RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS DE SÉCURITÉ RELATIVES À LA GESTION TECHNIQUE ET CENTRALISÉE DU BÂTIMENT (GTB/GTC)

GUIDE ANSSI

ANSSI-PA-110
27/04/2026

PUBLIC VISÉ :

Développeur | Administrateur | RSSI | DSI | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Recommandations de sécurité relatives à la gestion technique et centralisée du bâtiment (GTB/GTC) »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	27/04/2026	Version initiale

Table des matières

1
Introduction

Information

Cette version du guide tient compte des architectures actuellement déployées, ainsi que l'ensemble des éléments relatifs aux dispositifs de détection et à leur intégration technique. Une prochaine version sera publiée prochainement afin d'étendre la couverture aux architectures basées sur le protocole BACnet/SC et d'y intégrer les éléments spécifiques à détecter dans ce nouveau périmètre fonctionnel. Bien que ce guide soit illustré avec des exemples issus du monde hospitalier et de la santé, il est entièrement applicable à d'autres industries et secteurs économiques.

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*. Afin de faciliter la mise en œuvre des actions de sécurisation, les recommandations sont listées selon un ordre de priorisation préconisé. Par ailleurs, elles sont accompagnées par un niveau Nx, correspondant à un indicateur temporel de mise en œuvre, qui n'est pas corrélé avec le niveau de prescription de la recommandation. L'interprétation de ce niveau est la suivante :

- **N1** : Recommandation à mettre en œuvre à court ou moyen terme ;
- **N2** : Recommandation à mettre en œuvre à moyen ou long terme.

Pour certaines recommandations, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant une protection adaptée à son contexte et ses objectifs de sécurité.

Les recommandations sont présentées de la manière suivante :

R

[N*] Recommandation à l'état de l'art

La recommandation permet de mettre en place un niveau de sécurité optimal.

R -

[N*] Premier niveau de recommandation alternative

Cette recommandation propose un niveau de sécurité moindre que la recommandation R*x*.

2
Présentation de la GTB/GTC

Attention

Le système de gestion technique du bâtiment est très souvent géré sous forme de prestation. Comme précisé dans la suite du document, selon les cas d'application (hôpitaux, laboratoires, manufactures, etc.), ces systèmes peuvent être critiques, et nécessitent d'être connus et maîtrisés par les services techniques concernés.

2.1 Définition

La gestion technique du bâtiment (GTB) est un système permettant de contrôler à distance plusieurs éléments d'un bâtiment, à usage tertiaire ou hospitalier par exemple. La gestion technique centralisée (GTC) est un sous-élément de la gestion technique du bâtiment.

Ces systèmes sont composés, entre autres, de capteurs, d'actionneurs, d'automates et de postes de supervision.

La GTB permet de contrôler et d'optimiser (recherche d'une efficacité énergétique) les installations techniques suivantes :

- les systèmes de chauffage, de ventilation et de climatisation (CVC ou HVAC en anglais) ;
- les installations de plomberie ;
- les ascenseurs ;
- la transformation et la distribution d'électricité (dans ce cas, on peut parle de GTE) ;
- l'éclairage ;
- les équipements de sûreté d'un bâtiment tels que la vidéoprotection et le contrôle d'accès ;
- le système de sécurité incendie (SSI).

Bien que les constituants de la GTB du domaine tertiaire et des hôpitaux soient les mêmes, ces derniers sont parfois composés de plusieurs bâtiments nécessitant une mise en réseau, sur une étendue plus importante. Par ailleurs, dans les centres hospitaliers, des équipements sensibles sont également gérés par la GTB.

Il s'agit des éléments suivants :

- le poste de transformation et le tableau général basse tension permettant la protection et la distribution de l'énergie au sein des différents bâtiments ;

- le centre de traitement de l'air, le CTA (par exemple, en milieu hospitalier, les salles d'opération, y compris les zones aseptiques [1]);
- la surveillance des paramètres physiques de l'eau (notamment la température de l'eau chaude qui peut être source d'organismes microbiologiques responsables de l'augmentation de la concentration en légionnelles);
- la surveillance des onduleurs du bâtiment (présence d'une tension);
- les groupes frigorifiques;
- les laboratoires (virologie, laboratoire L3 permettant le confinement des agents biologiques manipulés);
- dans le milieu hospitalier, les fluides médicaux [2] (oxygène, air, protoxyde d'azote, etc.).

À cela peuvent s'ajouter des systèmes d'optimisation de l'énergie (gestion de panneaux solaires, de façades bioclimatiques, etc.).

Information

Contrairement au système informatique de gestion, qui est maintenu par le service informatique, la gestion technique du bâtiment est souvent confiée à un prestataire. La mise en œuvre des mesures permettant de garantir la disponibilité et l'intégrité de l'installation doit donc être une priorité.

2.2 Architecture type

Un système de GTB est généralement constitué de sous-systèmes GTC. Ces derniers permettent, comme précisé à la section 2.1, de gérer des fonctions techniques indépendantes. La figure 1 illustre de façon non exhaustive quelques fonctions pouvant être présentes au sein d'un système GTB.

Les sous-systèmes GTC communiquent avec un poste de supervision sur lequel est raccordé un ou plusieurs postes clients disposés à proximité du serveur et/ou dans les centres techniques GTC (ces postes ne figurent pas tous sur la figure).

Une zone GTE (gestion technique électrique) est présente sur la partie droite du schéma. Le serveur GTE est parfois raccordé à celui de la GTB, c'est pourquoi un lien a été représenté.

Au sein d'un site industriel ou d'un grand site tertiaire, il est fréquent de trouver plusieurs bâtiments, et donc tout autant de systèmes GTB. Seul un premier bâtiment a été détaillé sur la figure 1 et peut être reproduit autant de fois que de bâtiments.

Enfin, la présence d'un unique automate par GTC ne préjuge pas de la quantité réellement intégrée au sein d'un bâtiment.

1. Selon l'Académie nationale de médecine, afin de minimiser les risques de contamination et d'infections nosocomiales, toutes les salles d'opération aseptiques et hyper aseptiques doivent être en hyper pression, avec ventilation d'air hautement filtré à taux de renouvellement élevé et à haut débit. Une attention toute particulière doit être apportée à la température, au degré d'hygrométrie, etc.
https://www.academie-medecine.fr/09-11-bloc-operatoire-de-la-salle-doperation-a-la-plate-forme-interventionnelle/
2. Ces derniers sont parfois isolés du réseau de la GTB/GTC.

Information

Certains fournisseurs de SCADA imposent l'utilisation d'un serveur *Active Directory* pour l'authentification des utilisateurs. Ce guide ne traite pas des architectures d'authentification des utilisateurs sur l'environnement GTB/GTC.

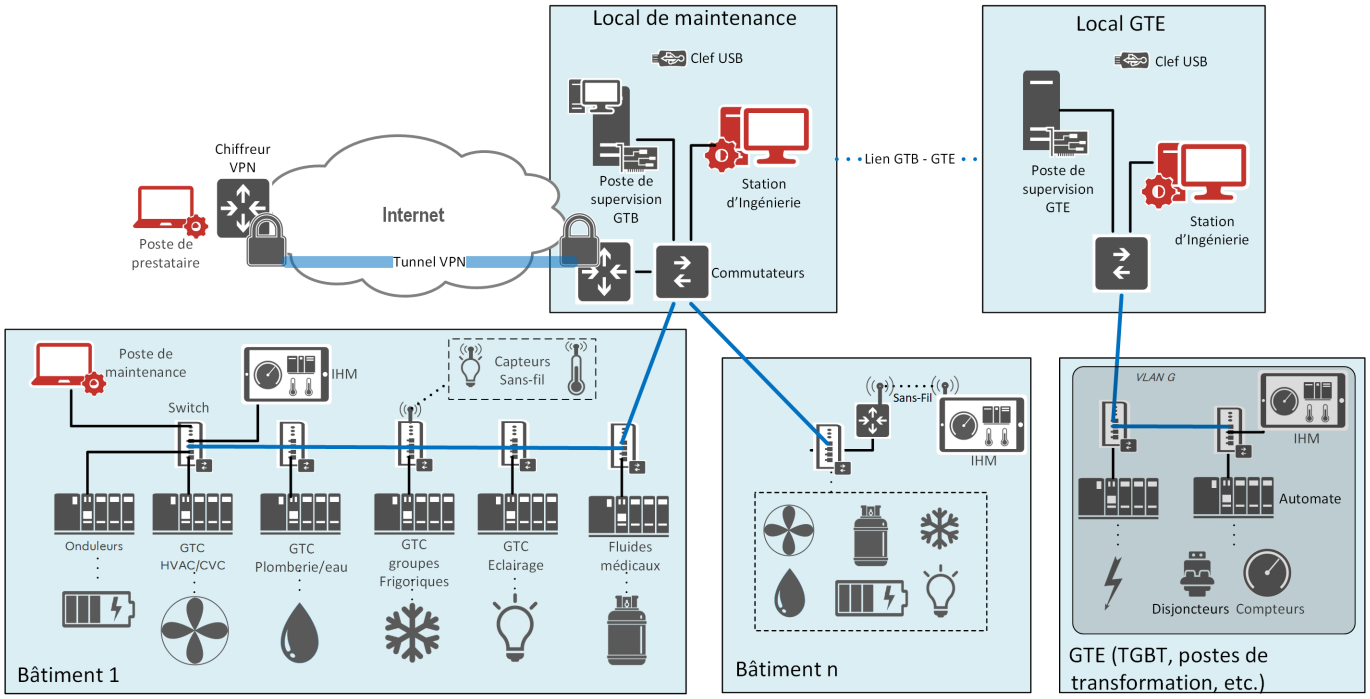

FIGURE 1 – Architecture type GTB/GTC

3
Sécurisation de la GTB/GTC

3.1 Architecture type sécurisée

La figure 2 représente des éléments de sécurisation de l'architecture type décrite en section 2.2. Pour cela, des numéros de couleur rouge ont été positionnés. Ces numéros correspondent aux fonctions de sécurité proposées et sont listées ci-dessous. Les numéros ne sont pas listés par ordre de priorité. Pour cela, il faut se référer au niveau **Nx** (voir la description au chapitre 1) de chaque recommandation.

1. Administration et station d'ingénierie (se référer à la section 3.2)
2. Cloisonnement (se référer à la section 3.3)
3. Réseau de la GTB (se référer à la section 3.4.1)
4. Filtrage et routage (se référer aux sections 3.3 et 3.4.2)
5. Durcissement des automates (se référer à la section 3.4.3)
6. Utilisation de médias amovibles comme une clef USB (se référer à la section 3.4.4)
7. Sécurisation des communications des composants de la GTB (se référer à la section 3.4.5)

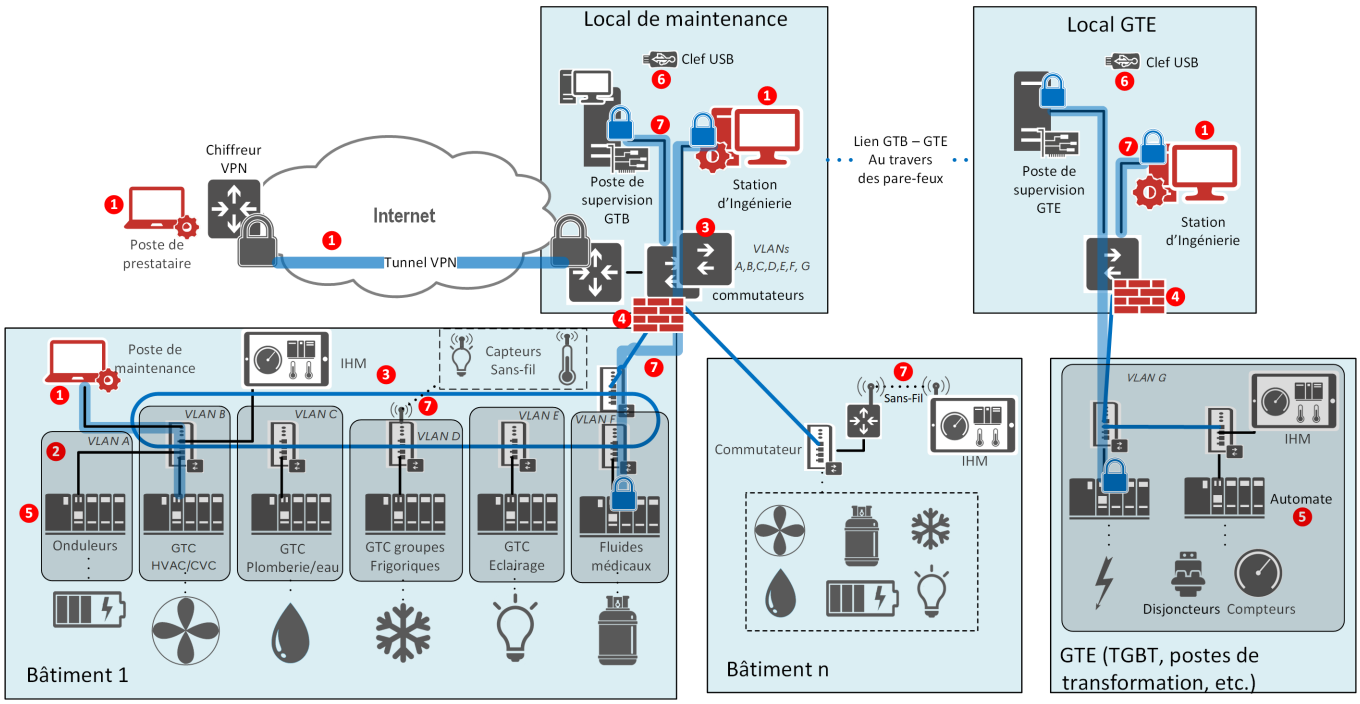

FIGURE 2 – Architecture type sécurisée GTB/GTC

3.2 Réseau et postes d'administration

Pour des questions de sécurité, il est conseillé de mettre en place un réseau logique dédié aux flux d'administration des équipements de la GTB, distinct du réseau métier de la GTB. De la même manière, les postes d'ingénierie doivent être dédiés à cet usage.

R1

[N1] Utiliser un poste d'ingénierie dédié et sécurisé

Il est recommandé d'utiliser un poste d'ingénierie strictement dédié à l'usage des actions d'administration de la GTB. Ces postes sont sécurisés et, en particulier, tout accès à Internet (Web, messagerie électronique) y est interdit, y compris en situation de mobilité. Ce poste doit répondre aux exigences du guide d'hygiène informatique [7] et des recommandations de configuration matérielle de postes clients et serveurs x86 [1].

R2

[N1] Cloisonner le réseau d'administration

Il est recommandé de regrouper les poste d'ingénierie dans un réseau IP dédié, cloisonné logiquement pu physiquement du reste du système d'information, par l'utilisation de VLAN et d'un équipement de filtrage empêchant toute connexion directe depuis les autres zones de confiance. Cela inclut une solution de filtrage logiciel sur les postes afin que les administrateurs de la GTB ne puissent pas avoir accès à Internet depuis un site distant (cas du domicile par exemple).

R3

[N1] Utiliser des protocoles sécurisés pour les flux d'administration

Il est recommandé d'utiliser des protocoles et des outils d'administration reposant sur des mécanismes de chiffrement et d'authentification robustes (cf. RGS [13]) et de privilégier les protocoles sécurisés standardisés et éprouvés (comme TLS ou SSH).

De nombreux équipements industriels intègrent des protocoles d'administration propriétaires ne mettant pas en œuvre des mécanismes cryptographiques robustes ou à l'état de l'art. Dans ce cas, l'emploi d'un tunnel VPN IPsec ou d'un tunnel TLS (dans sa version v1.3), depuis le serveur des outils d'administration ou le poste d'administration jusqu'au plus proche de la ressource administrée, permet de pallier ces carences.

Attention

Les protocoles de prise en main à distance comme « VNC » ne sont pas considérés comme sûrs et doivent donc être encapsulés au travers d'un tunnel VPN IPsec, comme présenté précédemment.

R3 -

[N1] Protéger les flux d'administration dans un tunnel VPN IPsec

À défaut d'interfaces d'administration dédiées ou d'outils d'administration permettant le chiffrement et l'authentification de bout en bout, les flux d'administration doivent être protégés par la mise en œuvre d'un tunnel VPN IPsec, avec authentification mutuelle par certificats, (par exemple depuis un bastion [3]utilisant un certificat vers les ressources administrées). Ce tunnel VPN IPsec doit être établi au plus proche de la ressource d'administration et de la ressource administrée. Cet équipement peut être mutualisé pour l'administration sécurisée de l'ensemble des automates présents dans le local.

Attention

Les postes des prestataires n'étant pas maîtrisés, les accès distants depuis ces derniers doivent transiter par une chaîne d'accès dédiée complétée par un bastion.

3.3 Cloisonnement de la gestion technique du bâtiment

De par leur conception, les équipements constituant le système de gestion technique de bâtiment intègrent des protocoles peu ou pas sécurisés par défaut. De plus, les constituants de ce système présentent des niveaux d'exposition souvent élevés compte tenu de leur emplacement et de leur accessibilité. Il est donc important que le système GTB soit cloisonné des autres SI et que les protocoles utilisés soient sécurisés conformément à la section 3.4.5.

R4

[N1] Cloisonner le système de GTB

Les équipements constituant le système de gestion technique du bâtiment doivent être cloisonnés des autres systèmes d'information, physiquement, ou logiquement par l'utilisation de VLAN. De la même manière, les constituants de ce système doivent être cloisonnés par fonction de GTC (par exemple, la gestion du traitement de l'air doit être cloisonnée de la gestion de l'eau chaude et eau froide).

Si des équipements entre sous-systèmes de GTC doivent communiquer ensemble, les flux doivent transiter au travers d'un pare-feu qui réalise les opérations de routage et de filtrage.

R5

[N2] Filtrer les flux de communication inter-VLAN

La mise en œuvre d'un cloisonnement efficace implique que tous les flux doivent transiter par un pare-feu configuré pour filtrer les seuls flux strictement nécessaires aux besoins fonctionnels.

Dans le cas d'une architecture GTB utilisant le protocole BACnet/IP, l'application des recommandations R4 et R5 nécessite la mise en place d'une architecture BACnet/IP avec BBMD (*BACnet Broadcast Management Device*, dès lors qu'un service de *broadcast* entre les sous-réseaux IP est

3. La mise en œuvre d'un bastion est décrite dans le guide Recommandations relatives à l'administration sécurisée des systèmes d'information [10].

nécessaire en production, afin de ne pas perturber le bon fonctionnement de la GTB. Pour plus d'informations, se référer à l'annexe B.

R6

[N1] Utiliser un tunnel VPN IPsec pour l'accès distant à la GTB

Pour assurer un niveau de sécurité suffisant pour les connexions à partir des postes nomades, il est recommandé, pour tous les utilisateurs, de mettre en œuvre un tunnel VPN IPSec et des mécanismes d'authentification robustes (par exemple multifacteur par certificat [15]) pour l'accès distant à la GTB.

R6 -

[N1] Utiliser un tunnel VPN TLS pour l'accès distant à la GTB

À défaut d'utiliser un tunnel VPN IPSec, l'utilisation d'un VPN TLS est tolérée si la version utilisée est TLS v1.3.

R7

[N1] Désactiver la fonctionnalité de « Foreign Device »

Il est recommandé de désactiver la fonctionnalité de « *Foreign Device* » dans les équipements BACnet/IP et de filtrer les services réseaux propres à son utilisation, conformément aux prescriptions fournies en Annexe B.

3.4 Défense en profondeur

3.4.1 Réseau et commutateurs

Les automates de la GTB/GTC sont raccordés entre eux ou avec le système de supervision SCADA au travers d'un réseau de type Ethernet constitué, le plus souvent, de commutateurs.

R8

[N1] Renforcer la disponibilité du réseau GTB

Afin d'assurer un niveau de disponibilité satisfaisant du réseau, il est recommandé d'assurer la redondance du support de transmission en réalisant, par exemple, un anneau (comme précisé à la figure 2). Il est également recommandé d'assurer la redondance des commutateurs situés au niveau du système de supervision comme présenté à la figure 2.

R9

[N1] Cloisonner les ports Ethernet muraux et désactiver les ports non utilisés

Il est recommandé que les ports Ethernet fixés aux murs des lieux accueillant du public soient intégrés dans un VLAN d'« accueil » et que les ports Ethernet non utilisés soient tous désactivés et positionnés dans un VLAN de quarantaine, conformément aux guides [2], [5] et [6].

R10

[N1] Durcir les commutateurs

Certains automates ne permettant pas leur sécurisation, il est recommandé de mettre en place le principe de défense en profondeur en sécurisant les équipements réseau à proximité, dont les commutateurs, conformément aux guides [2], [3] et [6].

R11

[N2] Mettre en place des « private VLAN » sur le réseau de la GTB/GTC

Afin de limiter les communications non souhaitées entre machines du réseau GTB/GTC, il est fortement recommandé de bloquer les communications entre les différentes ressources par la mise en œuvre du mécanisme PVLAN en mode isolé [4] au niveau des différents commutateurs desservant les locaux techniques GTB/GTC.

Certaines installations de GTB sont équipées d'équipements obsolètes et disposent d'interfaces de communication type RS485 (Modbus-RTU et BACnet-MSTP par exemple) au niveau des automates. Lorsque le système de supervision de l'installation est plus récent, il est fréquent de constater l'utilisation de passerelles protocolaires permettant la conversion de média RS485 vers TCP/IP. Ces équipements étant peu robustes et peu sécurisés, il est nécessaire de procéder à leur durcissement.

R12

[N1] Durcir les passerelles protocolaires

Les équipements utilisés pour la conversion de média RS485 vers TCP/IP doivent être maintenus en condition de sécurité afin d'intégrer les mises à jour de sécurité. En effet, ce type d'équipement peut présenter des vulnérabilités sévères. De plus, tout comme les composants d'un système IT, il est recommandé de limiter la surface d'attaque en désactivant les services non utilisés (DHCP, FTP, TFTP, HTTP, etc.). En effet, ces services font souvent l'objet de vulnérabilités critiques.

Outre le risque de provoquer des dysfonctionnements sur la GTB, une mauvaise synchronisation horaire a également des impacts sur la journalisation des évènements de sécurité. Certains protocoles d'exploitation (tel que BACnet) intègrent leur propre mécanisme de synchronisation horaire.

En cas d'investigation sur un incident, il est préférable de recourir à un serveur de temps fiable et de source identique aux équipements des fonctions connexes (IT, services techniques, biomédical, etc.) pour garantir l'intégrité et l'imputabilité des traces.

R13

[N1] Garantir la synchronisation horaire au sein du SI de la GTB

Afin d'uniformiser le synchronisation horaire et conformément à la règle R45 du guide de sécurisation des commutateurs [2], il est recommandé de ne pas utiliser les protocoles d'exploitation métier pour la synchronisation horaire et de préférer le protocole NTPv4 lorsque celui-ci est disponible sur les équipements.

4. *Private VLAN isolated*.

3.4.2 Pare-feu

La mise en œuvre d'un pare-feu au sein du SI de GTB/GTC permet de réaliser, entre autres, les fonctions suivantes :

- routage inter-VLAN (comme précisé à la section 3.3) ;
- filtrage des flux uniquement autorisés ;
- inspection et filtrage de trames illégitimes.

Pour cette dernière fonction, des éléments de configuration et de filtrage sont précisés dans les annexes A et B.

3.4.3 Automates

Certains automates disposent de fonctions de sécurité permettant de garantir l'intégrité de la configuration, du micrologiciel, le chiffrement des communications, etc. Les fonctions de sécurité concernées sont listées ci-dessous et doivent être mises en œuvre. Certaines sont activées par défaut lorsqu'il s'agit d'un automate avec un visa de sécurité de l'ANSSI - pour plus de détails, se reporter au site de l'ANSSI [5].

R14

[N1] Vérifier l'intégrité du micrologiciel et de la configuration de l'automate

Il est recommandé de vérifier périodiquement l'intégrité du logiciel d'ingénierie, du micrologiciel et de la configuration de l'automate. Ces contrôles d'intégrité permettent de savoir si une des bibliothèques utilisées par le logiciel ou une fonction de l'automate a été modifiée. Certains logiciels d'ingénierie proposent une fonction d'auto-test de leur intégrité.

R15

[N1] Protéger par un mot de passe les éléments sensibles de l'automate

Il est recommandé de protéger l'automate par la mise en place d'un mot de passe (modifier celui par défaut si ce dernier est déjà activé) pour les fonctionnalités suivantes (voir le guide de l'ANSSI sur le sujet [16]) :

- protection du programme : permet de protéger les modifications des blocs d'un programme (lecture, écriture ou aucun) ;
- protection de l'application : permet d'éviter le téléchargement ou l'ouverture de fichiers d'application de l'automate (et donc de conserver le confidentialité du contenu de la configuration) ;
- protection du micrologiciel : l'accès au micrologiciel des différentes cartes de l'automate est bloqué, évitant ainsi sa modification illégitime ;
- protection de l'application sauvegardée sur la carte mémoire de l'équipement : permet d'éviter une incohérence entre la configuration contenue dans l'automate et celle présente dans la carte mémoire, évitant ainsi l'exécution d'un programme illégitime se trouvant dans la carte mémoire.

5. https://cyber.gouv.fr/trouver-un-produitservice-de-securite-evalue

R16

[N1] Désactiver les services non utilisés

Tout comme les composants d'un système IT, il est recommandé de limiter la surface d'attaque en désactivant les services non utilisés (DHCP, FTP, TFTP, HTTP, etc.). En effet, ces services font souvent l'objet de vulnérabilités critiques. Si les automates requièrent l'utilisation d'un protocole non sécurisé dans le cadre de mise à jour, l'activation doit être réalisée à la demande.

R17

[N2] Activer le contrôle d'accès IP

Certains automates sont équipés d'une fonctionnalité permettant d'ajouter les adresses IP des équipements légitimes pour la configuration et l'accès à l'automate. Il est recommandé d'utiliser cette liste de contrôle d'accès afin de réduire la surface d'attaque et d'appliquer le principe de défense en profondeur.

R18

[N2] Activer la journalisation

Il est recommandé d'activer la fonction de journalisation pour la transmission d'évènements de sécurité ou pour la corrélation d'informations métier lors d'un incident. L'exploitation des informations de journalisation nécessite par ailleurs la mise en œuvre d'un serveur de collecte de journaux comme précisé dans le guide Recommandations de sécurité pour l'architecture d'un système de journalisation [12].

3.4.4 Médias amovibles USB

L'utilisation de médias amovibles, tels qu'une clef de stockage USB, est une des causes de la propagation d'un code malveillant. C'est pourquoi, plusieurs recommandations doivent être appliquées.

Laisser des interfaces ouvertes non maîtrisées augmente le risque d'attaque. Par exemple, ne pas bloquer les ports USB, et ainsi offrir la possibilité de connecter des périphériques non maîtrisés, peut favoriser l'introduction d'un virus dans le système et perturber son fonctionnement. Cette absence de blocage peut également être utilisée pour lancer ultérieurement une attaque depuis l'extérieur du site (en connectant un équipement Wi-Fi par exemple).

R19

[N1] Bloquer ou désactiver les ports USB non utilisés

Il est recommandé de bloquer les ports USB des postes d'ingénierie, des postes de supervision et des automates lorsque cela est possible. Ce blocage peut être réalisé à l'aide de mécanismes de sécurité physiques ou logiques, comme les verrous USB physiques (avec clés), ou par un logiciel de sécurité capable de bloquer l'utilisation de clés USB et autres périphériques. Le démarrage du poste à partir d'un support USB doit être désactivé dans le BIOS ou l'UEFI.

R20

[N2] Sécuriser l'accès au BIOS/UEFI

Conformément au guide de configuration matérielle de postes clients et serveurs x86 [1], il est recommandé de protéger l'accès au BIOS ou à l'UEFI par un mot de

passe.

R21

[N1] Utiliser un sas ou une station blanche avant l'introduction de médias amovibles

Pour les ports USB devant rester ouverts et l'utilisation de médias amovibles, il est recommandé d'utiliser un sas ou une station blanche, régulièrement mis à jour, conformément au référentiel de l'ANSSI [14]. Des solutions *open source* de station blanche sont disponibles sur Internet si besoin.

3.4.5 Sécurisation des communications de la GTB

Certains éléments constituant la GTB supportent différents modes de communication sans fil (ZigBee, LoRa, Wi-Fi ou 4G essentiellement). Leur mise en œuvre augmente très significativement l'exposition des dispositifs aux attaques logiques. Compte tenu du type de matériel employé et de leur localisation, l'utilisation d'équipements sans fil peut s'avérer nécessaire. C'est pourquoi, il est fortement recommandé d'utiliser un protocole de communication sécurisé. De plus amples informations sont disponibles dans le guide de sécurisation IOT [11].

R22

[N1] Privilégier l'utilisation de protocoles sécurisés pour les communications entre équipements utilisant un réseau sans fil

Dans le cadre de la GTB, il est recommandé de mettre en œuvre des équipements intégrant des protocoles sécurisés (au niveau réseau ou applicatif), notamment pour les communications sans fil (entre automate et capteur par exemple).

Si la communication sans fil n'est pas sécurisée, l'équipement peut être substitué par un équipement malveillant simplement par le support de la communication non sécurisée. Dans ce cas, l'utilisation d'un pare-feu restera une mesure applicable.

R22 -

[N1] Permettre les communications sans fil non sécurisées aux seuls composants non sensibles

Certains équipements, comme les objets connectés, ne permettent pas l'utilisation de protocoles sécurisés. À défaut d'utiliser un protocole sécurisé entres les composants sans fil, il est recommandé d'utiliser uniquement les capteurs sans fil dont l'indisponibilité n'a aucune conséquence sur le réseau GTB. Conformément au référentiel IOT [11], l'objet connecté doit être intrinsèquement protégé. Le cas échéant, il est nécessaire d'ajouter des règles de filtrage comme précisé au paragraphe 3.4.2.

Lorsqu'il n'est pas possible de supprimer les liaisons Wi-Fi des composants de la GTB, et conformément au guide de sécurisation relatif aux réseaux Wi-Fi [8], la recommandation R23 est à prendre en compte.

R23

[N2] Configurer un algorithme de chiffrement robuste du réseau Wi-Fi

Les points d'accès Wi-Fi doivent être configurés pour utiliser un chiffrement robuste. Les modes WPA2 avec l'algorithme de chiffrement AES-CCMP-128 ou WPA3 sont fortement recommandés avec une infrastructure d'authentification centralisée s'appuyant sur WPA-Entreprise.

R24

[N1] Privilégier l'utilisation de protocoles sécurisés pour les communications entre l'automate et le poste de supervision

Bien que le poste local de supervision de la gestion technique du bâtiment soit à proximité de l'installation, il est recommandé d'utiliser un protocole sécurisé entre l'automate de la GTB et le poste de supervision (certains automates intègrent des fonctions de chiffrement des communications comme IPsec ou OPC UA).

R25

[N2] Privilégier l'utilisation de protocoles sécurisés pour les communications entre l'automate et les entrées/sorties déportées

Il est recommandé d'utiliser un protocole sécurisé entre l'automate et les entrées/sorties déportées (certains automates intègrent des fonctions de chiffrement des communications comme IPsec ou OPC UA).

R26

[N1] Sécuriser les protocoles Modbus et BACnet

Dans le cas d'utilisation du protocole Modbus ou BACnet, il est recommandé d'appliquer les mesures de sécurité décrites respectivement dans les annexes A et B.

Annexe A
Modbus : détection et filtrage

A.1 Avant-propos

Cette annexe a pour but de définir des mesures de sécurité relatives à l'utilisation du protocole Modbus dans le cas où ce dernier ne peut pas être remplacé par un protocole sécurisé tel que OPC UA [6]. Modbus est un protocole d'exploitation assurant des besoins de communication métier entre plusieurs composants du système industriel :

- communication entre automate(s) et supervision (IHM locale ou SCADA) ;
- communication entre automates ;
- communication entre automates et entrées/sorties déportées ;
- dans certains cas, communication entre la station d'ingénierie et les automates ou IHM (terminal).

Pour cela, le protocole Modbus implémente des fonctions permettant d'effectuer des actions sur les équipements du système industriel telles que :

- la lecture de registres ;
- l'écriture de registres ;
- le diagnostic de l'équipement (identification, statistiques, etc.).

De par son ancienneté, ce dernier n'intègre pas de fonctions de cybersécurité. Ainsi, il est recommandé de filtrer ou détecter certaines fonctions dont l'usage en production doit alerter la supervision.

Information

Le positionnement des sondes de détection dans l'architecture de la GTB/GTC n'est pas traité dans ce document. Veuillez vous référer au guide Doctrine de détection pour les systèmes industriels [9] pour plus d'informations.

6. L'utilisation d'un protocole sécurisé s'appuyant par exemple sur le standard OPC UA ne permet pas de s'affranchir de la mise en œuvre d'un mécanisme de détection et de filtrage.

A.2 Recommandations de filtrage et de détection

En situation de production, il est recommandé de filtrer et/ou détecter l'utilisation des fonctions présentées ci-dessous (à l'aide d'un pare-feu et/ou d'un système de détection). Le tableau 1 récapitule l'application des fonctions de filtrage et de détection sur les fonctions Modbus.

Code (hex)	Fonction	Action
0x11	**ReportSlaveID**	**Filtrer**
0x14	**ReadFileRecord**	**Détecter**
0x15	**WriteFileRecord**	**Filtrer**
0x0F	**WriteMultipleCoils**	**Filtrer ou détecter**
0x10	**WriteMultipleRegisters**	**Filtrer ou détecter**
0x2B	**Encapsulated Interface Transport**	**Filtrer**
0x5A	**Schneider Electric - UMAS**	**Filtrer**

TABLE 1 – Filtrage et détection des fonctions Modbus

- **ReportSlaveID :** Cette fonction permet de récupérer des informations d'identification et de version d'un équipement, elle est entre autres utilisée par des outils de reconnaissance tels que le script NMAP « modbus-discover.nse ». Cette fonction est utile pour un attaquant et n'est en aucun cas utile en production.
- **ReadFileRecord :** Cette fonction permet une lecture massive de registres et n'est pas utile en production, mais elle permet à un attaquant de lire le contenu des registres de l'automate.
- **WriteFileRecord :** Cette fonction permet une écriture globale de registres et n'est donc pas utile en production. Par ailleurs, elle permet à un attaquant d'écrire massivement dans l'automate, ce qui augmente le risque d'exploitation d'une vulnérabilité dans l'implémentation des piles Modbus.
- **WriteMultipleCoils :** Cette fonction permet d'écrire plusieurs valeurs dans les registres de type « *Coils* » de l'automate et n'est généralement pas utilisée en production car il est possible et moins dangereux d'utiliser la fonction *WriteSingleCoil* permettant d'écrire sur un seul registre à la fois. Néanmoins, il est possible que l'exploitant exprime le besoin d'utiliser cette fonction en production, dans ce cas, le filtrage de cette fonction est laissé à la discrétion de l'exploitant.
- **WriteMultipleRegisters :** Cette fonction permet d'écrire en une seule requête des valeurs dans les registres de type *Holding Register* de l'automate. Elle n'est généralement pas utilisée en production car il est possible et moins dangereux d'utiliser la fonction *WriteSingleRegister* permettant d'écrire sur un seul registre à la fois. Néanmoins, il est possible que l'exploitant exprime le besoin d'utiliser cette fonction en production, dans ce cas, le filtrage de cette fonction est laissée à la discrétion de l'exploitant.
- **Encapsulated Interface Transport :** Cette fonction permet, d'après les spécifications, d'encapsuler des services à l'intérieur d'une donnée (ou PDU - *Protocol Data Unit*) Modbus. Celle-ci reste néanmoins utilisée pour récupérer des informations sur un équipement à distance via le code de sous-fonction n°12 *ReadDeviceIdentification*. Cette sous-fonction est, entre autres, utilisée par des outils de reconnaissance tels que le script NMAP « modbus-discover.nse ». Cette fonction est utile à un attaquant et ne l'est en aucun cas en production. Elle doit donc être détectée et filtrée.

- **Cas particulier - UMAS :** La fonction 0x5A de Modbus permet l'encapsulation du protocole d'administration propriétaire des équipements de marque Schneider Electric. Cette fonction est utilisée par les équipements d'ingénierie en phase de maintenance, et ponctuellement en production par des équipements Schneider Electric communiquant entre eux (par exemple le terminal ou IHM modèle Magelis avec Automate gamme Modicon). L'utilisation des fonctions UMAS en production est très dangereuse car elle permet un contrôle total sur l'équipement de par ses fonctions d'administration. Il est recommandé de filtrer la fonction 0x5A ou de n'autoriser que les fonctions nécessaires à la communication entre les équipements de marque Schneider.

Attention

L'ensemble des recommandations de filtrage s'applique à un système en production. Lors des phases de maintenance, d'évolution de l'installation ou de MCS, les flux doivent lever une alerte mais ne pas être bloqués.

A.3 Exemple d'implémentation

L'implémentation des règles de filtrage peut se faire via des équipements de filtrage applicatifs tels que des pare-feux implémentant des fonctions de type IPS. Il faudra cependant vérifier que la fonction IPS du pare-feu implémente le protocole Modbus. C'est le cas, par exemple, des pare-feux industriels qualifiés de marque Stormshield. Les fonctions sont décrites en détail dans le guide [4].

A.3.1 Cas d'usage d'un pare-feu STORMSHIELD (SNI)

Information

Les exemples ci-dessous ont été réalisés à partir d'un pare-feu industriel Stormshield (gamme SNI). Les configurations proposées peuvent être réalisées sur d'autres modèles de pare-feu Stormshield en intégrant la licence relative à la prise en charge des protocoles industriels (licence déjà incluse dans la gamme SNI).

Afin d'activer les fonctionnalités de filtrage IPS et IDS sur le pare-feu SNI, il est nécessaire de suivre les étapes ci-dessous :

- **Désactivez l'*anti-spoofing* UNIQUEMENT pendant la phase de mise au point :** La fonctionnalité d'*anti-spoofing* peut poser des problèmes dans l'analyse du fonctionnement des règles de filtrage et induire en erreur l'administrateur lors des tests.
  Dans l'onglet `Protection Applicative` → `Applications et protections`
  modifiez la valeur de la colonne « Action » des règles « IP address spoofing » et « IP address spoofing on bridge » à « Autoriser ».

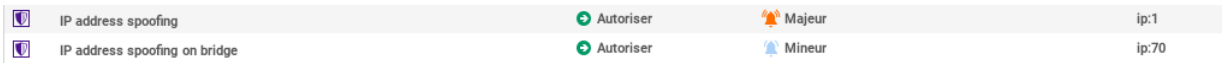

FIGURE 3 – Désactivation de l'*anti-spoofing*

- **Ajoutez une règle Modbus :** Dans l'onglet `Politique de sécurité` → `Filtrage et NAT`, après avoir renseigné la source et la destination, sélectionnez « Modbus » dans la colonne port de destination et « Modbus » dans la colonne protocole.

- **Activez le filtrage Modbus :** Dans la colonne « Action », sélectionnez « passer » et dans la colonne « Etat », sélectionnez « on ».
- **Configurez le profil IPS :** Dans l'onglet `Protection Applicative → Protocoles → Protocoles Industriels → Modbus`, sélectionnez les fonctions à filtrer et passer la colonne « Action » à « Bloquer ».

FIGURE 4 – Blocage d'une fonction Modbus

Attention

N'oubliez pas de vérifier que la case « Désactiver la prévention d'intrusion » est bien décochée.

- **Activez le profil IPS :** Dans l'onglet `Politique de sécurité → Filtrage et NAT`, sélectionnez le profil IPS précédemment configuré (IPS_00 par exemple).

FIGURE 5 – Règle IPS Modbus

- **Validez le bon fonctionnement :** Vérifiez le bon fonctionnement de l'installation puis vérifiez que les règles de filtrage sont effectives en réalisant par exemple un scan applicatif NMAP sur un équipement Modbus via la commande Linux suivante à partir d'une adresse IP autorisée :
  `nmap -Pn -p 502 --script=modbus-discover.nse [ip equipement Modbus]`
  Si le filtrage fonctionne, le scan réalisé avec l'outil NMAP ne doit pas renvoyer d'information sur l'équipement.
  Dans l'onglet `Monitoring → LOGS-JOURNAUX D'AUDIT → Alarmes`,
  vérifiez que les flux ont bien été filtrés et journalisés.
- **Réactivez l'*anti-spoofing* :** Dans l'onglet `Protection Applicative → Applications et protections`, passez la colonne « Action » des règles « IP address spoofing » et « IP address spoofing on bridge » à « Bloquer ».

A.3.2 Cas d'usage sonde Suricata

La sonde de détection Suricata permet de réaliser les fonctions de détection Modbus. Pour cela, il est possible d'utiliser le dissecteur Modbus inclus dans Suricata.

- **Installez et configurez *Suricata* :** Plusieurs systèmes d'exploitation disponibles en source ouverte embarquent la sonde *Suricata* ainsi qu'un ensemble d'outils permettant de tester et vérifier l'application des règles de détection. C'est le cas notamment de *SecurityOnion* et de *SELKS* (ces deux exemples ne sont pas cités à titre de recommandation d'usage mais bien à titre informatif). Nous utiliserons, dans l'exemple suivant, une instance de Suricata en version 7.0.4 directement installée sur une machine Linux. Pour l'installation de Suricata, veuillez suivre la documentation officielle.

- **Vérifiez les paramètres du dissecteur Modbus de Suricata :**
  Cette première étape consiste à vérifier que le dissecteur Modbus est bien configuré et activé dans Suricata.

  Pour cela, éditez le fichier */etc/suricata/suricata.yaml* et vérifiez que les paramètres suivants sont positionnés :

```
suricata :
  config :
    app-layer :
      protocols :
        modbus :
          enabled : 'yes'
          detection-ports :
            dp : 502
```

- **Ajoutez les règles de détection Modbus :**
  À titre d'exemple, nous allons créer une règle permettant de détecter l'utilisation de la fonction *ReportSlaveID* (voir la section A.2 pour la signification du rôle de cette fonction). Pour cela, il est nécessaire d'éditer le fichier */etc/suricata/suricata.yaml*, afin de fournir à Suricata le chemin des fichiers de règles à prendre en compte. Dans notre exemple, nous lui passerons uniquement un fichier de règles nommé *local.rules*. Pour cela, assurez-vous de définir les paramètres suivants :

```
default-rule-path : /opt/suricata/rules
rule-files :
    - local.rules
```

  Créez ensuite un fichier nommé *local.rules* dans le répertoire */opt/suricata/rules/* puis ajoutez la règle suivante dans ce fichier.

```
alert modbus any any -> any 502 (
    modbus: function 17;
    msg :"GTB - Modbus ReportSlaveId function Used, Possible SCAN";
    rev :1; sid :1000017;
)
```

Information

Pour plus d'information sur l'utilisation du dissecteur Modbus de Suricata, vous pouvez consulter la documentation officielle [17].

- **Testez la règle :**
  Exécutez Suricata en écoute sur l'interface de monitoring via la commande suivante :

```
sudo suricata -c /etc/suricata/suricata.yaml -i nom_interface_monitoring
```

  Générez du trafic à partir du script NMAP (voir le modèle de requête précédent) puis vérifiez la levée de l'alerte dans le fichier d'alerte de Suricata via la commande suivante :

```
tail -f /var/log/suricata/eve.json | grep Modbus
```

Annexe B
BACnet : Architecture, détection et filtrage

Information

Si l'architecture de votre réseau GTB/GTC repose uniquement sur des variantes de BACnet différentes de BACnet/IP, telles que BACnet/MS-TP, BACnet/LonTalk, BACnet/ARCnet, **cette annexe ne vous concerne pas**.

B.1 Avant-propos

BACnet/IP est un protocole d'exploitation assurant des besoins de communication métier entre plusieurs composants du système industriels :

- communication entre automates et supervision (IHM locale ou SCADA) ;
- communication entre automates ;
- communication entre automates et entrées/sorties déportées.

Pour cela, BACnet/IP implémente des fonctions permettant d'effectuer des actions sur les équipements de contrôle du système industriel telles que :

- l'accès aux fichiers ;
- l'accès aux objets ;
- l'administration à distance ;
- la gestion des terminaux virtuels ;
- la gestion du routage applicatif propre à BACnet ;
- la gestion de la diffusion et des équipements étrangers (*Foreign-Device*) [7].

Tout comme le protocole Modbus, BACnet n'a pas été conçu avec les problématiques de cybersécurité et, de ce fait, il intègre des fonctions qu'il est recommandé de filtrer et/ou dont l'usage en production doit alerter la supervision.

7. Équipements, disposant des fonctions BACNET/IP, isolés au sein d'un réseau ne comportant pas de BBMD.

B.2 Architecture

Le protocole BACnet/IP utilise la couche de transport UDP ainsi que les mécanismes de diffusion limitée au sous-réseau IP afin de propager, dans certains cas, des messages par *broadcast*. C'est le cas notamment des messages véhiculant les services BACnet : *Who-Is*, *I-Am*, *Who-has* et *You-Are*. Cela pose un problème dans le cadre de cloisonnement logique par VLAN, car un paquet IP avec une adresse diffusion ne sera pas propagé à l'extérieur de son sous-réseau. L'architecture BACnet/IP de base n'est donc pas adaptée à un cloisonnement logique ou physique (voir figure 6).

La figure 6 présente un réseau de supervision (sous-réseau C) connecté à deux réseaux de GTC distincts (sous-réseaux A et B) illustrant la non propagation des messages de diffusion à l'extérieur du sous-réseau.

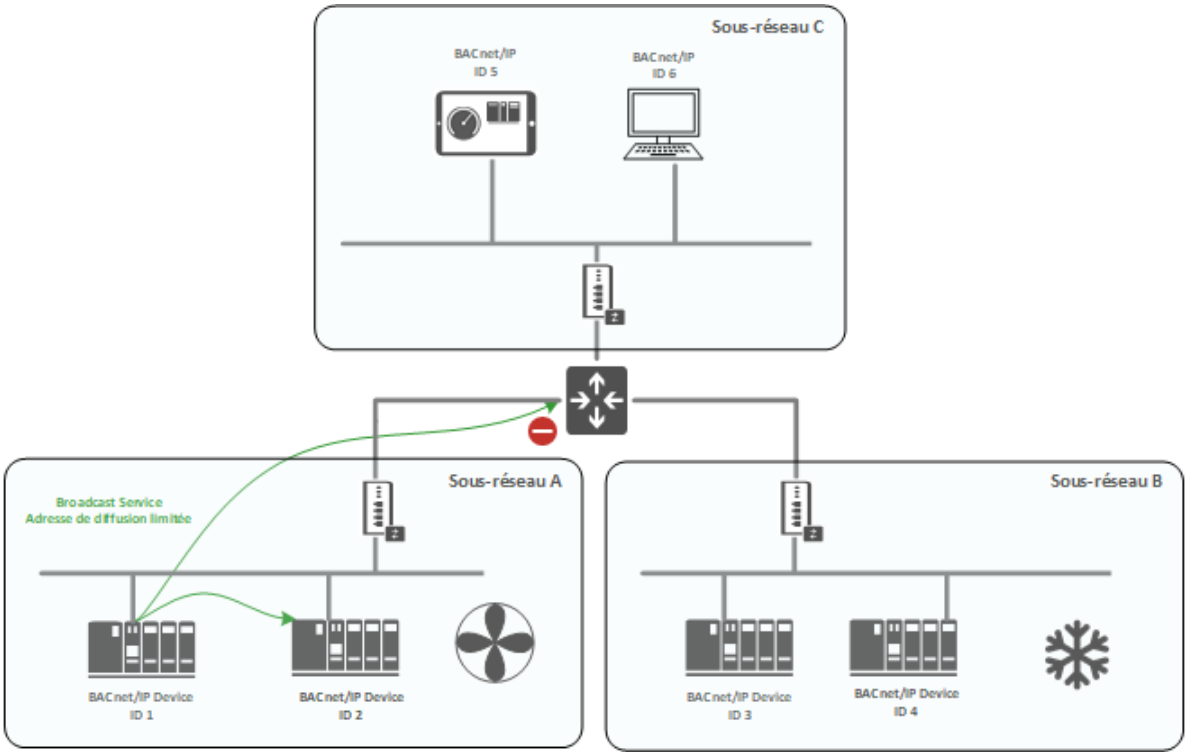

FIGURE 6 – Architecture BACnet/IP sans BBMD

Pour permettre la diffusion des messages de *broadcast*, BACnet/IP introduit le concept de BBMD (BACnet *Broadcast Management Device*) dont le rôle est de retransmettre en *unicast* les messages de *broadcast* à l'ensemble des BBMD présents dans sa table BDT (*Broadcast Distribution Table*). À réception d'un message *unicast* en provenance d'un BBMD distant, le BBMD local va retransmettre le message en *broadcast* à l'ensemble de son sous-réseau tel qu'illustré sur la figure 7 :

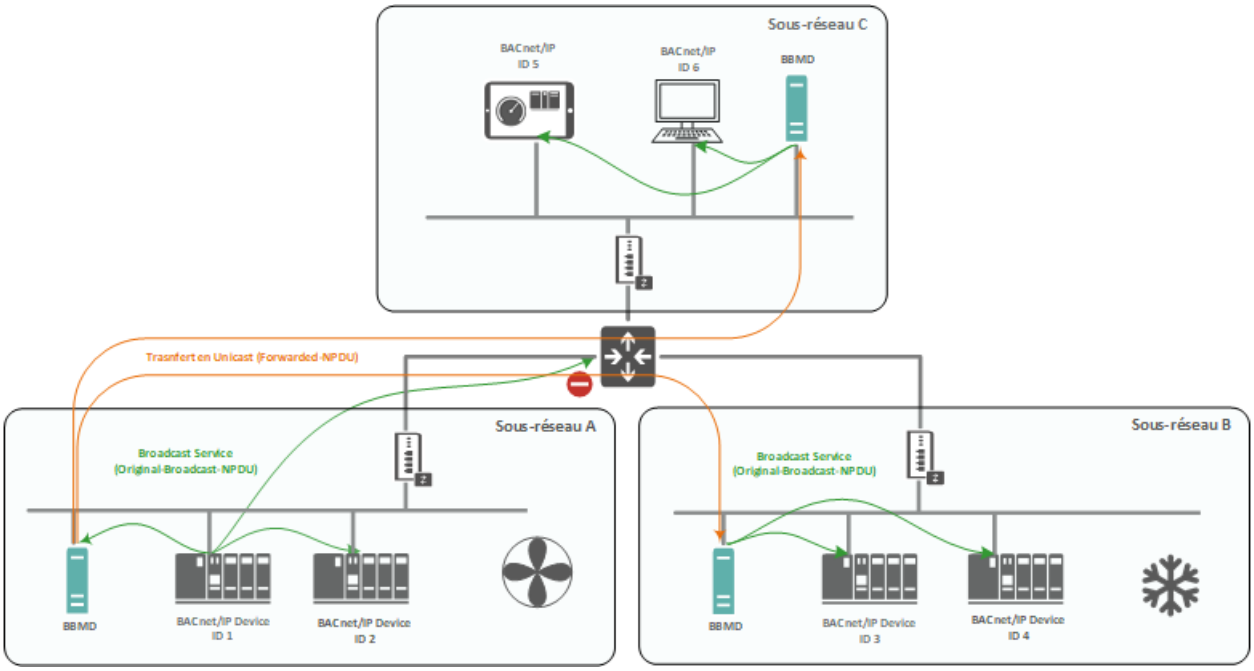

FIGURE 7 – Architecture BACnet/IP avec BBMD

Information

La fonctionnalité de BBMD est souvent incluse dans certains équipements BACnet tels que les automates. Il n'est donc pas toujours nécessaire d'acheter un équipement spécifique pour apporter cette fonction au sein d'un sous-réseau. Pour des raisons pédagogiques, l'architecture de la figure 7 distingue l'équipement assurant le rôle de BBMD comme un équipement à part entière.

Le protocole BACnet introduit également la notion de « *Foreign Device* », qui permet à un équipement « étranger » (équipement disposant des fonctions BACNET/IP, isolé au sein d'un sous-réseau ne comportant pas de BBMD) de rejoindre le réseau BACnet. Pour cela, le « *Foreign Device* » effectue une demande d'enregistrement auprès d'un BBMD dont l'adresse IP est connue à l'avance. Une fois enregistré, le *Foreign Device* reçoit l'ensemble des messages de *broadcast* reçus par le BBMD sur lequel il est enregistré.

Attention

Cette fonctionnalité permettant à un équipement « étranger » de rejoindre un réseau ne doit pas être utilisée car un attaquant pourrait l'implémenter afin de découvrir l'ensemble des équipements du réseau comme présenté sur la figure 8.

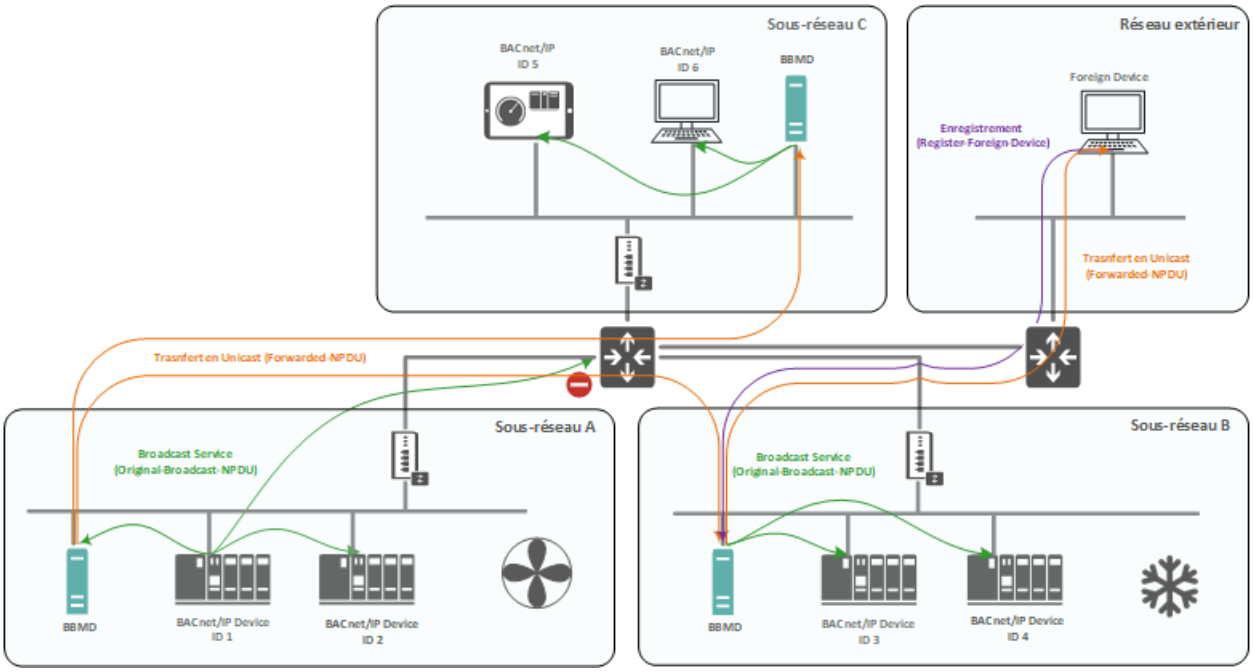

FIGURE 8 – Architecture BACnet/IP avec « *Foreign Device* »

B.3 Recommandation de filtrage et de détection

Le protocole BACnet dispose de trois couches protocolaires :

- **APDU :** *Application Protocol Data Unit* ;
- **NPDU :** *Network Protocol Data Unit* ;
- **BVLC :** BACnet *Virtual Link Control*.

En situation de production, il est recommandé de filtrer et/ou détecter l'utilisation des fonctions propres à chaque couche protocolaire BACnet à l'aide d'un pare-feu et/ou d'un système de détection.

Les tableaux 2 et 3 récapitulent l'application des fonctions de filtrage et de détection sur les fonctions BACnet sur la couche APDU.

Attention

La couche BACnet APDU utilise des services de type *Confirmed* pour ceux nécessitant une confirmation de réception. Des services de type *UnConfirmed* sont utilisés pour ceux ne nécessitant pas de confirmation de réception. Il est donc possible que deux codes de fonction soient identiques mais qu'il ne s'agisse pas du même service (par exemple le code « 9 »).

Code (dec)	Fonction	Action
6	**AtomicReadFile**	**Détecter**
7	**AtomicWriteFile**	**Filtrer**
9	**RemoveListElement**	**Filtrer**
10	**CreateObject**	**Filtrer**
11	**DeleteObject**	**Filtrer**
12	**ReadProperty (ID 4194303)**	**Filtrer**
16	**WritePropertyMultiple**	**Filtrer ou détecter**
17	**DeviceCommunicationControl**	**Filtrer**
18	**ConfirmedPrivateTransfer**	**Détecter**
20	**ReinitializeDevice**	**Filtrer**

TABLE 2 – Filtrage et détection des services *Confirmed* de la couche APDU

Code (dec)	Fonction	Action
4	**UnconfirmedPrivateTransfer**	**Détecter**
7	**TimeSyncrhonization**	**Filtrer**[7]
9	**UTCTimeSynchronization**	**Filtrer**[8]

TABLE 3 – Filtrage et détection des services *UnConfirmed* de la couche APDU

- **AtomicReadFile :** Ce service permet à un utilisateur de consulter, à distance, des fichiers de configuration de l'équipement (service présent sur des automates de marque WAGO par exemple). Son utilisation en production doit être détectée.

8. Cette règle est applicable si le service NTP est activé, conformément à la recommandation R13.

- **AtomicWriteFile :** Ce service permet à un utilisateur d'écrire, à distance, des fichiers de configuration de l'équipement (service présent sur des automates de marque WAGO par exemple). Le service peut mener à une compromission de la configuration de l'équipement. Son utilisation en production doit être détectée et filtrée.
- **ReinitializeDevice :** Ce service permet de réinitialiser la configuration BACnet d'un équipement à distance. Ce service est dédié pour l'administration des équipements et ne doit pas être utilisé en production. Son utilisation doit être détectée et filtrée.
- **RemoveListElement :** Ce service permet à un utilisateur de supprimer un ou plusieurs éléments d'une liste appartenant à une propriété d'un objet BACnet. Ce service peut permettre à un attaquant de modifier un objet BACnet. Son utilisation doit être détectée et filtrée.
- **CreateObject :** Ce service permet à un utilisateur de créer un objet BACnet. Ce service ne devrait pas être utilisé en production dans la mesure où tous les objets BACnet sont déjà définis. Son utilisation doit être détectée et filtrée.
- **DeleteObject :** Ce service permet à un utilisateur de supprimer des objets BACnet existants. Ce service ne devrait pas être utilisé en production car il permet à un attaquant de supprimer des objets et de perturber le fonctionnement de la GTB. Son utilisation doit être détectée et filtrée.
- **ReadProperty (sur l'ID 4194303) :** Chaque équipement BACnet possède un identifiant unique. Cet identifiant est requis par la majorité des services car il permet d'identifier l'équipement cible. La valeur minimale d'un identifiant est 0 et la valeur maximale est 4194303.
  Il existe deux méthodes pour récupérer cet identifiant :
  - La première méthode repose sur l'utilisation des services BACnet *Who-Is/I-Am* qui utilisent le *broadcast* pour requêter l'ensemble du réseau sur une plage d'identifiants donnée. Les équipements recevant la requête *Who-Is* répondront avec le service *I-Am* si leurs identifiants se situent dans la plage indiquée.
  - La deuxième méthode, moins conventionnelle, repose sur l'utilisation du service *ReadProperty*. En effet, chaque équipement BACnet possède un objet nommé *device* regroupant un ensemble de propriétés liées à sa configuration, dont l'identifiant *BACnet ID*. L'utilisation générale du service *ReadProperty* requiert de connaître au préalable cet identifiant. Cependant, il est possible d'utiliser ce service pour récupérer l'identifiant *BACnet ID* de l'équipement en remplaçant, dans la requête, la valeur de l'identifiant maximal possible, soit « 4194303 ».

  La dernière méthode est celle utilisée par les scripts NMAP « BACnet-discover-enumerate.nse » et « bacnet-info.nse ». Ce service sur le *BACnet ID* N°4194303 n'est pas utile en production et doit ainsi être détecté et filtré.
- **WritePropertyMultiple :** Ce service permet à un utilisateur d'effectuer des actions d'écriture sur plusieurs propriétés de plusieurs objets BACnet à la fois. Il est possible que l'exploitant exprime le besoin d'utiliser cette fonction en production, dans ce cas, le filtrage de cette fonction est laissé à la discrétion de ce dernier. Néanmoins, son utilisation doit être détectée.
- **DeviceCommunicationControl :** Ce service permet de couper la communication BACnet d'un équipement. Ce service est très sensible car son utilisation peut provoquer un déni de service sur la GTB. Il ne devrait pas être utilisé dans un système en production, son utilisation doit donc être détectée et filtrée.

- **ReinitializeDevice :** Ce service permet de réinitialiser à distance la configuration BACnet d'un équipement. Ce service est dédié à l'administration des équipements et ne doit donc pas être utilisé en production. Il doit être détecté et filtré.
- **ConfirmedPrivateTransfer / UnConfirmedPrivateTransfer :** Ces services permettent l'utilisation de fonctions propriétaires. Ils peuvent être utilisés à des fins variées propres à chaque installation. Ainsi, leur blocage peut potentiellement provoquer un déni de service sur la GTB dans le cas où ils sont utilisés à des fins d'exploitation. Néanmoins, l'utilisation de ces services en production requiert une attention particulière et doit être détectée.
- **TimeSynchronization / UTCTimeSynchronization :** Ces services permettent de modifier à distance l'heure locale d'un équipement BACnet/IP. Ce service ne devrait pas être utilisé en production dans le cas où un protocole type NTP ou autre protocole de synchronisation horaire est déjà mis en place. En effet, l'utilisation illégitime de ces services peut permettre à un attaquant de modifier l'heure locale d'un équipement, et ainsi perturber le fonctionnement de la GTB, la corrélation de la journalisation, etc.

Le tableau 4 récapitule l'application des fonctions de filtrage et de détection sur les fonctions BACnet sur la couche NPDU.

Code (hex)	Fonction	Action
0x00	Who-Is-Router-To-Network	Filtrer
0x01	Im-Router-To-Network	Filtrer
0x02	I-Could-Be-Router-To-Network	Filtrer
0x03	Reject-Message-To-Network	Filtrer
0x04	Router-Busy-To-Network	Filtrer
0x05	Router-Available-To-Network	Filtrer
0x06	Initialize-Routing-Table	Filtrer
0x07	Initialize-Routing-Table-Ack	Filtrer
0x08	Establish-Connection-To-Network	Filtrer
0x09	Disconnect-Connection-To-Network	Filtrer
0x12	What-Is-Network-Number	Filtrer
0x13	Network-Number-Is	Filtrer

TABLE 4 – Filtrage et détection des services de la couche NPDU

Attention

Le concept de routage dans BACnet n'est pas similaire au routage conventionnel au sens du protocole IP. Il s'agit d'un routage applicatif propre à BACnet permettant de transmettre des données entre « réseaux BACnet » de différents types (BACnet/MS-TP, BACnet/ARCnet etc.) via des routeurs BACnet. Ainsi, un routeur BACnet n'est pas équivalent à un routeur IP.

- **Architecture sans routeur BACnet :** Dans le cas d'une architecture BACnet avec un seul réseau BACnet (sans routeur BACnet), l'ensemble des fonctions de la couche NPDU citées en table 4 ne sont pas utiles car exclusivement réservées aux mécanismes liés aux routeurs BACnet. Ces fonctions doivent être filtrées par un pare-feu.

- **Architecture avec routeur BACnet :** Dans le cas d'une architecture BACnet composée de plusieurs réseaux BACnet (avec routeurs BACnet), aucune fonction de la couche NPDU citée dans le tableau 4 ne doit être filtrée, car le filtrage de ces fonctions pourrait provoquer un dysfonctionnement des mécanismes de routage BACnet et provoquer un déni de service.

Le tableau 5 récapitule l'application des fonctions de filtrage et de détection sur les fonctions BACnet sur la couche BVLC.

Code (hex)	Fonction	Action
0x00	**BVLC-Result**	**Aucune action**
0x01	**Write-Broadcast-Distribution-Table**	**Filtrer**
0x02	**Read-Broadcast-Distribution-Table**	**Filtrer**
0x03	**Read-Broadcast-Distribution-Table-Ack**	**Filtrer**
0x04	**Forwarded-NPDU**	**Aucune action**
0x05	**Register-Foreign-Device**	**Filtrer**
0x06	**Read-Foreign-Device-Table**	**Filtrer**
0x07	**Read-Foreign-Device-Table-Ack**	**Filtrer**
0x08	**Delete-Foreign-Device-Table-Entry**	**Filtrer**
0x09	**Distribute-Broadcast-To-Network**	**Filtrer**
0x0A	**Originial-Unicast-NPDU**	**Aucune action**
0x0B	**Original-Broadcast-NPDU**	**Aucune action**

TABLE 5 – Filtrage et détection des services de la couche BVLC

- **BVLC-Result :** Ces services sont utilisés pour fournir les résultats de la bonne exécution de certains services de la couche BVLC dont l'utilisation est légitime. De ce fait, la fonction *BVLC Result* ne doit pas être filtrée ni détectée.
- **Read/Write-Broadcast-Distribution-Table et Read-Broadcast-Distribution-Ack :** Ces services sont utilisés pour lire et écrire dans la table BDT d'un équipement BBMD. En production, l'ensemble des BDT de chaque BBMD du réseau de la GTB étant déjà configurés, ces services doivent être détectés et filtrés.
- **Forwarded-NPDU :** Ce service est utilisé pour retransmettre en *unicast* aux autres BBMD les messages de *broadcast* reçus par un équipement BBMD au sein de son propre réseau local. En production, ce service est massivement utilisé dès lors qu'une requête utilisant le *broadcast*, tel que *Who-Is / I-Am*, est envoyée par un équipement. Ce service **ne doit donc pas** être filtré et a peu d'intérêt à être détecté.
- **Register-Foreign-Device :** Ce service est utilisé par les équipements « étrangers » pour s'enregistrer dans la FDT d'un BBMD afin de pouvoir recevoir les messages de *broadcast*. En complément de la recommandation R7, ce service doit être détecté et filtré.
- **Read-Foreign-Device-Table et Read-Foreign-Device-Ack :** Ces services sont utilisés pour lire et acquitter le contenu de la FDT d'un BBMD. Ces services ne sont pas utiles en production et doivent être détectés et filtrés. Néanmoins, dans un contexte de détection avancée, il peut s'avérer utile d'autoriser l'utilisation de ces services par un équipement de *monitoring* afin de vérifier périodiquement que le contenu de la table FDT de chaque BBMD est bien vide.

- **Delete-Foreign-Device-Table-Entry :** Ce service est utilisé pour supprimer une entrée dans la table FDT d'un BBMD. Ce service doit être détecté et filtré.
- **Distribute-Broadcast-To-Network :** Ce service est utilisé par les *Foreign Devices* pour transmettre des messages de *broadcast* aux autres équipements BACnet/IP. En complément de la recommandation R7, ce service doit être détecté et filtré.

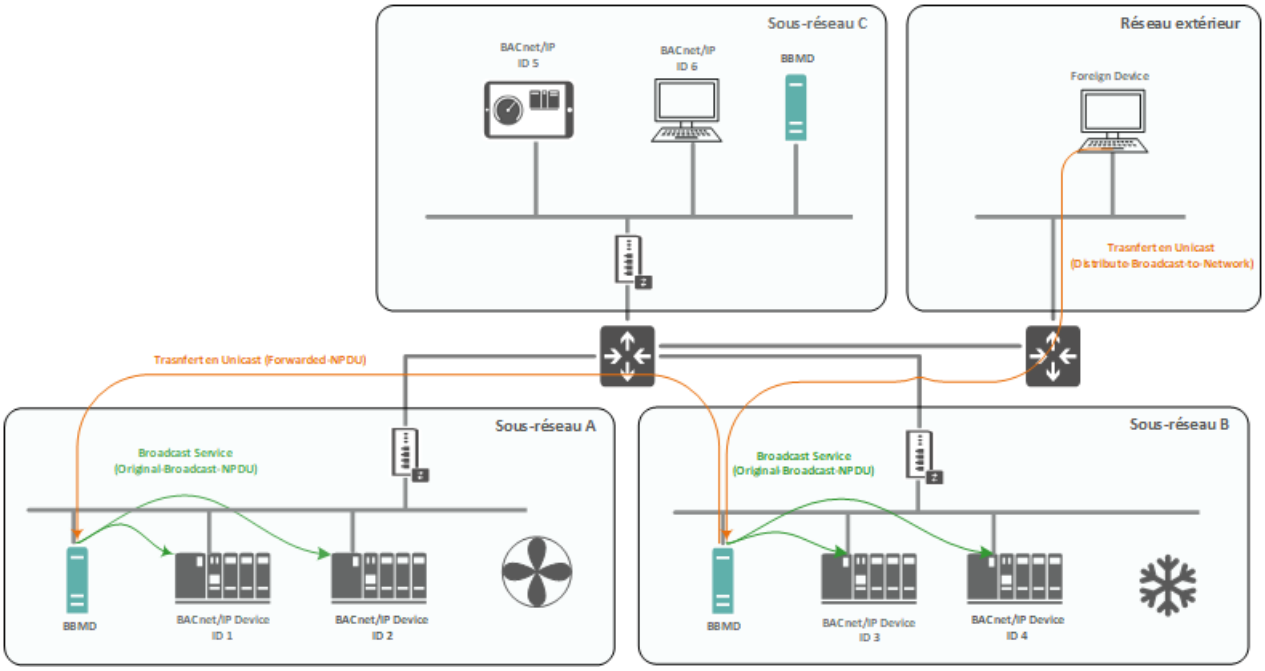

FIGURE 9 – Distribution d'un broadcast par un *Foreign Devices*

- **Original-Unicast-NPDU :** Ce service est utilisé par les équipements BACnet pour transmettre des messages en *unicast* aux autres équipements BACnet. Ce service est massivement utilisé en production car la plupart des services de la couche APDU l'utilise. Ce service **ne doit pas** être filtré ou détecté.
- **Original-Broadcast-NPDU :** Ce service est utilisé par les équipements BACnet et les routeurs BACnet pour envoyer des messages en *broadcast* aux autres équipements BACnet qui ne sont pas des *Foreign Devices*. Ce service est massivement utilisé en production car la plupart des services de la couche APDU l'utilisent. Ce service **ne doit pas** être filtré ou détecté.

B.4 Exemple d'implémentation

B.4.1 Cas d'usage APDU sur un pare-feu STORMSHIELD (SNI)

Information

L'implémentation des règles de filtrage applicatif de la couche APDU du protocole BACnet/IP est possible avec la version **4.3.x**. Les règles pour les couches BVLC et NPDU sont disponibles à partir de la version **5.0**.

Afin d'activer les fonctionnalités de filtrage IPS et IDS sur le pare-feu SNI, il est nécessaire de suivre les étapes ci-dessous :

- **Désactivez l'*anti-spoofing* UNIQUEMENT pendant la phase de mise au point :** La fonctionnalité d'*anti-spoofing* peut poser des problèmes dans l'analyse du fonctionnement des règles de filtrage et induire en erreur l'administrateur lors des tests.
  Dans l'onglet `Protection Applicative → Applications et protections;`
  modifiez la valeur de la colonne « Action » des règles « IP address spoofing » et « IP address spoofing on bridge » à « Autoriser ».

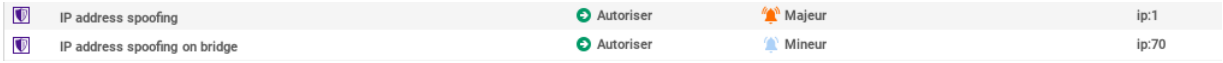

FIGURE 10 – Désactivation de l'anti-spoofing

- **Ajoutez une règle BACnet/IP :** Dans l'onglet `Politique de sécurité → Filtrage et NAT`, après avoir renseigné la source et la destination, sélectionnez « BACnet/IP » dans la colonne port de destination et « BACnet/IP » dans la colonne protocole.
- **Activez le filtrage BACnet/IP :** Dans la colonne « Action », sélectionnez « passer » et dans la colonne « Etat », sélectionnez « on ».
- **Configurez le profil IPS :** Dans l'onglet `Protection Applicative → Protocoles → Protocoles Industriels → BACnet/IP → → onglet Gestion des services;`
  Sélectionnez les fonctions à filtrer et passez la colonne « Action » à « Bloquer ».

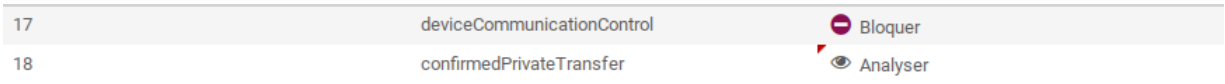

FIGURE 11 – Blocage d'une fonction BACnet/IP

Attention

N'oubliez pas de vérifier que la case « Désactiver la prévention d'intrusion » est bien décochée.

- **Activez le profil IPS :** Dans l'onglet `Politique de sécurité → Filtrage et NAT;`
  Sélectionnez le profil IPS précédemment configuré (IPS_00 par exemple).

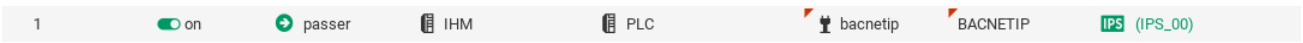

FIGURE 12 – Règle IPS BACnet/IP

- **Validez le bon fonctionnement :** Vérifiez le bon fonctionnement de l'installation, puis vérifiez que les règles de filtrage sont effectives en réalisant par exemple un scan applicatif NMAP sur un équipement BACnet/IP via la commande Linux suivante, à partir d'une adresse IP autorisée :
  `nmap -Pn -sU -p 47808 --script=bacnet-info.nse [ip equipement BACnet/IP]`
  Si le filtrage fonctionne, le scan utilisé avec l'outil NMAP ne doit pas renvoyer d'information sur l'équipement.
  Dans l'onglet `Monitoring → LOGS-JOURNAUX D'AUDIT → Alarmes;`
  Vérifiez que les flux ont bien étés filtrés et journalisés.

- **Réactivez l'*anti-spoofing* :** Dans l'onglet `Protection Applicative → Applications et protections;` Passez la colonne « Action » des règles « IP address spoofing » et « IP address spoofing on bridge » à « Bloquer ».

B.4.2 Cas d'usage NPDU sur un pare-feu STORMSHIELD (SNI)

Information

L'implémentation des règles de filtrage applicatif de la couche APDU du protocole BACnet/IP est possible avec la version **4.3.x**. Les règles pour les couches BVLC et NPDU sont disponibles à partir de la version **5.0**.

- Ajoutez et activez une règle comme précisé au chapitre précédent B.4.1.
- **Configurez le profil IPS :** Dans l'onglet `Protection Applicative → Protocoles → Protocoles Industriels → BACnet/IP → → FONCTIONS NPDU;`
  Sélectionnez les fonctions à filtrer (selon le tableau 4) et passez la colonne « Action » à « Interdire ».

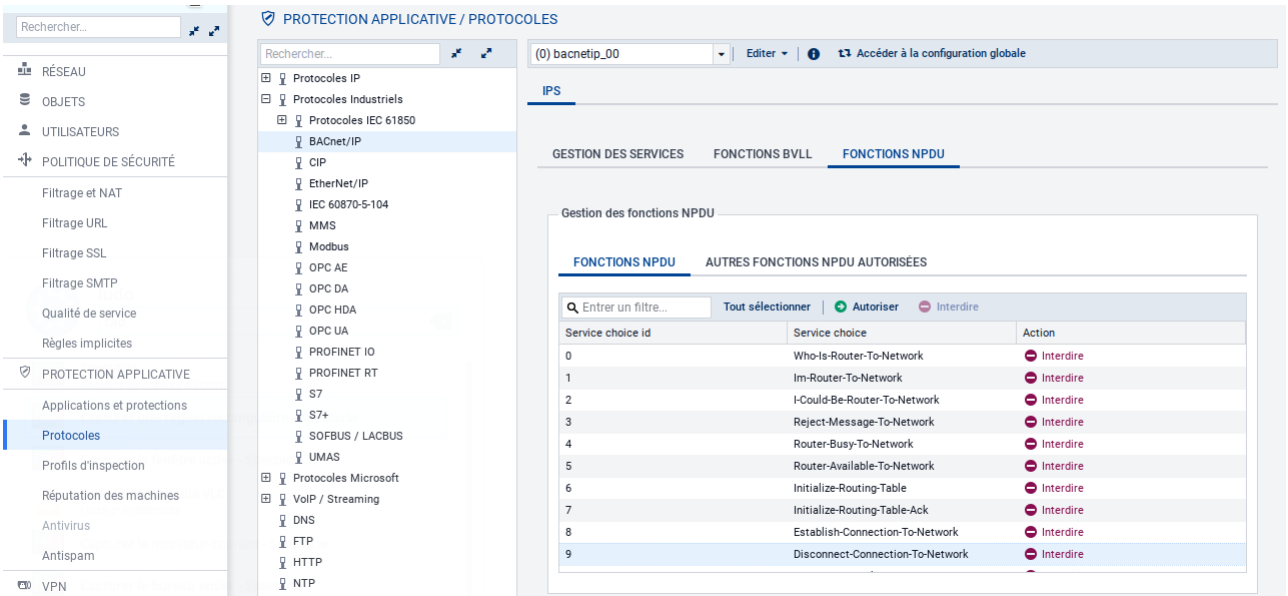

FIGURE 13 – Blocage d'une fonction NPDU de BACnet/IP

Attention

N'oubliez pas de vérifier que la case « Désactiver la prévention d'intrusion » est bien décochée.

- **Activez le profil IPS :** Dans l'onglet `Politique de sécurité → Filtrage et NAT;`
  Sélectionnez le profil IPS précédemment configuré (IPS_00 par exemple).

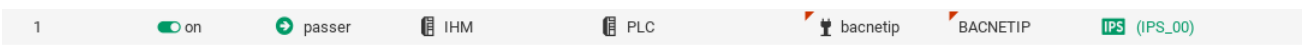

FIGURE 14 – Règle IPS BACnet/IP

B.4.3 Cas d'usage BVLC sur un pare-feu STORMSHIELD (SNI)

Information

L'implémentation des règles de filtrage applicatif de la couche APDU du protocole BACnet/IP est possible avec la version **4.3.x**. Les règles pour les couches BVLC et NPDU sont disponibles à partir de la version **5.0**.

- Ajoutez et activez une règle comme précisé au chapitre précédent B.4.1.
- **Configurez le profil IPS :** Dans l'onglet `Protection Applicative → Protocoles → Protocoles Industriels → BACnet/IP → → FONCTIONS BVLL;`
  Sélectionnez les fonctions à filtrer (selon le tableau 5) et passez la colonne « Action » à « Interdire ».

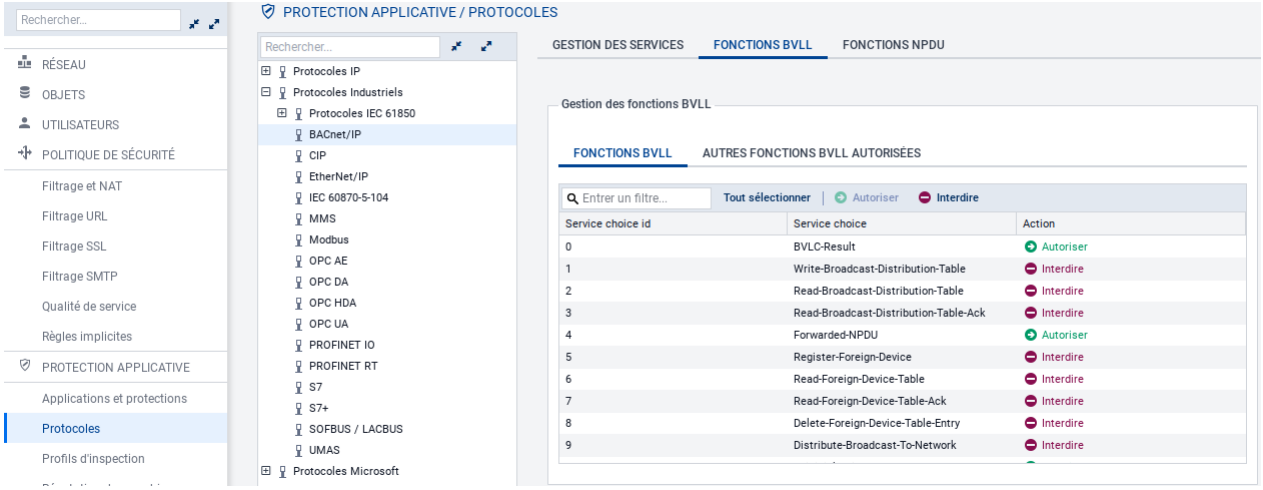

FIGURE 15 – Blocage d'une fonction BVLC de BACnet/IP

Attention

N'oubliez pas de vérifier que la case « Désactiver la prévention d'intrusion » est bien décochée.

- **Activez le profil IPS :** Dans l'onglet `Politique de sécurité → Filtrage et NAT;`
  Sélectionnez le profil IPS précédemment configuré (IPS_00 par exemple).

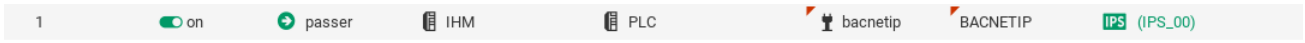

FIGURE 16 – Règle IPS BACnet/IP

B.4.4 Cas d'usage d'une sonde Suricata

La sonde de détection Suricata n'intègrant à ce jour pas de dissecteur BACnet, la mise en œuvre des règles de détection pour BACnet/IP implique l'utilisation de la valeur des codes de fonction relatifs à chaque couche BACnet/IP.

Attention

La taille de la charge utile des datagrammes UDP étant dépendante des messages BACnet/IP, la position du code de fonction peut varier. Il est donc nécessaire de créer un jeu de règles par couche et de définir des règles au cas par cas.

Information

Le positionnement des sondes de détection dans l'architecture de la GTB/GTC n'est pas traitée dans ce document. Veuillez vous référer au guide traitant de la détection pour les systèmes industriels [9] pour plus d'informations.

- **Installez et configurezSuricata :** Plusieurs systèmes d'exploitation disponibles en source ouverte embarquent la sonde Suricata ainsi qu'un ensemble d'outils permettant de tester et de vérifier l'application des règles de détection. C'est le cas notamment de *SecurityOnion* et de *SELKS*. Par souci de simplicité, nous utiliserons dans l'exemple suivant une instance de Suricata en version 7.0.4 directement installée sur une machine Linux. Pour l'installation de Suricata, veuillez suivre la documentation officielle.

- **Ajoutez les règles de détection BACnet/IP :** À titre d'exemple, nous allons maintenant créer une règle permettant de détecter l'utilisation de la fonction de la couche APDU nommée *AtomicReadFile*. Pour cela, il est nécessaire d'éditer le fichier */etc/suricata/suricata.yaml*, afin de fournir à Suricata le chemin des fichiers de règles à prendre en compte. Dans notre exemple, nous lui passerons uniquement un fichier de règles nommé *local.rules*. Pour cela, assurez-vous de définir les paramètres suivants :

```
default-rule-path : /opt/suricata/rules
rule-files :
    - local.rules
```

  Créez ensuite un fichier nommé *local.rules* dans le répertoire */opt/suricata/rules/* puis ajoutez la règle suivante dans ce fichier :

```
alert udp any 47808 <> any any (
    msg :"GTB - BACnet/IP APDU AtomicReadFile Function Used";
    content :"|81 0A|"; startswith ;
    content :"|04 00|"; offset :5; depth :2;
    content :"|6|"; offset :9; depth :1;
    rev :1; sid :10000106;
)
```

- **Testez la règle :** Exécutez Suricata en écoute sur l'interface de *monitoring* via la commande suivante :

```
sudo suricata -c /etc/suricata/suricata.yaml -i nom_interface_monitoring
```

  Générez du trafic impliquant la fonction AtomicReadFile à l'aide d'un client BACnet/IP, puis vérifiez la levée de l'alerte dans le fichier d'alerte de Suricata via la commande suivante :

```
tail -f /var/log/suricata/eve.json | grep BACnet/IP
```

Liste des recommandations

Bibliographie

[1] *Recommandations de configuration matérielle de postes clients et serveurs x86*.
Note technique DAT-NT-024/ANSSI/SDE/NP v1.0, ANSSI, mars 2015.
https://cyber.gouv.fr/publications/recommandations-de-configuration-materielle-de-postes-clients-et-serveurs-x86.

[2] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://cyber.gouv.fr/guide-commutateurs.

[3] *Recommandations de configuration des commutateurs et pare-feux Hirschmann*.
Guide ANSSI-BP-033 v1.1, ANSSI, juillet 2017.
Diffusion Restreinte.

[4] *Recommandations de sécurisation d'un pare-feu Stormshield Network Security (SNS) en version 3.7.17*.
Guide ANSSI-BP-031 v3.0, ANSSI, avril 2021.
https://cyber.gouv.fr/guide-sns.

[5] *Recommandations de configuration des commutateurs et pare-feux Hirschmann*.
Guide ANSSI-BP-033 v1.3, ANSSI, février 2022.
https://cyber.gouv.fr/guide-commutateurs-hirschmann.

[6] *Recommandations de configuration des commutateurs et pare-feux Siemens Scalance*.
Guide ANSSI-BP-094 v1.0, ANSSI, février 2022.
https://cyber.gouv.fr/guide-commutateurs-siemens.

[7] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://cyber.gouv.fr/hygiene-informatique.

[8] *Recommandations de sécurité relatives aux réseaux Wi-Fi*.
Note technique DAT-NT-005/ANSSI/SDE/NP v1.0, ANSSI, septembre 2013.
https://cyber.gouv.fr/guide-wifi.

[9] *Doctrine de détection pour les systèmes industriels*.
Guide ANSSI-PA-084 v1.0, ANSSI, décembre 2020.
https://cyber.gouv.fr/doctrine-detection-si-indus.

[10] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[11] *Sécurité des (systèmes d')objets connectés*.
Guide ANSSI-PA-087 v1.0, ANSSI, juillet 2021.
https://cyber.gouv.fr/guide-iot.

[12] *Recommandations de sécurité pour l'architecture d'un système de journalisation*.
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
https://cyber.gouv.fr/guide-journalisation.

[13] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[14] *Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés)*.
Guide ANSSI-PG-076 v1.0, ANSSI, juillet 2020.
https://cyber.gouv.fr/publications/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies.

[15] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[16] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[17] *Documentation Modbus Suricata*.
Page web, Suricata.
https://docs.suricata.io/en/latest/rules/modbus-keyword.html.

Version 1.0 - 27/04/2026 - ANSSI-PA-110

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité