SbC Firewall/Router

By Dr. Paul Rensing, Senior Software Developer, Cimetrics Inc.

Background

Secured by Cimetrics™ (SbC) is a framework designed to secure all BACnet devices. Devices conforming to the newly released BACnet/SC protocol use an inherently secure TLS-based data link; BACnet/IP and MS/TP devices, however, do not have secure data links. To facilitate bringing these devices into the secure SbC framework, SbC includes the concept of Firewall/Routers that provides an intelligent and configurable barrier which reduces the risks from unsecured devices.

It should be noted that, throughout this paper, we are explicitly referring to *BACnet* Routers and Firewall/Routers, which are really application-level firewalls in typical IT terminology, not IT-level routers.

Connecting Unsecured Devices

BACnet Routers will allow BAS installers to transition parts of an existing network to use secure BACnet/SC, while leaving other, functioning parts in place. For instance, a large facility may choose to use BACnet/SC as a “campus backbone”, providing secure communication over its “wide area” network. Other sites might switch to BACnet/SC within a building when it is being renovated.

In some customer installations, BACnet/SC routers will have a role which may be longer term. Some devices may only be available in non-SC versions of BACnet. Existing MS/TP installations may be too expensive to replace. In these types of cases, a BACnet/SC Router can connect the BACnet/IP or MS/TP devices to a larger BACnet/SC installation. It should be acknowledged by the installer that this type of installation is less secure than a pure BACnet/SC one, and the customer needs to decide if the risks are acceptable.

While using the older, unsecured data links in a BACnet installation inherently increases some security risks, a Router can reduce them by including “firewall” capabilities in the software. By including the ability to filter/block requests based on various attributes of the request, the network manager can limit the communication between the networks to approved actors (e.g. devices) and request types. For instance, the rules in an SbC Firewall/Router could be

programmed to allow Write-Property requests from a BACnet/SC controller to an MS/TP terminal unit controller, while blocking all Write-Properties from the MS/TP network into the SC one. Combined with physical security, a strong set of firewall rules can significantly reduce the risk of using the older, unsecured data links.

The firewall capabilities of a Router can also help with managing non-critical “add-on” devices, such as BAS Information Kiosks and data collection devices used for ongoing commissioning. While these devices generally do not have any control capabilities, isolating them behind an SbC Firewall/Router adds an additional layer of protection which is under the network manager’s control.

Segmenting BACnet/SC Networks

Many BAS installations will use multiple BACnet/SC networks. Very large customers will want to divide their network into manageable segments. Some sites may have different security requirements (different “trust domains”) in different areas, both geographically or functionally, or devices managed by different responsible parties. A BACnet Router which connects 2 BACnet/SC networks will allow networks to be managed under different rules, yet still communicate as needed.

Although an SC-to-SC Router connects two secure networks, firewall functionality is still an important feature, both for manageability and security. The two SC networks may be operated under different levels of security (for example, one network handles physical security devices); the firewall rules could be set to block various requests coming into the secure network, adding to the “security in depth”. In a very large network (e.g. a university campus), BACnet firewalls between SC networks can be programmed to block certain traffic, such as global broadcasts, thereby reducing load on the network and devices. In general, in the same way that large IT networks are segmented, BACnet/SC networks may be segmented and controlled with SC-to-SC routing firewalls.

Firewall Rules

SbC BACnet Firewall rules will be centrally managed in the “SbC Local Network/Security Manager” and distributed to the routers in the network. This will give the network manager a central view of their policies, allowing better visibility and control.

In terms of capabilities, an SbC BACnet Firewall/Router can filter on many of both the network-level (NPDU) and application-level (APDU) parameters of requests, for example:

- BACnet DeviceId, source and destination
- BACnet Network number, source and destination
- BACnet Object type
- Broadcast type: local, single network, global
- BACnet service: e.g. Write-Property, Time-Sync request, COV subscribe

Similar to IT firewalls, rules in an SbC BACnet Firewall/Router can trigger various reactions: allow, reject, or drop. Matching packets can be logged if desired, which can be useful for both diagnostics and ongoing security monitoring.

An SbC BACnet Firewall/Router can filter packets going in either direction, that is, from BACnet/SC to BACnet/IP or MS/TP and also in the other direction. It allows the network manager to program the rules using a “deny-all-by-default” approach, or the more permissive “deny-by-exception” approach.

Central Logging

Central logging of a wide class of events is an important part of modern cybersecurity systems. Logs are analyzed in real time for common threats and unusual activity, allowing network management staff to respond to threats. The SbC architecture relies on the “Local Network/Security Manager" to deliver the log events from the BACnet devices to a central system, such as an IT SEIM tool.

Routers are crucial network nodes in terms of event logging, since they route traffic between secure and unsecured network segments. Therefore, in addition to logging events directly related to the device itself, a Router will also log information about its through traffic and “downstream” devices, for instance:

- Important traffic between networks, e.g. Write-Property requests, authenticated requests
- Presence of new or unexpected devices on the unsecured network
- Blocked requests
- Specific firewall rules triggered

The specific event types which are logged by the Router should be tunable so as to allow some adjustment to the amount of log traffic, particularly if an event would also be logged by another device.

Traditional (non-SC) BACnet devices do not log events to a central facility, although they may support features like the BACnet Event Log object. An SbC BACnet Router can be configured to subscribe to the Event Logs of its downstream Devices in order to deliver them to the central logging system. That way, the cyber threat monitoring can be extended into the BACnet/IP and MS/TP networks.

Part of Secured by Cimetrics™

The SbC Firewall/Router is a key component of the Secured by Cimetrics framework, created by Cimetrics in collaboration with a BAS industry consensus group of leading vendors to define an interoperable and secure management for BACnet devices and systems. At the core of this framework is the Local Network/Security Manager (SbC Appliance), an on-premise device providing local, secure management during commissioning and operation. The SbC

Firewall/Router, like other managed devices in the system, are managed locally by this Manager.

The Firewall/Router provides a way to allow unmanaged and older BACnet/IP and MS/TP devices to participate in the secure and managed framework by providing functionality to ensure that, should any unsecured device be breached, that segment of the network can be isolated or any harmful commands be blocked through firewall policies.

Conclusion

While transitioning to BACnet/SC is the right thing to do for cybersecurity, unsecured BACnet/IP and MS/TP installations will be around for many years. An SbC BACnet Firewall/Router can help to connect the old and new network installations, and is also an important tool for network segmentation of large BACnet/SC systems. The SbC Firewall features can help maintain some separation between the secure and unsecured network segments, allowing management to monitor the traffic while reducing the risk.