BTune Edge Computer Deployment Primer

CONGRATULATIONS ON EMBARKING ON A BTUNE PROJECT TO SAVE ENERGY AND IMPROVE PERFORMANCE IN YOUR BUILDING!

To get the data-driven building optimisation process started, we will need to deploy a small computer in your building. This document describes the process we use.

We (BTune) supply an edge computer to be installed on your premises, with two ethernet connections, one to the BMS LAN, and the second to the internet. Having the edge computer on site generally means more robust data collection and a more rapid and simple setup process for all parties.

This edge computer periodically polls and collects the current values of selected BACnet objects using the BMS network and forwards those to a cloud server for storage and analysis. Following explicit permission from the client, we can also enable override of selected BMS points to implement energy efficiency measures.

A VPN overlay enables a point-to-point connection between the edge computer and the BTune cloud server. The overlay is established using UDP NAT traversal, minimising the need for firewall configuration changes (typically no incoming firewall exceptions are required, and no outgoing exceptions either).

Deployment Information

These questions help us to pre-configure the edge computer to help the deployment run smoothly:

Physical Site Assessment

Is there a location with the following:

- An available ethernet port connecting to an existing switch on the BMS LAN?
- An available ethernet port connecting to an existing switch providing Internet access?
- Space to mount the edge computer? (the computer physical size is 120x120x50mm excluding plugs, and can be mounted to a VESA mount (75x75 or 100x100 hole pitch), or just placed on a flat surface)
- An available NZ 240V power socket with enough space around for mains adapter plug-pack?
- Appropriate security (i.e. in a locked room) to prevent tampering?
- Appropriate ventilation / cooling (below 50°C under normal operating conditions)? The edge computer emits <40W of heat when running.
- Free from vibration and excessive dust? E.g. alongside the BMS controllers the interior of a switchboard is ideal.

Image: Example BTune edge computer (power and ethernet connectors on rear of unit)

Network Assessment

Connections:

- Can you provide network cable(s) as needed?

Local access:

- Is there a standalone BMS LAN or is it integrated into the wider building network?
- Can the edge computer be installed on the BMS LAN?
- What access controls or segmentation is in place that may restrict access to devices from which we intend to collect data?

Cloud access:

- Is there an existing Internet connection that can be used?
- What access controls or segmentation is in place that may restrict outbound access to the BTune cloud Infrastructure?

IP Addressing:

- Can a static IP address on the BMS LAN be assigned for the edge computer's local access interface? (Please provide to enable configuration prior to dispatch)
- Can a static IP address be assigned for the edge computer's internet access interface?). Alternately, please confirm that the internet access has DHCP, including configured gateway and DNS Servers? (Please provide to enable configuration prior to dispatch.

Legacy Controls Equipment Assessment

BACnet Compatible Devices: Are all desired BACnet devices accessible from the BACnet/IP network on the internal LAN segment? Are routed BACnet networks permitted to be accessed from the BACnet/IP segment on which the edge computer will be installed? Up to 3 ethernet ports on the edge computer can be used for connecting to networks as required.

Particular Site Notes: Are there any particular considerations for the target building? E.g. Labelling, planned shutdowns, audits, power quality, enhanced security?

Physical Installation

A BTune team member or a local network administrator plugs in the edge computer to the site's network(s) and to the power source. BTune customer support is available to provide remote technical support. Once customer support confirms that the deployed gateway can access devices on the required LAN segment, the initial site discovery and the remainder of the installation occurs remotely.

Power:

- Are power indicators lit?
- Is the power cable secure?

Installation:

- Is device securely mounted?
- Is the device labelled appropriately according to site standards?
- Are the cables tidied to prevent disturbances in future?

Network:

- Are the link and activity lights active on interfaces used for your deployment scenario?
- Is BTune customer support receiving communication from the edge device?
- Is BTune customer support able to access devices on the internal LAN segment?

Network Security Considerations:

Overview

Network security is provided by:

- HTTPS TLS 1.3 security for provisioning and control
- VPN overlay, provided using Tailscale software which is based on Wireguard. The VPN overlay enforces a zero trust, deny-by-default, encrypted, point to point communications between the edge computer and the cloud infrastructure. All data are encrypted with the Noise protocol. (more reading here: https://www.wireguard.com/protocol/)
- UDP NAT traversal unless all outbound traffic is disabled, in which case we may need to define a few address/port combos that need to be opened outbound only. No inbound establishment is required – all traffic is via the VPN overlay layer.

How the VPN is established

Network traffic from the edge computer is protected within a VPN overlay. The VPN overlay is established by:

- The edge computer uses an outbound (HTTPS TLS 1.3 protected) connection to a co-ordination server.
- The edge computer deposits its public key, and its public IP address with the co-ordination server.
- The edge computer polls the co-ordination server for the public key the public IP addresses for the monitoring and data processing servers.
- The edge computer attempts to access the monitoring and data processing servers, using the VPN overlay protected by the public keys.

How the edge computer is managed

The cloud platform also provides management functions, including ongoing patch management, access and activity logging, as well as regular reliability and stability software updates to the application and operating system remotely via the VPN. No physical access to the edge computer is normally required once installed unless a major change is required, or a failure occurs.

Typical data exiting site

The data transmitted off site are limited to time-series operational values from the BMS e.g. room temperatures, valve positions, fan speeds, polled at regular intervals. The data is collected and analysed on the cloud infrastructure. Generally, no personally identifiable information (PII) is collected. See snip below for example of typical data leaving a site:

Most Recent Data

time	point name	value
2021-05-24 15:35:00	FCU-L1-34-EN	1
2021-05-24 15:35:00	FCU-L1-34-HTG-VLV	100
2021-05-24 15:35:00	FCU-L1-34-RMT	23.1
2021-05-24 15:35:00	FCU-L1-34-RMT-CLG-SP	23.5
2021-05-24 15:35:00	FCU-L1-34-RMT-EFFSP	23.5
2021-05-24 15:35:00	FCU-L1-34-RMT-HTG-SP	23.5
2021-05-24 15:35:00	FCU-L1-34-SAT	27.7
2021-05-24 15:35:00	FCU-L1-34-SAT-SP	30
2021-05-24 15:35:00	FCU-L1-34-SPD	40
2021-05-24 15:35:00	FCU-L1-34-STS	1

Image: Sample of typical data exiting site

Software running on edge computer

The edge computer runs a Unix operating system and uses a configurable software package to collect BMS operational data only for analysis by our team and is capable of issuing commands back to the BMS (subject to client approval) to improve building performance. The edge computer also hosts the VPN overlay endpoint software.

Volume of data / bandwidth

The required bandwidth varies depending on building size, poll rate, and complexity of control system. Generally, using the use of an existing ADSL or fibre connection is appropriate. If an internet connection is not available, we can provide a 4G cellular data connection if required.

Refer also diagrams following for more network information. If you require further information, please get in touch with us directly via your BTune contacts and we would be happy to help.

Deployment Information Proforma

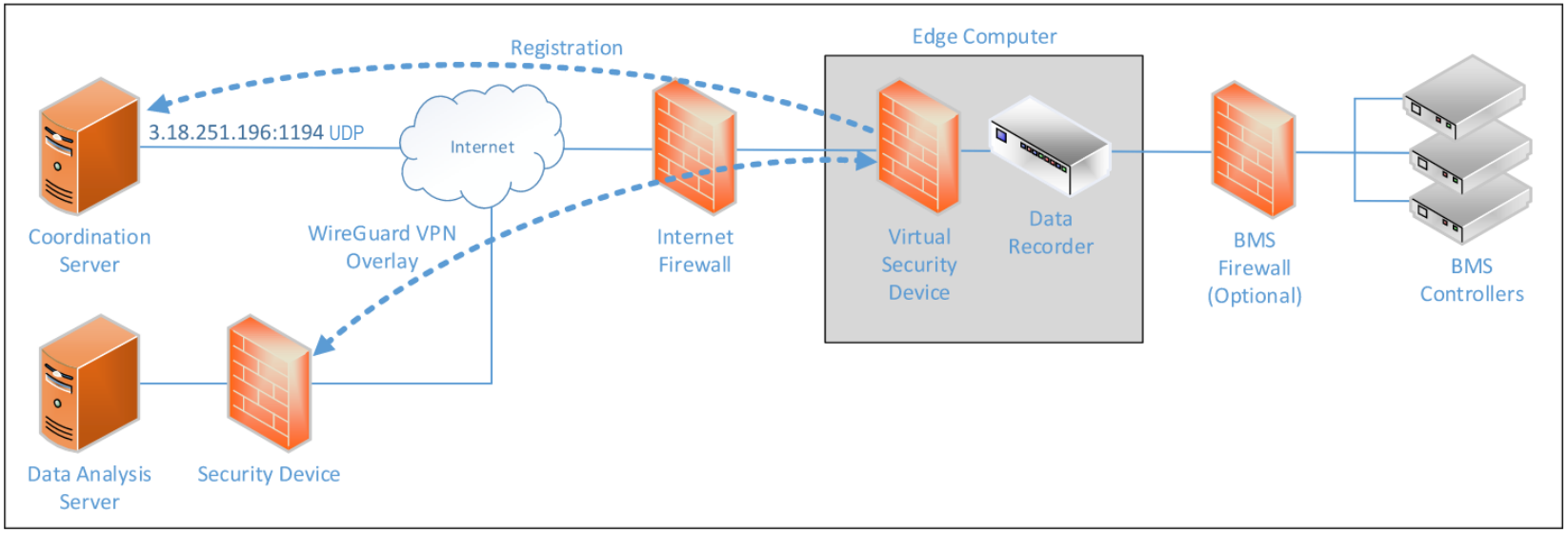
Site Name:	.....		
Site Address:	.....		
Edge computer location on site:	.....		
Client contact name:	.....		
Client contact number:	.....		
Local network administrator name:	.....		
Local network administration contact number:	.....		
Internal LAN segment address range:	.....		
Ethernet interface 1 (labelled WAN):	Not Used	Static (___.___.___.___)	DHCP
Ethernet interface 2 (labelled LAN):	Not Used	Static (___.___.___.___)	DHCP
Ethernet interface 3 (labelled OPT1):	Not Used	Static (___.___.___.___)	DHCP
Ethernet interface 4 (labelled OPT2):	Not Used	Static (___.___.___.___)	DHCP

Notes:

e.g. non-standard BACnet port

BTune Networking Diagram

PROPOSED BTUNE NETWORK CONFIGURATION



DEVICES

Within the Edge Computer are 2 separate software components, being:

1. a Security Device, responsible for the establishment of a WireGuard VPN Overlay with the corresponding security device in front of the Data Analysis Server, using a Coordination Server to share Public keys and register endpoint details.
2. a Data Recorder, responsible for querying the BMS controllers and uploading the point data to the Data Analysis Server

PHYSICAL CONNECTIONS

The Edge Computer requires 2 connections, including IP addresses, being:

1. A connection to the Internet
2. A connection on the BMS Controller sub-net

INTERNET FIREWALL SETTINGS

The Security Device uses the following outbound internet connections:

1. Coordination Server: 3.18.251.196:1194 UDP
2. Security device in front of the Data Analysis Server: Dynamic, as advised by the Coordination Server

There is no need for inbound firewall rule configuration

BMS FIREWALL SETTINGS

If required, a security device can be installed between the Edge Computer and BMS Controllers.
The recommended approach is for a layer 2 firewall permitting BACnet communications (port 47808), otherwise further configuration is required with BACnet Broadcast Management Devices (BBMDs) etc. Please contact Beca to discuss.