Local Network/Security Manager

By Keith Corbett, Director Product Development, Cimetrics Inc.

Background

Secured by Cimetrics™ (SbC) is a framework for improving the cybersecurity of BACnet-based *systems*, building upon the BACnet/SC foundation. Whereas BACnet provides tools that vendors can employ to achieve interoperability *within building automation systems*, SbC provides additional tools that vendors can employ to improve cybersecurity *in cooperation with IT management systems*.

SbC defines features for BACnet devices that allow them to be managed securely. The ***SbC Local Network/Security Manager*** *(also known as the SbC Appliance)* is an on-premise device (implemented as a BAS workstation/server, supervisory controller, software running in a datacenter VM, or a stand-alone device) that provides local, secure management during commissioning and operation.

Onboarding and network configuration

BACnet/SC requires devices to be configured with credentials and network settings before they can join the network. Those credentials and network settings need to be maintained and re-issued periodically. The SbC Local Network/Security Manager issues those credentials (or works with an IT authority that issues site credentials) and configures devices with those network settings.

Authorization

Secure BACnet/SC networks may be connected to insecure legacy BACnet networks. Vendors may not wish to allow configuration of their devices (particularly credentials and network settings) by just any device connected to a BACnet/SC network. BAS server/workstations manage authorization policy for their users, but the cybersecurity principle of defense in depth requires moving some authorization responsibility to the endpoint (device) level.

Secured by Cimetrics allows for endpoint authorization of sensitive BACnet requests. The SbC Local Network/Security Manager is trusted by devices, maintains policy, and issues authorization credentials to authenticated clients as needed.

Diagnostics and cybersecurity

SbC provides interoperable mechanisms for devices to share information for diagnostic and security management purposes. The SbC Local Network/Security Manager collects, monitors, and forwards this information.

Interface to IT systems

SbC systems will need to be integrated into IT environments and IT tools such as network monitoring tools, authentication server, certificate authority, and security information and event management (SEIM) software. The SbC Local Network/Security Manager is responsible for forwarding, proxying, and translating protocols on behalf of SbC devices.

Why a Local Network/Security Manager is necessary

Some comparable management functionality exists in proprietary BAS systems. But SbC features and on-the-wire transactions allow interoperability for network and security management. BACnet/SC systems require a single point of control for certificate signing and for authorization. Owner/operators need a single network and security management screen. With SbC, one control vendor's Local Network/Security Manager can manage the network and security needs of another control vendor's subsystem, or third-party equipment.

On-site Local Network/Security Managers are needed for installations where cloud access is not permitted and to allow for continuity of operations when cloud access is interrupted.

Some Local Network/Security Manager features (e.g., certificate signing, configuration) may only be needed for initial commissioning and periodic maintenance. Other features (e.g., authorization, event logging, monitoring, interfacing to IT) need to be continually operational. "***Cybersecurity is a process.***"

The Local Network/Security Manager is a single point in the SbC architecture that provides impedance matching between fast evolving IT tools/standards and long-lived BAS systems. SbC devices do not need to be continually updated and reconfigured to interface with IT systems.

Role in the architecture

The SbC Local Network/Security Manager functionality includes:

- User Interface for network and security management functions
- BACnet/SC Hub
- Network Management Tool
- Authorization Server
- Certificate Authority
- Event Logger/Analytics

A high-level explanation of management features

- Device Onboarding

  Onboarding pertains to the initial installation of new or like-new devices (e.g., reflashed devices) onto the secure SbC network to ensure that only legitimate devices are installed. A key component to onboarding is the issuance of security certificates in accordance with the different needs of the building owner's policy regarding certificates. Onboarding could be a totally local matter or involve a cloud-based mechanism for conformity across diverse portfolios.

SbC Local Network/Security Manager (Appliance)

Onboarding also needs to consider network design, device inventory, diagnostics, and troubleshooting during installation. The onboarding process is also aligned with the typical skillsets of installers of BAS devices who are mostly focused on the functionality of devices rather than security issues. SbC onboarding is designed to be performed by BAS professionals, scale to multi-vendor projects, and abide by the needs of IT and Cybersecurity policies of the facility.

- Authentication and authorization

SbC systems are designed to ensure that only authenticated and authorized users and devices are allowed to be on the network. For users, this means authenticated by approved techniques such as OAuth, OpenID, or other authentication servers provided by the IT organization responsible for the system. Once a user is authenticated, a mechanism of authorization must be in place to control access to all system components. Local IT's best practices may require the use of role-based authentication or other mechanisms demanded by the IT departments having jurisdiction.

Likewise, SbC will need to authenticate each device as per the onboarding mechanism, and using system BAS management tools, the device must be given the authority to be on the network to perform the function intended by the BAS system specifications. Further, BAS specifications may dictate device groupings based on location and device types, such as all VAVs in a building having specific authorization rules.

To enable audit and post-event forensics, SbC is designed to maintain comprehensive logs of both user and device authentication and authorization activities, either on the Local Manager, the Cloud Manager, or in IT systems.

- Certificate management

Key to the secure device-device communication is the initial issuance, maintenance, and expiry of certificates that are required by every single device on a SbC system for the use of the BACnet/SC network transport using TLS 1.3.

The SbC Local Manager can itself act as the Certificate Authority (CA) in some projects, while in others, the Local Manager can act as a proxy to a CA provided by the IT departments of the facility either locally or through the use of a cloud-based authority. A key design criterion is that once configured, the difference between the varying CA policies should not affect how BAS engineers go about their work to install and manage devices.

TLS 1.3 certificates are assigned a finite life after which they expire. The expiry time is typically set as part of the security policies defined by the IT organization. SbC is designed to allow all reasonable certificate expiry as demanded by local policy and to automate monitoring the expiry of all devices under its management scope.

- Asset Management & IAM

By their very nature, SbC systems are large and distributed with most devices in hard-to-reach locations. A key function of a cyber-secure system is that all components of the system are known and managed regardless of where they reside. The SbC Asset Management function is designed to keep a device inventory, perform necessary diagnostics during normal operation, and raise an alert should a new unauthorized device be detected or an authorized device behaves outside of normal condition.

Beyond monitoring for anomalies, SbC is designed to provide defense strategies in the case of an intrusion, including isolating devices and/or groups of devices, automated certificate revocation while alerting both BAS and IT users, and black-listing devices known or suspected to be malicious. A key criterion of BAS systems is that devices that have not been impacted by a breach could and should continue to operate in isolation to maintain the facility environment to the desired quality.

- Routing Firewall policies

The SbC architecture includes the SbC Routing Firewall designed to provide a way to incorporate BACnet devices that communicate using unsecured MS/TP or UDP/IP transport protocols. This routing device effectively isolates the unsecured devices behind a firewall for which firewall policies will need to be created and managed.

The Routing Firewall, as well as the policies they obey, are themselves managed by the Local Manager just like any other SbC device. This ensures that any user manipulating the firewall and policies is legitimately authenticated and authorized. To enable management at scale, the Global Manager in the cloud may be used to apply policies across multiple portfolios of buildings. Lastly, the Local Manager captures firewall logs pertaining to any policy or admin changes as well as detected anomalies.

- Network & Security Configuration

Tied closely with many of the features listed here is the need to securely manage the multitude of devices in the SbC system, specifically devices that may come from different vendors. While different vendors may legitimately have different needs to configure their applications and functions, the network and security configuration must be inherently interoperable.

Any capable SbC-compliant tool must be able to configure the network and security parameters of any Managed Device from any vendor. The tools must abide by specifications defined by SbC including authentication and authorization as well as creating logs and other information for management and audit purposes.

- Backup/Restore

An important area of management that is specified in SbC is how the system handles backing up and restoration of device images and configuration. Bearing in mind that devices may come from multiple vendors, the Backup/Restore process must work in an interoperable way, thus enabling the backup/restore of all devices using a single SbC-compliant tool. This starts with engineers being able to specify a backup policy that would then run autonomously.

The Backup/Restore feature is also implemented to aid the replacement of a failed device. This provides a vendor-neutral and interoperable way to maintain the system by performing a backup, then onboarding the new compatible device, and restoring the image to the new device.

The Backup/Restore will have mechanisms to utilize the Local Manager as a backup location and/or forward images to the local IT storage resources as well as cloud-based storage per the requirements of the facility. Restoration of images will need to be invoked manually or as part of a recovery procedure following an incident. Logs of all backup and restoration are to be kept and forwarded to IT as the site policy demands.

- Version/Firmware Tracking

With the vast number of devices, potentially from multiple vendors and of different types and functionalities, keeping track of software versions of all of the devices on a SbC system is of paramount importance. This process starts with defining the firmware version policy that may differ according to the type of facility and the security requirements defined by facility owners.

A key role for the Local Manager is to maintain a full inventory of all devices under its watch in its location, including software components that often make up a single device. In many devices, this would include configuration versions and potentially other add-on components.

By design, SbC systems will push this information to the Global Manager in the cloud so that it can maintain a complete inventory of all devices in all buildings under management. At the Global level, SbC can then facilitate threat intelligence by continuously comparing versions in the system with known vulnerability information from vendors or third-party threat detection services. This feature will also provide SbC the ability to automate firmware updates if allowed by the local policy.

- Event Logging

SbC is designed to work with tools used by IT and Cybersecurity departments by streaming logs from the Local or Global Manager to the specific tools in use by the IT and Cybersecurity departments responsible for monitoring the building. Types of tools anticipated include Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and others that typically ingest time-series data for constant or batch analysis.

In SbC, security logs are created by all devices under management as well as hubs, routers, firewalls, and gateways. The Local Manager will always maintain a certain amount of log history up to its storage capacity and will forward all logs to a connected IT tool as well as the Global Manager for long-term storage, analysis, and processing. Both the Local and Global Manager will provide rudimentary diagnostics to identify common issues and configuration problems to assist BAS engineers in their tasks.

Conclusion

For over two decades BACnet has provided on-the-wire interoperability between controls vendors and third-party equipment providers for control and monitoring in BAS systems. Controls vendors have developed sophisticated proprietary configuration and management tools for their product lines. SbC allows vendors to add interoperable network and security management capability to their tools and products. The SbC Local Network/Security Manager is the on-premise center of that capability.