the facility
- BACnet operator workstation that supports BACnet/SC

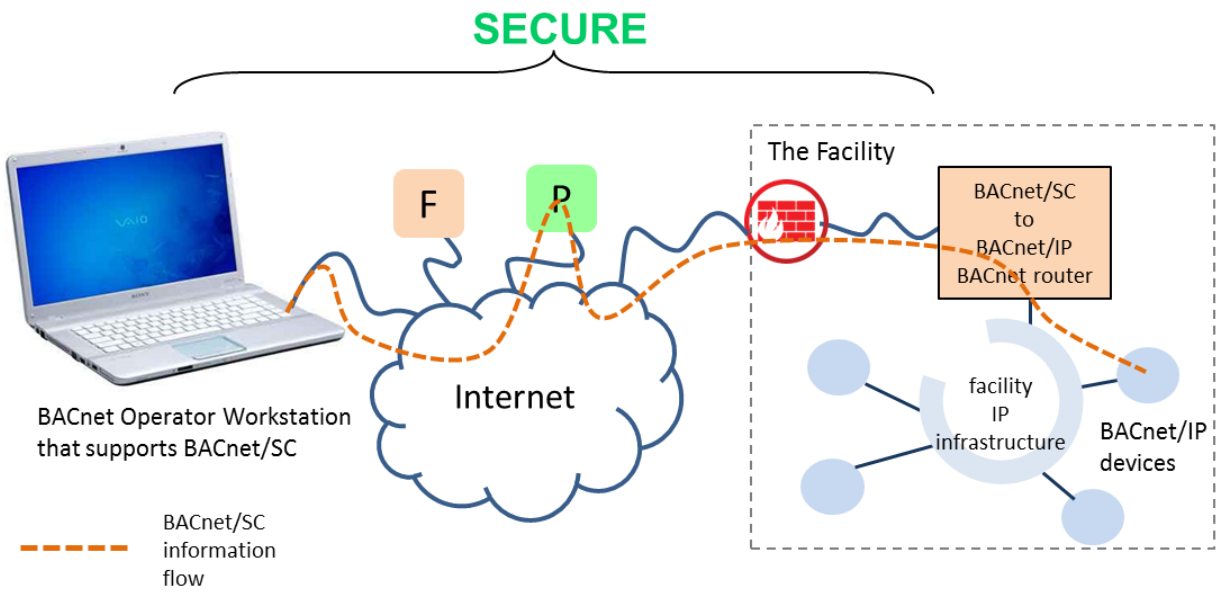


Figure 1: Secure Access from Outside the Facility

Scenario #2

A new building where IT policies do not allow unsecured BACnet traffic on a shared IP network

In this case, all IP-based BACnet devices will need to support BACnet/SC. A BACnet/SC hub and failover hub will need to be installed as part of the network.

New Equipment

- BACnet devices that support BACnet/SC
- BACnet/SC hub ("P" in Figure 2)
- BACnet/SC failover hub ("F" in Figure 2)
- BACnet operator workstation that supports BACnet/SC

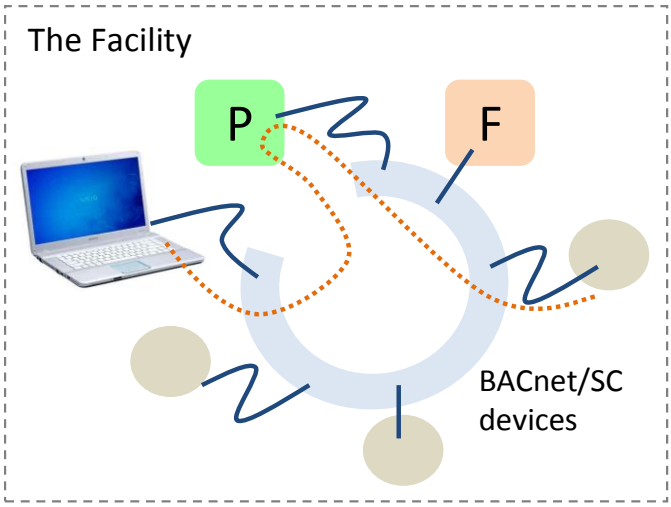


Figure 2: Secure Access within the Facility

Scenario #3

A building using mixed secure and insecure/legacy devices

In this example the primary and failover hubs are *inside* the firewall and are used to secure BACnet/SC devices within the facility. A BACnet/SC-to-BACnet/IP router is included to allow connectivity between the BACnet/SC secure network and legacy BACnet networks. Although a traditional BACnet/IP-to-MS/TP router could be used, the example also shows a BACnet/SC-to-MS/TP router that extends secure access to the edge of a given MS/TP trunk. Note that this does *not* secure the MS/TP trunk itself from actors with physical access to the trunk but *does* secure the trunk against outside access from the IP infrastructure and from the Internet. In this example, outside (remote) access is provided by enabling the firewall to forward the BACnet/SC port using a public static IP address.

New Equipment

- BACnet devices that support BACnet/SC
- BACnet/SC hub (“P” in Figure 3)
- (Optional) BACnet/SC failover hub (“F” in Figure 3)
- BACnet/SC to BACnet/IP and/or MS/TP router(s) for legacy connections
- BACnet operator workstation that supports BACnet/SC

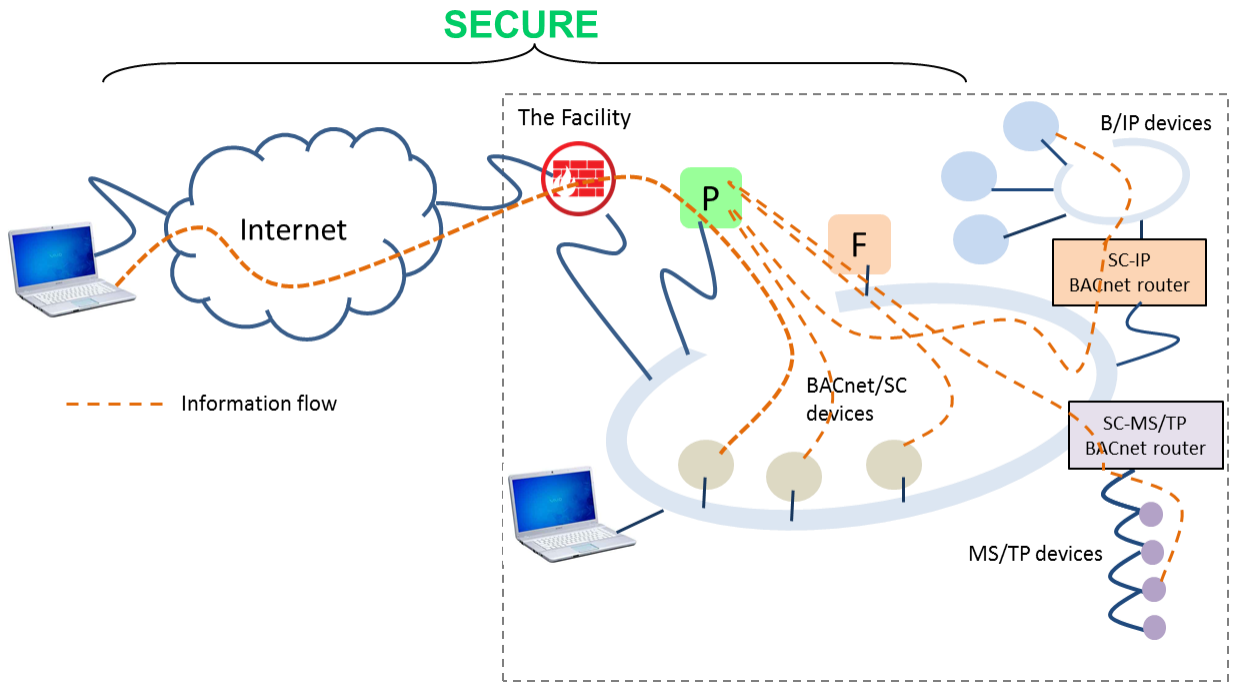


Figure 3: Mixed Scenario—Secure Access Outside and within the Facility with Isolated Areas

Scenario #4

A regional chain of big-box stores managed from a regional management center with connectivity via public Internet or WAN

In this example the primary and failover hubs are located in the cloud, and each store has its own collection of BACnet/SC devices or a BACnet/SC-to-some other BACnet router. The diagram shows an SC-to-MS/TP router but it could be an SC-to-BIP router or just BACnet/SC devices.

New Equipment

- BACnet devices that support BACnet/SC
- BACnet/SC hub ("P" in Figure 4)
- (Optional) BACnet/SC failover hub ("F" in Figure 4)
- BACnet operator workstation that supports BACnet/SC

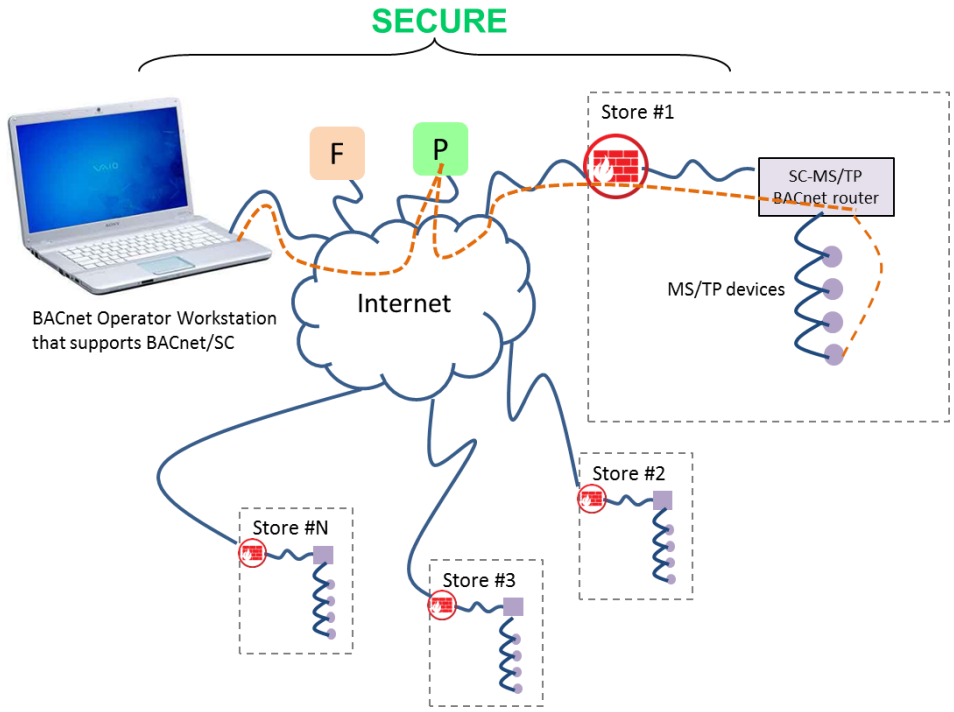


Figure 4: Secure Access to Multiple Facilities across the Internet

Conclusion

Today various approaches are used to secure BACnet infrastructure, but these solutions can be difficult to setup, and they place a burden on IT groups. BACnet/SC will make it much easier to create secure and standardized BA infrastructure that is fully compatible with existing BACnet deployments, friendly to IT best practices, and that enables cloud-based applications.