RECOMMANDATIONS DE CONFIGURATION DES COMMUTATEURS ET PARE-FEUX SIEMENS SCALANCE

GUIDE ANSSI

ANSSI-BP-094
11/02/2022

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations de configuration des commutateurs et pare-feux SIEMENS SCALANCE »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Sauf disposition réglementaire contraire, ces 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	11/02/2022	Version initiale

Table des matières

1 Introduction

1.1 Objectif du guide

Ce document présente les bonnes pratiques relatives à la sécurisation des commutateurs et des pare-feux de la marque *SIEMENS*, gamme *SCALANCE*. Autant que possible, les explications et recommandations contenues dans ce document sont auto-porteuses afin d'éviter au lecteur de devoir à consulter des références externes. Sur les sujets plus généraux, les explications seront plus concises et viendront en complément des publications de l'ANSSI.

1.2 Convention de lecture

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 la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

Les recommandations ont été formulées à partir de modèles de commutateurs `X310`, `XB208`, `XC216` et `XM408`, et d'un pare-feu `S615`. Les versions des équipements sont mentionnées dans le tableau ci-contre.

Type d'équipement	Version du micrologiciel
`X310`	4.1.3
`XB208` et `XC216`	4.2.0
`XM408`	6.3.1
`S615`	6.2.0

TABLE 1 – Versions logicielles des équipements testés

Information

Ces recommandations sont également valables pour les produits listés dans l'annexe A. En effet, pour un type de produit, une même version de micrologiciel est utilisée pour une gamme complète (seule la partie matérielle est différente et/ou des fonctionnalités (dés)activées).

Les équipements concernés par le présent document sont généralement dédiés pour les cas d'usage décrits ci-après (données fournies par le constructeur) :

- `XB208` : commutateur industriel équipé de 8 ports 100Mb/s. Cet équipement est généralement utilisé sur des réseaux d'automates dits de *process* ou des réseaux dits de « terrain » (raccordement des modules d'entrées/sorties) pour des petites installations. Pas de module optique ni de fonction de routage sur cet équipement ;
- `XC216` : commutateur industriel équipé de 16 ports cuivres 1Gb/s et 4 ports optiques. Cet équipement est généralement utilisé sur des réseaux d'automates dits de *process* y compris des installations déportées (cas des automates dits de terrain) ou sur des points de convergence de flux (flux automates et flux SCADA). Pas de module optique ni de fonction de routage sur cet équipement ;
- `X310` : commutateur industriel équipé de 10 ports cuivres 1Gb/s. Cet équipement est remplacé progressivement par la gamme XC des commutateurs (XC216 par exemple) ;
- `XM408` : commutateur industriel équipé de 8 ports cuivres 1Gb/s et 4 ports optiques. Cet équipement est généralement utilisé sur des réseaux d'automates dits de *process* y compris des installations déportées (cas des automates dits de terrain) ou sur des points de convergence de flux (flux automates et flux SCADA). Cet équipement inclus également des fonctions de routage. Il peut ainsi être utilisé en frontière vers un site distant (avec un pare-feu) ;
- `S615` : pare-feu industriel (disposent de fonctions NAT, PAT et tunnel IPsec). Cet équipement est utilisé, entre autres fonctionnalités, pour la protection d'automates d'un site distant par exemple, le cloisonnement de réseau de niveaux de criticité différents ou à la frontière entre les automates dits de *process* et le réseau SCADA (positionné en tête de ligne). Il est également utilisé pour sécuriser les liaisons de données avec des équipements distants.

Chaque système d'information (SI) étant unique, il est nécessaire d'adapter les configurations données en exemple dans ce document aux particularités du SI considéré. Une application des configurations sans compréhension préalable de leurs impacts sur le fonctionnement des équipements peut conduire à des indisponibilités du SI. Il est donc nécessaire de tester les recommandations avant toute modification de la configuration d'équipements en production.

Information

L'hypothèse principale prise en compte lors de la rédaction de ce guide est que seules les personnes autorisées disposent d'un accès physique aux équipements. La mise en œuvre sécurisée des systèmes de contrôle d'accès physique et de vidéoprotection est détaillée dans le guide [9].

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [1], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

La liste récapitulative des recommandations est disponible en page 66.

1.3 Liste des sigles et acronymes

- **AAA** : *Authentication, Authorization, Accounting*. Protocole d'authentification, d'autorisation et de traçabilité.
- **ACL** : *Access Control List*. Filtrage de protocoles ou de services suivant des conditions définies par l'administrateur de l'équipement.
- **API** : *Automate programmable industriel*. Il s'agit d'un équipement disposant d'un ensemble d'entrées/sorties électriques sur lesquelles sont raccordées des capteurs et actionneurs et qui exécute un programme de façon cyclique afin de piloter un procédé industriel.
- **BPDU** : *Bridge Protocol Data Unit*. Trame de données transportant les informations de topologie STP.
- **CLI** : *Command Line Interface*. Interface avec l'équipement proposée en ligne de commande.
- **Client** : élément de confiance d'un réseau 802.1X servant de point d'accès au réseau (commutateur, point d'accès wifi, etc.).
- **DDoS** : *Distributed Deny of Service*. Attaques par déni de service distribué.
- **EAP** : *Extended Authentication Protocol*. Protocole réseau permettant d'abstraire le mécanisme d'authentification spécifique utilisable.
- **ETHERNET** : *Norme ISO 8802-3*. Protocole de réseau local à commutation de trames.
- **GARP** : *Generic Attribute Registration Protocol*. Protocole d'enregistrement fournissant une architecture dynamique pour les commutateurs, par exemple l'enregistrement de VLAN.
- **GVRP** : *GARP VLAN Registration Protocol*. Protocole d'enregistrement dynamique de VLAN par le biais du protocole GARP.
- **IGC** : *Infrastructure de Gestion de Clefs*. Procédures et composants électroniques et informatiques assurant la gestion des certificats électroniques d'une entité.
- **LLDP** : *Link Layer Discovery Protocol*. Protocole permettant la découverte de topologie réseau.
- **MRP** : *Media Redundancy Protocol*. Protocole industriel permettant de déterminer une topologie de niveau 2 sans boucle.
- **NTP** : *Network Time Protocol*. Protocole permettant la synchronisation horaire d'un ou plusieurs équipements à partir d'une source de temps de référence.
- **OSI** : *Open Systems Interconnection*. Modèle de communication entre systèmes informatiques.

1. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [7].

- **RADIUS** : *Remote Authentication Dial-In User Service*. Serveur central d'authentification.
- **RMON** : *Remote MONitoring*. Extension du protocole SNMP qui permet de transmettre, sur demande, vers un serveur centralisé, des informations relatives aux différentes couches du modèle OSI (1 et 2 pour RMON1 et couches 3 à 7 pour RMON2). Il peut s'agir, par exemple des statistiques relatives au nombre de paquets reçus et émis, des paquets supprimés, des erreurs dans les trames, des applications selon le protocole utilisé, etc. Il est également possible de transmettre les métas données des captures de trames réseau (taille des paquets, entête, protocoles, etc.).
- **SCADA** : *Supervisory Control And Data Acquisition*. Ensemble de moyens informatiques permettant aux opérateurs et techniciens la supervision fonctionnelle et le contrôle, à distance ou localement, des installations techniques d'un ou plusieurs sites.
- **TCN** : *Topology Change Notification*. Trame permettant de notifier un changement de topologie du réseau aux différents équipements constituant la boucle *Spanning Tree*.
- **VLAN** : *Virtual Local Area Network*. Réseau logique de niveau 2.
- **VPN** : *Virtual Private Network*. Réseau privé virtuel, chiffré ou non, constitué d'un groupe d'utilisateurs restreints.

2
Menaces et objectifs des attaquants

Les systèmes industriels sont de plus en plus la cible d'attaquants. Les problèmes de disponibilité (du simple ralentissement à l'interruption de service) peuvent avoir des conséquences lourdes tant humainement que financièrement.

Les menaces les plus connues pesant sur les sites industriels sont la compromission des ressources, le vol de données et le déni de service.

La transition vers l'industrie du futur présente plusieurs risques en cybersécurité :

- l'utilisation de protocoles non ou mal sécurisés offre à un attaquant la possibilité de modifier ou forger des trames, ou de récupérer des identifiants de connexion circulant en clair sur le réseau ;
- l'augmentation du volume d'information transportable par les réseaux peut engendrer des difficultés à contrôler les valeurs acceptables et ainsi autoriser des attaques de type *buffer overflow* (débordement de tampon) ou DDoS ;
- les technologies sans fil utilisées sans mesures de protection exposent les systèmes industriels à des problèmes de disponibilité d'avantage que les infrastructures filaires (brouillage de signaux) et facilitent les compromissions (injection de trafic malveillant, modification de trames) ;
- les équipements et protocoles « historiques » qui étaient isolés physiquement (*air gap*) sont désormais accessibles par l'intermédiaire d'autres équipements connectés au réseau bureautique, directement ou via une passerelle de communication.

Les attaques informatiques majeures contre des systèmes industriels ont été exécutées en exploitant spécifiquement les protocoles ou solutions en usage dans l'entité victime, démontrant une phase de reconnaissance importante du système d'information de la cible choisie. La plupart des attaques sur des architectures de systèmes industriels ont été motivées par une intention de sabotage. Les motivations secondaires ont été l'espionnage et le vol de données.

La protection contre ces menaces passe à la fois par la sécurisation des automates (API), lorsque des fonction de sécurité sont disponibles, mais aussi par la sécurisation des infrastructures périmétriques comme les commutateurs et pare-feu.

3
Administration

Comme pour tout équipement réseau déployé dans un SI, l'administration des commutateurs et des pare-feux doit se faire en respectant un certain nombre de recommandations de sécurité.

Objectif

Sécuriser et maîtriser les accès au réseau d'administration, séparer ce dernier des autres réseaux de l'équipement.

3.1 Réseau dédié à l'administration

Pour des questions de sécurité, il est conseillé de mettre en place un réseau dédié aux flux d'administration des équipements du SI, distinct des réseaux de données utilisés par les services métier (se référer au guide de l'ANSSI [6] pour plus d'informations).

3.1.1 Port physique dédié à l'administration

Il est préférable d'utiliser un port physique dédié à l'administration des équipements type commutateur et pare-feu, lorsque cela est possible, afin de ne pas mélanger les flux d'administration et les flux métier. Cette pratique paraît d'autant plus aisée à réaliser que les commutateurs disposent, en général, d'un nombre important de ports physiques.

R1

Dédier un port à l'administration

Il est recommandé de dédier une interface physique du commutateur ou pare-feu à son administration.

3.1.2 Réseau spécifique

Afin de procéder à une séparation entre le réseau d'administration et les autres réseaux, plusieurs techniques peuvent être mises en œuvre. La méthode idéale consiste à utiliser un réseau physique dédié. Cependant, si cela n'est pas possible, une séparation logique peut être envisagée mais constitue une solution moins robuste que l'utilisation d'un réseau physique dédié.

R2

Créer un réseau d'administration physiquement dédié

Il est recommandé de mettre en place une séparation physique entre les réseaux d'administration et les réseaux métier.

R2 -

Créer un réseau d'administration logiquement dédié

Si une séparation physique est impossible, une séparation logique, utilisant, par exemple, les VLAN, peut-être envisagée sous réserve de respecter les recommandations du guide de l'ANSSI [6].

Des explications plus approfondies sur la configuration des VLAN se trouvent à la section 4.1.

3.2 Accès aux interfaces d'administration

L'interface physique ou logique d'administration est clairement identifiée au niveau de l'interface de programmation et permet de configurer une seule adresse IP d'administration.

R3

Configurer une adresse IP d'administration statique

Il est recommandé de configurer une adresse IP d'administration statique.

Par défaut, l'attribution de l'adresse d'administration est réalisée dynamiquement par les protocoles `BootP/DHCP` [2].

L'adresse IP attribuée est définie à partir du serveur `BootP/DHCP` [3].

Information

Il est nécessaire de vérifier la désactivation [4] du protocole DHCP avant d'attribuer une adresse IP à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent` → `Agent Enabled Features`. Décocher la case `DHCP` ou `BootP`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `Configuration`. Décocher la case `DHCP Client`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 3 (IPv4)` → `Subnets` → onglet `Configuration`, sélectionner le VLAN d'administration et décocher la case `DHCP`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 3 (IPv4)` → `Subnets` → onglet `Configuration`, sélectionner le VLAN d'administration (la mise en œuvre du

2. Pour l'équipement `S615`, les protocoles `BOOTP/DHCP` ne sont pas activés. En effet, une adresse IP fixe externe et une adresse IP fixe interne sont configurées par défaut sur l'équipement.
3. Il existe d'autres façons d'attribuer une adresse IP sur les équipements (avec l'application *TIA PORTAL*, avec *Primary setup Tool* ou en ligne de commande pour le matériel équipé d'un port série).

VLAN d'administration est décrite au chapitre 4.1) et décocher la case DHCP. Valider la saisie en appuyant sur le bouton Set Values.

L'adresse IP se configure à partir du menu suivant :

- **pour l'équipement** X310, Agent → Agent IP Configuration.
- **pour l'équipement** XB208, Layer 3 (IPv4) → Subnets → onglet Overview. Sélectionner, dans la liste déroulante, le VLAN d'administration précédemment créé et appuyer sur le bouton Create. A partir de l'onglet Configuration du même menu, sélectionner le VLAN d'administration et attribuer une adresse IP et un masque de sous-réseau. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XC216, Layer 3 (IPv4) → Subnets → onglet Overview. Sélectionner, dans la liste déroulante, le VLAN d'administration précédemment créé et appuyer sur le bouton Create. A partir de l'onglet Configuration du même menu, sélectionner le VLAN d'administration et attribuer une adresse IP et un masque de sous-réseau. Cocher la case TIA Interface[5]. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XM408, Layer 3 (IPv4) → Subnets → onglet Overview. Sélectionner, dans la liste déroulante, le VLAN d'administration précédemment créé et appuyer sur le bouton Create. A partir de l'onglet Configuration du même menu, sélectionner le VLAN d'administration et attribuer une adresse IP et un masque de sous-réseau. Cocher la case TIA Interface. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** S615, Layer 3 (IPv4) → Subnets → onglet Overview. Sélectionner, dans la liste déroulante, le VLAN d'administration précédemment créé et appuyer sur le bouton Create. A partir de l'onglet Configuration du même menu, sélectionner le VLAN d'administration et attribuer une adresse IP et un masque de sous-réseau. Cocher la case TIA Interface. Valider la saisie en appuyant sur le bouton Set Values ;

Plusieurs services sont disponibles pour administrer les équipements (en ligne de commande ou à partir d'une interface *WEB*). Tous ne permettent cependant pas d'obtenir le même niveau de sécurité.

R4

Sécuriser les protocoles d'administration distante

Il est recommandé d'activer uniquement les services SSH et HTTPS et de désactiver les protocoles HTTP et TELNET pour l'administration distante des équipements.

Pour chaque équipement, le menu à utiliser est le suivant :

- **pour l'équipement** X310, Agent → Agent Enabled Features. Décocher la case TELNET et cocher la case HTTPS only. Vérifier que le protocole SSH est activé (case SSH cochée par défaut). Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XB208, System → Configuration. Décocher la case TELNET et cocher la case HTTPS Server only. Vérifier que le protocole SSH est activé (case SSH cochée par défaut). Valider la saisie en appuyant sur le bouton Set Values ;

4. Il est possible d'activer ou désactiver le service DHCP de façon globale sur l'équipement, ou uniquement sur un ou plusieurs VLAN. La méthode décrite dans ce chapitre présente la désactivation globale.

5. Cette option correspond à l'affectation de la découverte réseau par le protocole PNIO-DCP dans le VLAN concerné. L'activation de cette option est imposée par le micrologiciel dans le VLAN d'administration.

- **pour l'équipement** `XC216`, `System` → `Configuration`. Décocher la case `TELNET` et cocher la case `HTTPS Server only`. Vérifier que le protocole SSH est activé (case `SSH` cochée par défaut). Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `Configuration`. Décocher la case `TELNET` et cocher la case `HTTPS Server only`. Vérifier que le protocole SSH est activé (case `SSH` cochée par défaut). Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `Configuration`. Dans la liste déroulante `HTTP Services`, sélectionner le paramètre `HTTPS`. Décocher la case `TELNET`. Vérifier que le protocole SSH est activé (case `SSH` cochée par défaut). Valider la saisie en appuyant sur le bouton `Set Values`.

Pour l'équipement `S615`, il est possible d'activer ou désactiver des services dans un VLAN particulier à partir du menu suivant : `Security` → `Firewall` onglet `Predefined IPv4`.

R5

Autoriser uniquement les flux nécessaires par des règles de filtrage

Il est recommandé de désactiver les services de manière globale à partir du menu `Security` → `Firewall` onglet `Predefined IPv4` et de n'autoriser uniquement que les flux nécessaires à partir des règles de filtrage (menu `System` → `Firewall` onglet `IP Rules`).

Parmi les différents services permettant d'administrer les équipements, il existe le protocole SNMP.

R6

Ne pas utiliser le protocole SNMP pour l'administration distante

Il est recommandé de ne pas utiliser ce protocole à des fins d'administration mais uniquement de supervision comme précisé au chapitre 8.1 du présent document.

Enfin, seuls les postes d'administration doivent pouvoir se connecter aux équipements conformément au recommandations du guide [6].

R7

Filtrer les connexions à destination de l'interface d'administration

Il est recommandé de filtrer les accès aux services d'administration.

Ce filtrage peut être réalisé par un pare-feu lorsque que les recommandations R2 et R2- ont été mises en œuvre ou par le biais des ACL locales. Ces dernières permettent de restreindre l'accès à l'interface d'administration à une ou plusieurs adresses IP distantes.

La configuration des ACL est s'effectue à partir du menu :

- **pour l'équipement** `X310`, Activer le service à partir du menu `Agent` en cochant la case `Management ACL`. Valider la saisie en appuyant sur le bouton `Set Values`. Créer ensuite la règle à partir du menu `Agent` → `Management ACL`. Sélectionner `New Entry` et créer la règle de filtrage. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Security` → `Management ACL`. Insérer l'adresse IP du poste d'administration et le masque associé (255.255.255.255 pour filtrer une adresse précise). Renseigner ensuite le VLAN d'administration (ne pas utiliser le VLAN par défaut). Cocher uniquement les

services HTTPS et SSH (le service SNMP peut être ajouté pour superviser l'équipement). Cocher uniquement le port raccordé sur le poste d'administration. Si aucun poste n'est raccordé directement sur l'équipement, il est nécessaire de sélectionner le ou les port(s) de *Trunk* sur le(s)quel(s) est (sont) véhiculé(s) le VLAN d'administration. Il est nécessaire d'activer le service d'ACL de façon globale en cochant la case Management ACL. Valider la saisie en appuyant sur le bouton Set Values;

- **pour l'équipement** XC216, Security → Management ACL. Insérer l'adresse IP du poste d'administration et le masque associé (255.255.255.255 pour filtrer une adresse précise). Renseigner ensuite le VLAN d'administration (ne pas utiliser le VLAN par défaut). Cocher uniquement les services HTTPS et SSH (le service SNMP peut être ajouté pour superviser l'équipement). Cocher uniquement le port raccordé sur le poste d'administration. Si aucun poste n'est raccordé directement sur l'équipement, il est nécessaire de sélectionner le ou les port(s) de *Trunk* sur le(s)quel(s) est (sont) véhiculé(s) le VLAN d'administration. Il est nécessaire d'activer le service d'ACL de façon globale en cochant la case Management ACL. Valider la saisie en appuyant sur le bouton Set Values;

- **pour l'équipement** XM408, Security → Management ACL. Insérer l'adresse IP du poste d'administration et le masque associé (255.255.255.255 pour filtrer une adresse précise). Renseigner ensuite le VLAN d'administration (ne pas utiliser le VLAN par défaut). Cocher uniquement les services HTTPS et SSH (le service SNMP peut être ajouté pour superviser l'équipement). Cocher uniquement le port raccordé sur le poste d'administration. Si aucun poste n'est raccordé directement sur l'équipement, il est nécessaire de sélectionner le ou les port(s) de *Trunk* sur le(s)quel(s) est (sont) véhiculé(s) le VLAN d'administration. Il est nécessaire d'activer le service d'ACL de façon globale en cochant la case Management ACL. Valider la saisie en appuyant sur le bouton Set Values.

- **pour l'équipement** S615, (les autres équipements nécessitant la mise en place d'ACL), le filtrage de l'interface d'administration peut être réalisé de la façon suivante : Security → Firewall onglet IP Rules. Un exemple de règle est présenté dans le tableau 2.

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence [6]
❑	IPv4	Accept	Vlan admin	Device	192.168.10.10/32[5]	192.168.10.254/32	SSH	Info	0
❑	IPv4	Accept	Vlan admin	Device	192.168.10.10/32[5]	192.168.10.254/32	HTTPS	Info	1
❑	IPv4	Reject	Vlan admin	Device	0.0.0.0/0	0.0.0.0/0	all	Critical	2

TABLE 2 – Exemple de règles pour filtrer l'adresse du poste d'administration pour le service HTTPS et le protocole SSH.

5. Il s'agit de l'addresse IP du poste d'administration.
6. Cette colonne concerne l'ordre d'exécution des règles.

Attention

Assurez-vous bien que les interfaces d'administration ont été migrées vers le nouveau VLAN d'administration avant de mettre en place ces règles de filtrage. La mise en œuvre du VLAN d'administration est décrit au chapitre 4.1.

3.3 Configuration des interfaces d'administration

Les configurations par défaut des services d'administration nécessitent d'être ajustées.

3.3.1 Configuration de l'interface SSH

Le serveur SSH utilise des clefs cryptographiques déjà présentes dans l'équipement afin de s'authentifier. Ne disposant d'aucune information sur le mécanisme de génération initiale de ces clefs, il est plus prudent d'en générer de nouvelles en accord avec le guide sur OpenSSH [1] publié par l'ANSSI.

Les équipements qui font l'objet du présent guide ne permettent pas d'importer les clefs RSA générées depuis une autre application. Pour cela, il est nécessaire de rénitialiser les équipements lors de leur mise en œuvre.

R8

Remplacer les clefs SSH générées par défaut

Il est recommandé de générer de nouvelles clefs RSA en réinitialisant les équipements à partir de la configuration « usine ».

Pour réinitialiser les équipements, le menu à utiliser est le suivant :

- **pour l'équipement** `X310`, `System` → `Restart & Defaults`. Appuyer sur le bouton `Restore Factory Defaults and Restart`;
- **pour l'équipement** `XB208`, `System` → `restart`. Appuyer sur le bouton `Restore Factory Defaults and Restart`;
- **pour l'équipement** `XC216`, `System` → `restart`. Appuyer sur le bouton `Restore Factory Defaults and Restart`;
- **pour l'équipement** `XM408`, `System` → `restart`. Appuyer sur le bouton `Restore Factory Defaults and Restart`;
- **pour l'équipement** `S615`, `System` → `restart`. Appuyer sur le bouton `Restore Factory Defaults and Restart`.

Afin de s'assurer de la fermeture des sessions des administrateurs, un *timeout* est configuré par défaut pour les connexions en ligne de commande (SSH). Il est nécessaire d'activer ce délai lorsque ce n'est pas le cas et de l'uniformiser pour les sessions HTTPS et SSH.

Par défaut, les valeurs de *timeout* SSH sont :

- **pour l'équipement** `X310`, 300 secondes ;
- **pour l'équipement** `XB208`, 300 secondes ;
- **pour l'équipement** `XB216`, 300 secondes
- **pour l'équipement** `XM408`, 300 secondes ;
- **pour l'équipement** `S615`, 300 secondes.

R9

Configurer une fermeture de session automatique SSH

Il est recommandé de configurer un délai de fermeture de session *timeout* automatique sur l' interface d'administration SSH (par exemple 5 minutes qui est la valeur par défaut).

Pour chaque équipement, les paramètres de session SSH sont accessibles à partir du menu :

- **pour l'équipement** `X310`, `Agent` → `Timeout Config`. Configurer la valeur du champ `CLI(TELNET, SSH, Serial)`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `Auto Logout`. Configurer la valeur du champ `CLI(TELNET, SSH, Serial)`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `Auto Logout`. Configurer la valeur du champ `CLI(TELNET, SSH, Serial)`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `Auto Logout`. Configurer la valeur du champ `CLI(TELNET, SSH, Serial)`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `Auto Logout`. Configurer la valeur du champ `CLI(TELNET, SSH)`. Valider la saisie en appuyant sur le bouton `Set Values`.

3.3.2 Configuration de l'interface Web

Le serveur HTTPS des équipements est configuré par défaut avec un certificat autosigné. Ne disposant d'aucune information sur le mécanisme de génération initiale de ce dernier, il convient de le remplacer par un certificat respectant les recommandations du RGS ([12], [13] et [14]) généré depuis une IGC de confiance.

R10

Remplacer le certificat HTTPS par défaut

Il est recommandé de remplacer le certificat usine installé par défaut sur les équipements par un certificat généré depuis une IGC de confiance.

Le nom DNS de l'équipement doit être présent dans le *Subject Alternative Name* afin de permettre la vérification du certificat par le navigateur client. De plus, l'autorité de certification ayant signé le certificat de l'interface *WEB* doit être présente dans le magasin d'autorités du navigateur client.

Attention

L'insertion de la clef privée dans l'équipement X310 nécessite de supprimer le mot de passe du fichier *.PEM. La manipulation de ce fichier est à réaliser avec précautions. De plus, l'équipement ne supporte pas de clef privée de plus de 2048 bits. La suppression du mot de passe peut-être réalisée de la façon suivante :

```
user@poste1:/home# openssl rsa -in X310_pwd.pem -out
   x310_notpwd.pem
Enter pass phrase for X310_pwd.pem:
writing RSA key
```

Pour chaque équipement, l'import d'un certificat et de la clef privée s'effectue à partir du menu suivant :

- **pour l'équipement** X310, System → Save & Load HTTP. Appuyer sur le bouton SSL Private Key File → Browse... et insérer la clef privée sans mot de passe au format *.PEM. Valider en appuyant sur le bouton Load Private Key. Appuyer sur le bouton SSL Certificate File → Browse... et insérer le certificat au format *.PEM. Valider en appuyant sur le bouton Load Certificate and Restart;
- **pour l'équipement** XB208, System → Load&Save onglet HTTP, appuyer sur le bouton Load de la ligne HTTPSCert et insérer le certificat de l'équipement au format *.P12. a partir de l'onglet Passwords insérer le mot de passe de la clef privée, dans le champ Password de la ligne HTTPS Certificate;
- **pour l'équipement** XC216, System → Load&Save onglet HTTP, appuyer sur le bouton Load de la ligne HTTPSCert et insérer le certificat de l'équipement au format *.P12. a partir de l'onglet Passwords insérer le mot de passe de la clef privée, dans le champ Password de la ligne HTTPS Certificate;
- **pour l'équipement** XM408, System → Load&Save onglet HTTP, appuyer sur le bouton Load de la ligne HTTPSCert et insérer le certificat de l'équipement au format *.P12. a partir de l'onglet Passwords insérer le mot de passe de la clef privée, dans le champ Password de la ligne HTTPS Certificate;
- **pour l'équipement** S615, System → Load&Save onglet HTTP, appuyer sur le bouton Load de la ligne HTTPSCert et insérer le certificat de l'équipement au format *.P12. a partir de l'onglet Passwords insérer le mot de passe de la clef privée, dans le champ Password de la ligne HTTPS Certificate.

Attention

Le protocole HTTPS combine les protocoles HTTP et TLS. Par défaut, tous les équipements utilisent la version 1.1 de TLS qui est obsolète.

Attention

L'ensemble des équipements intègrent une implémentation de TLSv1.2 avec des algorithmes de signature (dans le cadre de l'authentification) obsolètes

(RSA_PKCS1_SHA1 et DSA_SHA1). Pour cette raison, il est nécessaire d'utiliser la version 1.3 de TLS lorsque celle-ci est disponible.

R11

Durcir le protocole TLS

Il est recommandé d'utiliser au moins la version 1.3 du protocole TLS et des suites cryptographiques non vulnérables conformément au guide [8].

Pour chaque équipement, la version peut être configurée à partir du menu suivant :

- **pour l'équipement** `X310`, Aucun menu ne permet de sélectionner la version de TLS à utiliser. Seules les versions 1.1 et 1.2 sont disponibles pour cet équipement. **Il n'est pas possible de forcer une des deux versions disponibles** ;
- **pour l'équipement** `XB208`, `System` → `Configuration` → `Minimum TLS Version`. Sélectionner la version et valider la saisie en appuyant sur le bouton `Set Values`.
  Les versions 1.1, 1.2 et 1.3 sont disponibles pour cet équipement ;
- **pour l'équipement** `XC216`, `System` → `Configuration` → `Minimum TLS Version`. Sélectionner la version et valider la saisie en appuyant sur le bouton `Set Values`.
  Les versions 1.1, 1.2 et 1.3 sont disponibles pour cet équipement ;
- **pour l'équipement** `XM408`, `System` → `Configuration` → `Minimum TLS Version`. Sélectionner la version et valider la saisie en appuyant sur le bouton `Set Values`.
  Les versions 1.1, 1.2 et 1.3 sont disponibles pour cet équipement ;
- **pour l'équipement** `S615`, `System` → `Configuration` → `Minimum TLS Version`. Sélectionner la version et valider la saisie en appuyant sur le bouton `Set Values`.
  Les versions 1.1 et 1.2 sont disponibles pour cet équipement.

Attention

Dans le protocole TLS, in de ne pas compromettre la confidentialité d'une communication enregistrée et dont la clef privée d'un correspondant est connue, il existe une fonctionnalité appelée *Perfect Forward Secrecy* (PFS). Cette fonctionnalité n'est pas implémentée sur les équipements `S615` et `X310`, quelle que soit la version de TLS.

Attention

Les suites cryptographiques ci-dessous sont activées sur l'équipement `X310` lors de la sélection de TLSv1.2 et ne peuvent pas être désactivées localement.

Code TLS	Nom de la suite	Echange des clefs	chiffrement
0x009c	AES128-GCM-SHA256	RSA	AES
0x003c	AES128-SHA256	RSA	AES
0x002f	AES128-SHA	RSA	AES
0x0041	CAMELLIA128-SHA	RSA	CAMELLIA

TABLE 3 – Suites cryptographiques à définir en liste noire sur les navigateurs

> Selon le navigateur WEB, il est possible de renseigner, dans une liste noire, les suites à désactiver.

Afin de s'assurer de la fermeture des sessions des administrateurs, un *timeout* est configuré par défaut sur les interfaces *WEB* (HTTPS). Il est nécessaire d'activer ce délai lorsque ce n'est pas le cas et de l'uniformiser pour les sessions HTTPS et SSH.

Par défaut, les valeurs de *timeout* WEB sont :

- **pour l'équipement** `X310`, 900 secondes ;
- **pour l'équipement** `XB208`, 900 secondes ;
- **pour l'équipement** `XB216`, 900 secondes
- **pour l'équipement** `XM408`, 900 secondes ;
- **pour l'équipement** `S615`, 900 secondes.

R12

Configurer une fermeture automatique de session HTTPS

Il est recommandé de configurer un délai de fermeture de session *timeout* automatique sur l'interface d'administration HTTPS (par exemple 5 minutes).

Pour chaque équipement, les paramètres de session HTTPS sont accessibles à partir du menu :

- **pour l'équipement** `X310`, `Agent` → `Timeout Config`. Configurer la valeur du champ `Web Based Management`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `Auto Logout`. Configurer la valeur du champ `Web Based Management`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `Auto Logout`. Configurer la valeur du champ `Web Based Management`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `Auto Logout`. Configurer la valeur du champ `Web Based Management`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `Auto Logout`. Configurer la valeur du champ `Web Based Management`. Valider la saisie en appuyant sur le bouton `Set Values`.

3.4 Gestion des comptes utilisateur

3.4.1 Utilisation de comptes nominatifs

L'utilisation des comptes nominatifs doit être généralisée. En effet, l'utilisation de ce type de compte permet de tracer efficacement les actions des administrateurs et facilite la gestion des équipements comme énoncé dans le guide de recommandations [6].

R13

Utiliser des comptes nominatifs d'administration

Il est recommandé de généraliser l'utilisation des comptes nominatifs pour l'administration des équipements.

Attention

Seul un compte administrateur de secours non nominatif doit rester présent. Ce compte doit alors disposer d'un mot de passe fort [7] et ne doit être utilisé qu'afin de rétablir l'accès aux comptes nominatifs. Son mot de passe doit être conservé au coffre-fort et son utilisation doit être contrôlée et limitée à un ensemble déterminé de personnes.

Attention

L'équipement `X310` ne permet pas la création de plus d'un compte utilisateur avec privilège, la recommandation R13 ne peut donc pas s'appliquer à cet équipement.

Il existe deux façons d'effectuer un contrôle d'accès sur les commutateurs :

- **le contrôle d'accès local** : le commutateur compare le couple nom d'utilisateur/mot de passe saisi avec le contenu de sa configuration afin d'autoriser ou non l'accès à son interface d'administration avec les droits associés à ce compte ;
- **le contrôle d'accès distant** : le commutateur interroge un service d'authentification distant reposant sur un annuaire.

La gestion des comptes locaux se révèle très lourde dès lors que le nombre d'administrateurs ou d'équipements sur le SI devient conséquent. L'utilisation de comptes centralisés est la méthode d'administration à privilégier comme énoncé au chapitre 3.4.2.

3.4.2 Comptes centralisés

Les comptes nominatifs sont créés dans un annuaire central. Ces comptes sont utilisés par les administrateurs pour effectuer leurs tâches d'administration quotidiennes. Sur chaque équipement, un compte administrateur local de secours non nominatif (ex : *localadmin*) peut être créé en cas de perte de l'annuaire central par exemple. Ce compte doit respecter les recommandations des comptes non nominatifs évoquées au chapitre 3.4.1.

Attention

Les équipements réseau utilisés dans le cadre de la bureautique implémentent généralement le protocole de diffusion d'annuaire LDAP. Le protocole LDAP n'est pas compatible sur les équipements faisant l'objet du présent guide. C'est pourquoi, si un annuaire LDAP est présent, il peut être raccordé au serveur d'authentification de type RADIUS.

7. Se reporter au guide [16].

R14

Mettre en place une gestion centralisée des utilisateurs

L'utilisation d'un moyen de contrôle d'accès distant reposant sur un annuaire doit être mis en place pour les connexions au commutateur. L'authentification locale ne doit être autorisée que pour le compte local d'administration.

Il est par ailleurs recommandé d'utiliser un annuaire dédié aux comptes d'administration du SI, comme expliqué dans le guide [6] de l'ANSSI relatif à l'administration sécurisée des SI.

Le contrôle d'accès distant permet non seulement de s'appuyer sur une gestion centralisée des comptes utilisateurs, mais aussi de conserver une traçabilité des demandes d'accès directement au niveau du service de contrôle d'accès.

Il existe un certain nombre de protocoles de contrôle d'accès distant reposant sur un annuaire, appelés protocoles AAA. Ces protocoles permettent, en plus de gérer l'authentification des utilisateurs *(Authentication)* et l'attribution de leurs droits *(Authorization)*, de journaliser les authentifications et les commandes entrées par les utilisateurs dans un but de traçabilité *(Accounting)*. Les équipements concernés par le présent guide utilisent le protocole RADIUS pour le contrôle d'accès centralisé. Aucun des équipements mentionnés ne propose la fonctionnalité *Accounting* du protocole RADIUS, en revanche, la traçabilité des connexions est couverte par la journalisation comme énoncé au chapitre 7.

R15

Vérification des paramètres d'authentification

Il est recommandé de configurer la manière dont les paramètres d'authentification seront vérifiés avec l'option `Radius and fallback local`.

L'option `RADIUS and fallback local` du champ `Login Authentication` permet, lorsque le serveur n'est pas joignable (après trois essais infructueux), de vérifier localement, la présence du compte.

Pour chaque équipement, le contrôle d'accès centralisé est configuré à partir du menu suivant :

- **pour l'équipement** `X310`, `System` → `Passwords`. Sélectionner le paramètre `RADIUS and LOCAL local` dans le champ `Login Mode`. Valider la saisie en appuyant sur le bouton `Set Values`. La configuration du serveur s'effectue à partir du menu : `Switch` → `IEEE 802.1X` → `RADIUS Config`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Security` → `AAA` → onglet `General`. Sélectionner le paramètre `Radius and fallback local` du champ `Login Authentication`. Valider la saisie en appuyant sur le bouton `Set Values`. La configuration du serveur s'effectue à partir du menu : `Security` → `AAA` → onglet `RADIUS Client`. Sélectionner le paramètre `Vendor Specific`[8] du champ `RADIUS Authorization Mode`. Valider la saisie en appuyant sur le bouton `Create` ;
- **pour l'équipement** `XC216`, `Security` → `AAA` → onglet `General`. Sélectionner le paramètre `Radius and fallback local` du champ `Login Authentication`. Valider la saisie en appuyant sur le bouton `Set Values`. La configuration du serveur s'effectue à partir du menu : `Security` → `AAA` → onglet `RADIUS Client`. Sélectionner le paramètre `Vendor Specific` du champ `RADIUS Authorization Mode`. Valider la saisie en appuyant sur le bouton `Create` ;

- **pour l'équipement** `XM408`, `Security` → `AAA` → onglet `General`. Sélectionner le paramètre `Radius and fallback local` du champ `Login Authentication`. Valider la saisie en appuyant sur le bouton `Set Values`. La configuration du serveur s'effectue à partir du menu : `Security` → `AAA` → onglet `RADIUS Client`. Sélectionner le paramètre `Vendor Specific` du champ `RADIUS Authorization Mode`. Valider la saisie en appuyant sur le bouton `Create` ;
- **pour l'équipement** `S615`, `Security` → `AAA` → onglet `General`. Sélectionner le paramètre `Radius and fallback local` du champ `Login Authentication`. Valider la saisie en appuyant sur le bouton `Set Values`. La configuration du serveur s'effectue à partir du menu : `Security` → `AAA` → onglet `RADIUS Client`. Sélectionner le paramètre `Vendor Specific` du champ `RADIUS Authorization Mode`. Valider la saisie en appuyant sur le bouton `Create`.

3.4.3 Comptes locaux

Lorsque des comptes locaux sont utilisés, il est nécessaire de durcir les configurations en paramétrant, par exemple, le nombre d'essais, la taille minimale du mot de passe, la politique de mot de passe, etc. En effet, les mots de passe utilisés doivent résister aux attaques par force brute.

R16

Durcir les paramètres des comptes locaux

Lorsque des comptes locaux sont utilisés, il est recommandé de :
- spécifier une taille minimale de mot de passe ;
- spécifier une politique de mot de passe ;
- verrouiller l'utilisateur après plusieurs échecs à l'exception du compte de secours.

Attention

Pour tous les équipements, aucune option ne permet de configurer une taille minimale pour le mot de passe local.
- Pour l'équipement `X310`, la longueur minimale acceptée est de **1** caractère et la longueur maximale de **16** caractères.
- Pour tous les autres équipements, le mot de passe doit être constitué d'au moins **8** caractères comprenant au moins un chiffre, une lettre majuscule et un caractère spécial.

Information

Après 10 tentatives de connexions erronées à partir de l'interface WEB, l'accès à l'équipement est bloqué (uniquement pour la session WEB) durant 1 heure, quel que soit le compte utilisé (y compris une authentification au travers d'un serveur RADIUS). Le blocage est retreint à une adresse IP. En effet, le blocage n'est plus effectif si la connexion s'effectue à partir d'une autre adresse IP.

8. Le champ `RADIUS Authorization Mode` est décrit au chapitre 3.4.4.

3.4.4 Droits d'accès

Pour limiter les erreurs de manipulation, éviter l'installation de services vulnérables et maîtriser les accès privilégiés, chaque opérateur ne doit disposer que des droits strictement nécessaires aux actions dont il a la charge sur l'équipement. Ces droits sont positionnés pour un administrateur ou pour un groupe d'administrateurs (cas de l'authentification centralisée présentée en 3.4.2).

Les équipements du présent guide disposent des fonctions *Authentication* et *Authorization* du protocole RADIUS et la gestion des droits est locale à l'équipement. Chaque utilisateur est associé à un rôle local. Il existe deux rôles par défaut (`admin` et `user`), il est possible de supprimer ces derniers et de créer des groupes nécessaires à l'organisation de l'entreprise (par exemple un groupe « Operateur », un groupe « Auditeur » et un groupe « Administrateur »).

Lorsque les rôles sont créés, il est nécessaire de les attribuer aux groupes d'utilisateurs.

La création des rôles s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, Il n'y a pas la possibilité de créer des rôles ou des groupes d'utilisateur à partir de cet équipement comme précisé en fin de section 3.4.4 ;
- **pour l'équipement** `XB208`, `Security` → `Users` → onglet `Roles`. Insérer un nom de rôle dans le champ `Role Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le type de compte à partir de la liste déroulante `Function Right` [9]. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Security` → `Users` → onglet `Roles`. Insérer un nom de rôle dans le champ `Role Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le type de compte à partir de la liste déroulante `Function Right`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Security` → `Users` → onglet `Roles`. Insérer un nom de rôle dans le champ `Role Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le type de compte à partir de la liste déroulante `Function Right`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `Security` → `Users` → onglet `Roles`. Insérer un nom de rôle dans le champ `Role Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le type de compte à partir de la liste déroulante `Function Right`. Valider la saisie en appuyant sur le bouton `Set Values`.

L'attribution des rôles aux groupes s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, Il n'y a pas la possibilité de créer des rôles ou des groupes d'utilisateur à partir de cet équipement comme précisé en fin de section 3.4.4 ;
- **pour l'équipement** `XB208`, `Security` → `Users` → onglet `Groups`. Insérer un nom de groupe dans le champ `Group Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le rôle à attribuer à partir de la liste déroulante `Role`. Valider la saisie en appuyant sur le bouton `Set Values` ;

9. La valeur « 1 » correspond à un utilisateur avec des accès en lecture. La valeur « 15 » correspond à un utilisateur avec des accès d'administrateur.

- **pour l'équipement** `XC216`, `Security` → `Users` → onglet `Groups`. Insérer un nom de groupe dans le champ `Group Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le rôle à attribuer à partir de la liste déroulante `Role`. Valider la saisie en appuyant sur le bouton `Set Values`;
- **pour l'équipement** `XM408`, `Security` → `Users` → onglet `Groups`. Insérer un nom de groupe dans le champ `Group Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le rôle à attribuer à partir de la liste déroulante `Role`. Valider la saisie en appuyant sur le bouton `Set Values`;
- **pour l'équipement** `S615`, `Security` → `Users` → onglet `Groups`. Insérer un nom de groupe dans le champ `Group Name`. Valider la saisie en appuyant sur le bouton `Create`. Sélectionner le rôle à attribuer à partir de la liste déroulante `Role`. Valider la saisie en appuyant sur le bouton `Set Values`.

Sur les équipements du présent guide, il existe deux modes d'autorisation pour le serveur RADIUS (`RADIUS Authorization Mode`, se reporter à la section 3.4.2 pour la configuration de ce mode dans les équipements), **Standard** et **Vendor Specific**.

Vendor Specific :
Lors de la connexion d'un utilisateur, l'équipement transmet une requête au serveur RADIUS. Si l'utilisateur est autorisé, la réponse du serveur RADIUS contient le nom du groupe auquel il appartient. L'équipement compare ce groupe à ceux présents localement pour attribuer les droits à l'utilisateur.

Losqu'un utilisateur local est créé à partir du menu `Security` → `Users`, un compte externe est généré automatiquement dans une table appelée *External User Accounts* (il s'agit de la même table d'utilisateur locaux qui est visible dans ce même menu).

Quand un serveur RADIUS authentifie un utilisateur, si le groupe n'est pas présent dans l'équipement, ce dernier vérifie si l'utilisateur est présent dans la table *External User Accounts*. Si l'utilisateur existe dans la table, il sera authentifié avec les droits correspondants au rôle mentionné dans la table.

Information

Si un utilisateur est présent localement et dans un groupe du serveur RADIUS, l'utilisateur se voit assigner les droits les plus élevés entre ceux attribués sur le serveur RADIUS et ceux attribués localement.

La mise en œuvre du serveur RADIUS permettant d'évaluer les groupes d'utilisateurs nécessite d'effectuer certaines configurations décrites ci-après (exemple pour l'application FREERADIUS).

Ajouter les éléments ci-dessous dans le fichier `/etc/freeradius/users`[8] ou `/etc/freeradius/3.0/mods-config/files/authorize`[8] (selon la version de FREERADIUS).

```
nom_utilisateur Cleartext-password:= "motdepasse"

                Siemens_group:= "group_admin"
```

Ouvrir le fichier `/user/share/freeradius/dictionary` et ajouter la ligne ci-dessous.

```
$INCLUDE dictionary.siemens_scalance
```

Créer le fichier `/user/share/freeradius/dictionary.siemens_scalance` et y ajouter les éléments présentés ci-dessous.

```
VENDOR Siemens_scalance 4196

BEGIN-VENDOR Siemens_scalance

ATTRIBUTE Siemens_group 1 string

END-VENDOR Siemens_scalance
```

Standard :
Ce mode ne permet pas la gestion des groupes d'utilisateurs. L'utilisateur est connecté en tant que *User* sauf si le serveur transmet à l'équipement le libellé `Administrative-User` pour l'attribut `Service-Type`.

Exemple de configuration du fichier `/etc/freeradius/users`[8] ou `/etc/freeradius/3.0/mods-config/files/authorize`[8] (selon la version de FREERADIUS) pour un utilisateur avec des droits d'administration.

```
nom_utilisateur ClearText-Password:= "motdepasse"

                Service-Type = "Administrative-User"
```

Attention

Les équipements du présent guide n'utilisent pas de fonctions de hachage pour protéger les mots de passe lors de leur stockage. C'est pourquoi, le mot de passe de l'utilisateur présent dans l'exemple précédent est en clair. Il convient donc de veillller à la protection du fichier « user.conf » du serveur RADIUS.

Information

Si le serveur RADIUS est accessible mais que le compte n'est pas présent sur ce dernier, ce même compte ne sera pas testé localement même s'il existe dans l'équipement. En effet, lorsque le paramètre `Standard` est sélectionné la table *External Users* n'est pas évaluée. Ainsi, aucun accès ne sera autorisé malgré la présence en local du compte. La table *External Users* est évaluée uniquement en mode `Vendor Specific`.

8. Les équipements du présent guide ne permettent pas d'effectuer une authentification RADIUS avec un condensat de mot de passe, il est donc nécessaire que ce fichier soit protégé en lecture et écriture et accessible uniquement aux administrateurs du serveur RADIUS conformément aux recommandations sur les fichiers sensibles du guide [4].

R17

Mettre en place des groupes RADIUS

Il est recommandé d'utiliser le paramètre `Vendor specific` afin de mettre en œuvre la gestion des comptes par groupe d'utilisateurs.

Information

Contrairement aux autres équipements, le modèle `X310` ne permet pas la création de rôle. Ainsi, il est nécessaire de créer uniquement des utilisateurs dans la base RADIUS dans le fichier suivant : `/etc/freeradius/users` ou `/etc/freeradius/3.0/mods-config/files/authorize` pour la version FREERADIUS v3.0.

3.5 Comptes utilisateurs par défaut

Un compte utilisateur (compte *admin*) est présent dans les équipements en sortie d'usine. Lors d'une première connexion à l'équipement (par SSH ou *WEB*) un menu s'affiche à l'écran afin de modifier le mot de passe par défaut. Les caractéristiques de complexité du mot de passe sont les suivantes :

- au moins huit caractères ;
- dont une majuscule ;
- et un caractère spécial.

Attention

Contrairement aux autres équipements du présent guide, deux comptes sont présents par défaut sur l'équipement `X310`, le compte *admin* et le compte *user*. Les mots de passe par défaut de ces comptes doivent être modifiés dès la première utilisation de l'équipement. Les caractéristiques de complexité des mots de passe de l'équipement `X310` sont d'un niveau faible :

- au moins un caractère ;
- ne peut excéder 16 caractères ;
- pas de caractère spécial ni de majuscule exigés.

R18

Modifier les mots de passe par défaut

Il est recommandé de modifier le mot de passe des comptes *admin* et *user* sur l'équipement `X310` et de respecter les règles relatives à la génération des mots de passe décrites dans le guide de l'ANSSI [16].

Pour respecter la recommandation R18, la configuration de l'équipement `X310` s'effectue à partir du menu suivant : `System` → `Passwords`.

3.6 Configuration des outils d'administration

Deux moyens d'administration sont disponibles :

- via un client léger (navigateur *WEB*) ;
- via une connexion SSH.

3.6.1 Le client léger

Le client léger administre les équipements exclusivement en HTTPS. Le premier élément de sécurité est l'authentification du serveur. Le protocole HTTPS repose sur une autorité de confiance afin de vérifier la validité du certificat présenté par l'équipement. La présence de l'autorité de confiance (AC) dans les magasins d'autorités de confiance du navigateur est donc indispensable.

R19

Ajouter l'autorité de confiance dans le magasin de certificats

Il est recommandé d'ajouter la ou les autorités de confiance nécessaires dans le magasin de certificats du client léger. L'accès au serveur HTTPS ne doit lever aucune exception de sécurité relative à la validité des certificats mis en œuvre.

Information

L'ajout de l'autorité de confiance dans le magasin de certificats est réalisé au travers du navigateur *WEB* en insérant le certificat de l'autorité, par exemple, au format *.PEM.

En accord avec le guide de recommandations TLS [8] publié par l'ANSSI, seules certaines suites cryptographiques doivent être utilisées avec ce protocole. De la même manière seul TLSv1.2 doit être configuré et utilisé pour administrer les équipements.

R20

Durcir le protocole TLS sur le navigateur

Pour l'équipement `X310`, il est recommandé de configurer le navigateur pour n'utiliser que la version 1.2 du protocole TLS et des suites cryptographiques non vulnérables conformément au guide [8].

3.6.2 Administration par SSH

Les équipements s'administrent également à partir du protocole SSH. Les clients SSH adoptent par défaut le modèle *Trust On First Use* (le fonctionnement TOFU est expliqué dans la note technique OpenSSH [1]). La confiance envers le serveur SSH est établie lors de la première connexion. Il est important de vérifier l'empreinte du serveur affichée par le client et de la comparer avec l'empreinte présente sur le serveur.

R21

Vérifier l'empreinte SSH de l'équipement

Il est recommandé de comparer l'empreinte SSH générée par le client avec celle qui est présente sur le serveur en utilisant un canal de communication de confiance (première connexion en local, à proximité de la machine par exemple).

Pour chaque équipement, l'empreinte de la clef SSH est consultable à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent → SSH Fingerprints` , l'empreinte se situe dans la partie inférieure de l'écran ;
- **pour l'équipement** `XB208`, `Information → Security` puis onglet `Overview → SSH Fingerprint SHA256`, l'empreinte se situe dans la partie supérieure de l'écran ;
- **pour l'équipement** `XC216`, `Information → Security` puis onglet `Overview → SSH Fingerprint SHA256`, l'empreinte se situe dans la partie supérieure de l'écran ;
- **pour l'équipement** `XM408`, `Information → Security` puis onglet `Overview → SSH Fingerprint SHA256`, l'empreinte se situe dans la partie supérieure de l'écran ;
- **pour l'équipement** `S615`, `Information → Security` puis onglet `Overview → SSH Fingerprint SHA256`, l'empreinte se situe dans la partie supérieure de l'écran.

4
Configuration du réseau

4.1 VLAN

D'une manière générale, les réseaux locaux doivent être cloisonnés pour des raisons de sécurité et de performances. Concernant la sécurité, comme tous les équipements d'un même réseau peuvent établir des communications entre eux, réduire la taille de ces réseaux a pour effet, de limiter l'exposition de ces équipements. Concernant les performances, le fait de multiplier les équipements sur un même segment réseau a pour effet de multiplier les occurences de colisions et donc de diminuer les performances.

Objectif

Mettre en place les bonnes pratiques de configuration des VLAN afin d'améliorer la performance et la sécurité des équipements.

Le cloisonnement peut être physique ou virtuel. Le premier est plus sécurisé et plus performante, tous les liens sont dédiés et aucun équipement réseau n'est mutualisé. En revanche, il est plus onéreux et les contraintes physiques ne le permettent pas toujours.

Le cloisonnement logique nécessite uniquement des modifications de configuration. Dans ce cas, les liens physiques et les commutateurs sont mutualisés. Cependant, la mise en œuvre ou la modification d'un ou plusieurs réseaux virtuels peut être une source d'erreur(s) dans les configurations, induisant un décloisonnement des flux de production/métiers ainsi que ceux d'administration (cas du non respect de la recommandation R2). Par ailleurs, l'introduction de nombreux réseaux virtuels peut influer sur les performances du commutateur ou du pare-feu.

Attention

Avant de choisir entre cloisonnement physique et cloisonnement logique des réseaux de production/métiers, il est nécessaire de mener une analyse de risque et de vérifier ce qui est autorisé par la réglementation en vigueur et ce que prévoit la politique de sécurité des systèmes d'information de l'entité.

Le cloisonnement virtuel des réseaux locaux (niveau 2 du modèle OSI) est associé au concept de VLAN. Le principe du VLAN est d'ajouter un marquage sur la trame *Ethernet* contenant, entre autres, l'identifiant du réseau virtuel. Les équipements étudiés dans le présent guide intègrent la

technologie VLAN, il est cependant nécessaire de respecter des bonnes pratiques de configuration afin de conserver un niveau de sécurité du réseau acceptable.

Un commutateur gère l'attribution d'un ou plusieurs VLAN par port. Ces ports peuvent être configurés dans l'un des deux modes suivants :

- mode *trunk* : le port est utilisé pour transporter plusieurs réseaux virtuels sur un seul lien physique. Le commutateur s'interconnecte avec un autre équipement compatible avec cette mutualisation. Les trames Ethernet en provenance ou à destination de ces équipements sont marquées par un identifiant de VLAN à l'exception du VLAN natif comme indiqué dans le guide de recommandations des commutateurs [2] ;
- mode *access* : le port est directement connecté à un équipement terminal (automate, poste bureautique, imprimante, téléphone IP, etc.). Les trames Ethernet en provenance ou à destination de ces équipements ne sont pas marquées sur ce type de port.

Chacun de ces deux modes a des particularités de configuration. Les paragraphes suivants détaillent les spécificités de ces modes et précisent la façon de les configurer.

Information

La mise en place de réseaux logiques nécessite un paramétrage cohérent des VLAN sur l'ensemble des équipements réseaux. Conformément à la recommandation R34, les ports non utilisés sont à positionner dans un VLAN différent du VLAN 1.

Pour chaque équipement, la création des VLAN et l'affectation des ports s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `VLAN`, appuyer sur le bouton `New Entry`, saisir le numéro de VLAN à créer. Valider la saisie en appuyant sur le bouton `Set Values`. A partir du menu `Switch` → `VLAN` → `Port`, sélectionner le VLAN concerné et modifier le numéro `Port VLAN ID` par celui créé précédemment. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `VLAN`, onglet `General`. Positionner le paramètre `Base Bridge Mode` avec le paramètre `802.1Q VLAN Bridge`. Valider la saisie en appuyant sur le bouton `Set Values`. A partir du menu `Layer 2` → `VLAN` → `Port Based VLAN`, sélectionner le VLAN concerné et modifier le numéro `Port VID` par celui créé précédemment. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `VLAN`, onglet `General`. Positionner le paramètre `Bridge Mode` avec le paramètre `Customer`. La valeur `Provider` de cette option n'est pas recommandée (en effet, cette fonctionnalité permet l'utilisation du mode Q-in-Q [11] afin de transporter le traffic sur un réseau de niveau 2 d'un opérateur). Positionner le paramètre `Base Bridge Mode` avec le paramètre `802.1Q VLAN Bridge`. Valider la saisie en appuyant sur le bouton `Set Values`. A partir du menu `Layer 2` → `VLAN` → `Port Based VLAN`, sélectionner le VLAN concerné et modifier le numéro `Port VID` par celui créé précédemment. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `VLAN`, onglet `General`. Positionner le paramètre `Base Bridge Mode` avec le paramètre `802.1Q VLAN Bridge`. Valider la saisie en appuyant sur le bouton `Set Values`. A partir du menu `Layer 2` → `VLAN` → `Port Based VLAN`, sélectionner le VLAN

concerné et modifier le numéro `Port VID` par celui créé précédemment. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `S615`, `Layer 2` → `VLAN`, onglet `General`. Positionner le paramètre `Base Bridge Mode` avec le paramètre `802.1Q VLAN Bridge`. Valider la saisie en appuyant sur le bouton `Set Values`. A partir du menu `Layer 2` → `VLAN` → `Port Based VLAN`, sélectionner le VLAN concerné et modifier le numéro `Port VID` par celui créé précédemment. Valider la saisie en appuyant sur le bouton `Set Values`.

4.1.1 Ports en mode trunk

Par défaut, quand un port est configuré en mode *trunk* sur un commutateur ou pare-feu *Scalance*, seuls les réseaux explicitement autorisés sont transportés. Cette discrimination des réseaux logiques est réalisée par l'utilisation des marquages (*tags*) ayant des valeurs définies par l'administrateur. Seules des trames marquées avec ces valeurs circulent sur ce port.

R22

Configurer les ports de type trunk de manière sécurisée

Il est recommandé de configurer un port de type *trunk* de la manière suivante :

- interdire les trames non marquées ;
- configurer les VLAN autorisés comme marqués ;
- ne pas affecter de ports sur le VLAN 1 (uniquement sur l'équipement `X310`) ;

Information

Sur les équipements testés, le VLAN 1 est le VLAN par défaut. De plus amples informations sont disponibles dans le guide de sécurisation des commutateurs [2].

Pour chaque équipement, la mise en place des identifiants VLAN et les affectations des ports s'effectuent à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `VLAN`. Chaque VLAN autorisé à circuler sur un port en mode *trunk*, doit être affecté avec le symbole « **T** » sur le port concerné. L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `VLAN`, onglet `General`. Chaque VLAN autorisé à circuler sur un port en mode *trunk*, doit être affecté avec le symbole « **T** » sur le port concerné. L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `VLAN`, onglet `General`. Chaque VLAN autorisé à circuler sur un port en mode *trunk*, doit être affecté avec le symbole « **T** » sur le port concerné. L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `VLAN`, onglet `Port Assignment`. Chaque VLAN autorisé à circuler sur un port en mode *trunk*, doit être affecté avec le symbole « **T** » sur le port concerné.

11. Terme définissant la possibilité d'encapsuler un second identifiant de VLAN selon le standard IEEE 802.1ad.

L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `S615`, `Layer 2` → `VLAN`, onglet `General`. Chaque VLAN autorisé à circuler sur un port en mode *trunk*, doit être affecté avec le symbole « **T** » sur le port concerné. L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values`.

L'affectation des VLAN par port est illustrée sur la figure 4 du chapitre 4.3 du présent guide.

Les équipements du présent guide intègrent une fonctionnalité de filtrage permettant d'interdire la circulation des trames non marquées sur les liens en mode *trunk*. Cette opération est à réaliser à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `VLAN` → `Ports`. Sélectionner le numéro du VLAN concerné et cocher la case `Tagged Frames`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Tagged Frames Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Tagged Frames Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Tagged Frames Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `Layer 2` → `VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Tagged Frames Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values`.

4.1.2 Ports en mode access

Contrairement au mode *trunk*, un port en mode *access* permet la connexion des équipements terminaux. Il est le principal vecteur d'attaque car l'équipement terminal ne peut pas toujours être considéré comme de confiance. Par ailleurs, dans certains contextes, des prises réseaux sont accessibles librement (pour des terminaux de maintenance par exemple). La configuration du raccordement doit être imposée par le commutateur, en particulier le VLAN d'appartenance.

R23

Configurer les ports de type access de manière sécurisée

Il est recommandé de configurer un port de type *access* de la manière suivante :

- positionner l'identifiant du VLAN d'appartenance ;
- autoriser la circulation des trames non marquées ;
- activer la fonction *Ingress Filtering* ;
- configurer le VLAN autorisé comme non marqué ;

- empêcher toute interaction avec les protocoles de redondance niveau 2 (se référer au chapitre 4.2) ;
- limiter le nombre d'adresses MAC autorisées par port (se référer au chapitre 4.3.2).

Pour chaque équipement, la mise en place des identifiants VLAN et les affectations des ports s'effectuent à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `VLAN`. En mode *access*, le port du VLAN concerné doit être marqué du symbole « **U** ». L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `VLAN`, onglet `General`. En mode *access*, le port du VLAN concerné doit être marqué du symbole « **U** ». L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `VLAN`, onglet `General`. En mode *access*, le port du VLAN concerné doit être marqué du symbole « **U** ». L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `VLAN`, onglet `Port Assignment`. En mode *access*, le port du VLAN concerné doit être marqué du symbole « **U** ». L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `Layer 2` → `VLAN`, onglet `General`. En mode *access*, le port du VLAN concerné doit être marqué du symbole « **U** ». L'ensemble des VLAN non autorisés à circuler sur ce port doivent être affectés avec le symbole « **F** ». Valider la saisie en appuyant sur le bouton `Set Values`.

L'affectation des VLAN par port est illustrée sur la figure 4 du chapitre 4.3 du présent guide.

Les équipements du présent guide intègrent une fonctionnalité de filtrage permettant d'interdire la circulation des trames marquées sur les liens en mode *access*. Cette opération est à réaliser à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `VLAN` → `Ports`. Sélectionner le numéro du VLAN concerné et cocher la case `Untagged Frames`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Untagged and Priority Tag Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Untagged and Priority Tag Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `XM408`, `Layer 2 → VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Untagged and Priority Tag Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `Layer 2 → VLAN`, onglet `Port Based VLAN`, colonne `Acceptable Frames`, à partir de la liste déroulante, sélectionner la valeur `Untagged and Priority Tag Only` pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values`.

Attention

Les équipements disposent d'une fonctionnalité permettant le transfert d'une trame vers l'ensemble des ports d'un VLAN lorsque l'identifiant VLAN reçu ne correspond pas à celui du port concerné.

R24

Désactiver la fonctionnalité de transfert de trame

Pour éviter l'intercommunication des VLAN, il est recommandé de désactiver la fonctionnalité de transfert de trame provenant d'un VLAN inconnu.

Cette opération est à réaliser à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch → VLAN → Ports`. Sélectionner le numéro du VLAN concerné et cocher la case `Ingress Filtering`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2 → VLAN`, onglet `Port Based VLAN`, colonne `Ingress Filtering`, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2 → VLAN`, onglet `Port Based VLAN`, colonne `Ingress Filtering`, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2 → VLAN`, onglet `Port Based VLAN`, colonne `Ingress Filtering`, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `Layer 2 → VLAN`, onglet `Port Based VLAN`, colonne `Ingress Filtering`, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values`.

4.1.3 VLAN par défaut

Conformément au guide [2], le ou les VLAN(s) par défaut doi(ven)t être supprimé(s).

Information

Les équipements `XC216`, `XB208` et `XM408` présentent un VLAN par défaut (VLAN 1). L'équipement `X310` présente deux VLAN par défaut (VLAN 1 et VLAN 500). L'équipement `S615` présente deux VLAN par défaut (VLAN 1 et VLAN 2).

Attention

Le micrologiciel de l'équipement X310 ne permet pas de supprimer le VLAN 1. L'équipement X310 n'est donc concerné que par les mesures numéro 1 et 2 de la configuration listée ci-dessous.

Afin de supprimer le VLAN 1, plusieurs éléments de configuration sont à vérifier ou à réaliser dont la méthodologie est la suivante (par ordre d'opérations à vérifier ou réaliser) :

1. n'affecter aucun port dans le VLAN 1, 2 ou 500 (voir les sections 4.1.1 et 4.1.2) ;
2. ne pas renseigner de numéro de VLAN 1, 2 ou 500 pour les Port VID (se reporter aux éléments à configurer ci-dessous) ;
3. l'option TIA Interface doit être validée [11] sur un autre VLAN que le numéro 1 ou 2 (voir la section 3.2) ;
4. le sous-réseau du VLAN 1 doit être supprimé (se reporter aux éléments à configurer ci-dessous) [11] ;
5. uniquement pour le S615 : l'interface PPPoE doit être affectée sur un autre VLAN que le numéro 1 ou le numéro 2.

Pour chaque équipement, les modifications nécessaires à la suppression (hormis pour l'équipement X310) du VLAN par défaut (le VLAN 1) s'effectuent à partir du menu suivant :

- **pour l'équipement X310**, A partir du menu Switch → VLAN → Port, sélectionner tous les VLAN et modifier chaque numéro Port VLAN ID. Valider la saisie en appuyant sur le bouton Set Values. A partir du menu Switch → VLAN, sélectionner le VLAN 500 et appuyer sur le bouton Delete ;
- **pour l'équipement XB208**, Layer 2 → VLAN → Port Based VLAN, sélectionner chaque VLAN et modifier le numéro Port VID. Valider la saisie en appuyant sur le bouton Set Values. A partir du menu Layer 2 → VLAN → General, sélectionner la case correpondant au VLAN 1 et appuyer sur le bouton Delete ;
- **pour l'équipement XC216**, Layer 2 → VLAN → Port Based VLAN, sélectionner chaque VLAN et modifier le numéro Port VID. Valider la saisie en appuyant sur le bouton Set Values. A partir du menu Layer 3 → Subnet onglet Overview, cocher la case du VLAN 1 et appuyer sur le bouton Delete. A partir du menu Layer 2 → VLAN → General, sélectionner la case correpondant au VLAN 1 et appuyer sur le bouton Delete ;
- **pour l'équipement XM408**, Layer 2 → VLAN → Port Based VLAN, sélectionner chaque VLAN et modifier le numéro Port VID. Valider la saisie en appuyant sur le bouton Set Values. A partir du menu Layer 3 → Subnet onglet Overview, cocher la case du VLAN 1 et appuyer sur le bouton Delete. A partir du menu Layer 2 → VLAN → General, sélectionner la case correpondant au VLAN 1 et appuyer sur le bouton Delete ;
- **pour l'équipement S615**, Layer 2 → VLAN → Port Based VLAN, sélectionner chaque VLAN et modifier le numéro Port VID. Valider la saisie en appuyant sur le bouton Set Values. A partir du menu Layer 3 → Subnet onglet Overview, cocher la case du VLAN 1 et appuyer sur le bouton Delete. Se rendre dans le menu Interfaces → PPP onglet Configuration, sélectionner un

11. Cette configuration ne concerne pas les équipements X310 et XB208.

autre VLAN que celui par défaut. A partir du menu `Layer 2` → `VLAN` → `General`, sélectionner la case correpondant au VLAN 1 et appuyer sur le bouton `Delete`. Supprimer également le VLAN 2 en ayant pris soin d'affecter l'interface externe sur une autre VLAN que ce dernier.

Attention

L'équipement `S615` présente un défaut relatif à la configuration d'un lien de type *trunk*. En effet, l'équipement accepte la configuration de type `access` (U) et `trunk` (T) sur le même port. Ainsi, si le VLAN par défaut n'est pas supprimé ou si les ports `trunk` sont affectés avec ce dernier, il est possible d'effectuer un saut de VLAN à partir du VLAN 1. Il est donc nécessaire de suivre les recommandations 4.1.1 et 4.1.2.

4.2 Mécanismes de redondance de niveau 2

Les mécanismes de redondance de niveau 2 participent à la disponibilité du système. Ils possèdent des propriétés de convergence rapide du réseau mais aucune fonction de sécurité. En effet, tout membre d'une topologie redondante est en mesure d'en perturber le fonctionnement.

Objectif

Mettre en œuvre les configurations permettant de sécuriser la ou les topologie(s) réseau comprenant des liens et/ou des commutateurs redondés.

Attention

L'équipement de type pare-feu `S615` ne supporte pas les protocoles de redondance de niveau 2 dans la version logicielle testée. Il n'est pas en mesure d'interpréter ces types de trames et ainsi de modifier l'état de ses ports. Il ne doit pas participer à une topologie redondante de niveau 2 (STP ou MRP par exemple).

R25

Maîtriser les membres d'une topologie redondante de niveau 2

Il est recommandé que seuls les équipements de confiance utilisant des interconnexions de confiance puissent être membres d'une topologie redondante de niveau 2.

R26

Limiter le nombre de ports liés aux mécanismes de redondance

Il est recommandé que seuls les ports participant à une topologie redondante puissent faire transiter les trames associées au protocole de redondance.

R27

Activer une seule technologie de redondance de niveau 2 par port

Il est recommandé de n'activer qu'une seule technologie de redondance de niveau 2 par port d'accès (la technologie dépendant du besoin métier).

Les descriptions de ces recommandations sont précisées dans les paragraphes qui suivent.

4.2.1 Configuration MRP

Les systèmes industriels (automates ou SCADA par exemple) sont généralement raccordés entre eux au travers d'une topologie réseau en anneau. Le protocole MRP est souvent associé au réseau industriel car il permet de réduire la durée de coupure du réseau lors de la perte d'un équipement ou d'un lien.

Les trames de gestion du protocole MRP doivent être cloisonnées au sein d'un VLAN afin de les isoler des flux métiers. Ceci permet d'éviter d'inonder le réseau de production de flux servant uniquement au fonctionnement du réseau mais aussi de ne pas perturber le fonctionnement du réseau en modifiant des trames des flux de production.

Attention

Pour l'équipement `X310`, le micrologiciel impose que les ports concourant à l'anneau MRP fassent partie du VLAN par défaut (le VLAN 1).

R28

Désactiver MRP sur l'équipement `X310`

Il est recommandé de ne pas utiliser le protocole MRP avec l'équipement `X310`.

Information

Pour les autres équipements, le micrologiciel ne permet pas de définir le VLAN auquel les trames MRP feront partie. En effet, ces ports doivent nécessairement être configurés dans le VLAN d'administration.

Les équipements disposent d'une fonctionnalité permettant d'attribuer automatiquement le rôle alloué à ce dernier dans l'anneau MRP. Cette fonction appelée `Automatic Redundancy Detection` ne doit pas être sélectionnée, en effet, il est préférable de définir le rôle de chaque équipement dans la boucle MRP.

R29

Imposer le rôle du port

Afin d'optimiser la configuration du protocole MRP, il est recommandé d'imposer le rôle de l'équipement au sein de l'anneau MRP.

La configuration des deux ports permettant de faire transiter le protocole de redondance MRP s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, **(l'activation de ce service n'est pas recommandé sur cet équipement)** `X-300` → `Ring Redundancy` → `Ring Config`. A partir de la liste déroulante `Redundancy Mode`, sélectionner `MRP Auto-Manager` ou `MRP Client` selon le rôle à attribuer. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `Ring Redundancy`, onglet `Ring`, cocher la case `Ring Redundancy`. Sélectionner `MRP Auto-Manager` ou `MRP Client` selon le rôle à attribuer. Définir

les ports participant à l'anneau MRP (ces ports doivent appartenir au VLAN d'administration). Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `XC216`, `Layer 2 → Ring Redundancy`, onglet `Ring`, cocher la case `Ring Redundancy`. Sélectionner `MRP Auto-Manager` ou `MRP Client` selon le rôle à attribuer. Définir les ports participant à l'anneau MRP (ces ports doivent appartenir au VLAN d'administration). Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2 → Ring Redundancy`, onglet `Ring`, cocher la case `Ring Redundancy`. Sélectionner `MRP Auto-Manager` ou `MRP Client` selon le rôle à attribuer. Définir les ports participant à l'anneau MRP (ces ports doivent appartenir au VLAN d'administration). Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, ce protocole n'est pas disponible sur cet équipement.

Il est possible de vérifier l'état de la connexion MRP à partir du menu suivant : :

- **pour l'équipement** `X310`, **(l'activation de ce service n'est pas recommandé sur cet équipement)** `X-300 → Ring Redundancy` ;
- **pour l'équipement** `XB208`, `Information → Redundancy`, onglet `Ring Redundancy` ;
- **pour l'équipement** `XC216`, `Information → Redundancy`, onglet `Ring Redundancy` ;
- **pour l'équipement** `XM408`, `Information → Redundancy`, onglet `Ring Redundancy` ;
- **pour l'équipement** `S615`, ce protocole n'est pas disponible sur cet équipement.

4.2.2 Configuration du Spanning Tree

Le protocole *Spanning Tree* (STP) s'adapte à toutes les topologies réseau. Lorsque le STP est activé globalement, tout port est par défaut membre de la topologie. Lorsque que le protocole est désactivé globalement, le commutateur transfère les trames de contrôle STP : les BPDU.

Lorsque que le *Spanning Tree* est activé globalement et explicitement désactivé sur un port, les BPDU provenant de ce port sont bloquées et ne sont pas interprétées, empêchant le commutateur de détecter d'éventuelles boucles.

R30

Configurer explicitement le STP

Il est recommandé d'activer globalement le *Spanning Tree* et de le désactiver sur les ports utilisant un autre mécanisme de redondance de niveau 2 (MRP ou HSR) conformément à la recommandation R27.

Pour chaque commutateur, l'activation globale du protocole STP s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, menu `Switch`, cocher la case STP ou RSTP. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2 → Spanning Tree`, onglet `General`, cocher la case `Spanning Tree` et sélectionner le protocole STP ou RSTP de la liste déroulante `Protocol Compatibility`. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `XC216`, `Layer 2` → `Spanning Tree`, onglet `General`, cocher la case `Spanning Tree` et sélectionner le protocole STP ou RSTP de la liste déroulante `Protocol Compatibility`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `Spanning Tree`, onglet `General`, cocher la case `Spanning Tree` et sélectionner le protocole STP ou RSTP de la liste déroulante `Protocol Compatibility`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, ce protocole n'est pas disponible sur cet équipement.

Pour chaque commutateur, l'activation ou la désactivation du protocole *Spanning Tree* par port s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `STP/RSTP` → `Ports`, sélectionner le port concernée. Décocher la case `(R/M)STP enabled` pour désactiver le service sur le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `Spanning Tree`, onglet `ST Port`. Décocher la case `Spanning Tree Status` pour désactiver le service sur le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `Spanning Tree`, onglet `CIST Port`. Décocher la case `Spanning Tree Status` pour désactiver le service sur le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `Spanning Tree`, onglet `CIST Port`. Décocher la case `Spanning Tree Status` pour désactiver le service sur le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, ce protocole n'est pas disponible sur cet équipement.

Lorsque le protocole STP est activé sur le port d'accès, le commutateur est en attente de réception de trames STP. Si aucune de de ces trames n'est reçue, le port est considéré comme raccordé à un client final et le port est opérationnel (à l'état actif et permettant de transférer des trames quelconques). Cette phase introduit un délai de plusieurs secondes lors du raccordement ou du démarrage d'un client (durant cette phase, le port est actif mais ne permet pas de transférer des trames).

R31

Imposer le mode de fonctionnement du port

Afin d'optimiser la configuration du protocole *Spanning Tree*, il est recommandé d'imposer et d'activer le mode de fonctionnement d'un port d'accès avec la fonction *Edge Port*.

Pour chaque commutateur, le mode de fonctionnement *Edge Port* d'un port STP s'active à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `STP/RSTP` → `Ports`. Sélectionner le port concernée, cocher uniquement la case `Admin Edge Port` et décocher la case `Auto Edge port`. Lorsqu'il ne s'agit pas d'un port d'accès, les options `Admin Edge Port` et `Auto Edge port` doivent être décochées. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `XB208`, `Layer 2 → Spanning Tree`, onglet `ST Port`. Sélectionner le paramètre `Admin` de la liste déroulante `Edge Type`. Lorsqu'il ne s'agit pas d'un port d'accès, le paramètre « - » de la liste déroulante `Edge Type` doit être sélectionnée. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2 → Spanning Tree`, onglet `CIST Port`. Sélectionner le paramètre `Admin` de la liste déroulante `Edge Type`. Lorsqu'il ne s'agit pas d'un port d'accès, le paramètre « - » de la liste déroulante `Edge Type` doit être sélectionnée. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2 → Spanning Tree`, onglet `CIST Port`. Sélectionner le paramètre `Admin` de la liste déroulante `Edge Type`. Lorsqu'il ne s'agit pas d'un port d'accès, le paramètre « - » de la liste déroulante `Edge Type` doit être sélectionnée. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, ce protocole n'est pas disponible sur cet équipement.

Comme précisé dans le document [2], il existe plusieurs attaques sur le protocole STP dont :

- l'écoute du traffic de diffusion en s'autodéclarant commutateur racine (*Root*) ;
- un déni de service par envoi de trames BPDU.

Sur un port d'accès, seul un client peut être raccordé et ainsi aucun BPDU ne doit être émis vers ce port. La fonctionnalité *Root Guard* permet de désactiver le port lorsque celui-ci reçoit un BPDU d'élection *Root*.

Information

Lors d'un changement de topologie de niveau 2 du réseau, une trame de type TCN est émise par l'équipement à l'ensemble du réseau. Lors de la réception de cette trame, chaque équipement réinitialise dans un délai de 15s sa table d'enregistrement des adresses MAC (au lieu de 300s par défaut).

La fonctionnalité de restriction TCN permet de désactiver le port sur réception d'un BPDU de changement de topologie du réseau. La mise en place de ces protections est décrite ci-dessous.

R32

Activer la fonction de sécurité Root Guard sur les ports d'accès

Il est recommandé d'activer la fonction de sécurité *Root Guard* du protocole STP sur les ports d'accès.

Pour chaque commutateur, la fonction *Root Guard* d'un port STP s'active à partir du menu suivant :

- **pour l'équipement** `X310`, cette fonctionnalité n'est pas disponible sur cet équipement ;
- **pour l'équipement** `XB208`, `Layer 2 → Spanning Tree`, onglet `ST Port`. Dans la colonne `Restr. Role`, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** XC216, Layer 2 → Spanning Tree, onglet CIST Port. Dans la colonne Restr. Role, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XM408, Layer 2 → Spanning Tree, onglet CIST Port. Dans la colonne Restr. Role, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** S615, ce protocole n'est pas disponible sur cet équipement.

Information

Lors du déclenchement de la fonctionnalité *Root Guard*, le port est désactivé durant 30s après la réception de la dernière trame BPDU.

R33

Activer la fonction de sécurité Restricted TCN sur les ports d'accès

Il est recommandé d'activer la fonction de sécurité *Restricted TCN* du protocole STP sur les ports d'accès.

Pour chaque commutateur, la fonction *Restricted TCN* d'un port STP s'active à partir du menu suivant :

- **pour l'équipement** X310, cette fonctionnalité n'est pas disponible sur cet équipement ;
- **pour l'équipement** XB208, Layer 2 → Spanning Tree, onglet ST Port. Dans la colonne Restr. TCN, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XC216, Layer 2 → Spanning Tree, onglet CIST Port. Dans la colonne Restr. TCN, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XM408, Layer 2 → Spanning Tree, onglet CIST Port. Dans la colonne Restr. TCN, cocher la case pour le port concerné. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** S615, ce protocole n'est pas disponible sur cet équipement.

Afin de vérifier le fonctionnement du protocole STP, Il est possible d'en visualiser le statut à partir du menu suivant :

- **pour l'équipement** X310, Switch → STP/RSTP et Switch → STP/RSTP → Ports ;
- **pour l'équipement** XB208, Layer 2 → Spanning Tree, onglets ST General et ST Port ;
- **pour l'équipement** XC216, Layer 2 → Spanning Tree, onglets CIST General et CIST Port ;
- **pour l'équipement** XM408, Layer 2 → Spanning Tree, onglets CIST General et CIST Port ;
- **pour l'équipement** S615, ce protocole n'est pas disponible sur cet équipement.

4.3 Sécurisation des ports

Objectif

Mettre en œuvre les configurations permettant de sécuriser les interfaces physiques des équipements.

4.3.1 Ports non connectés

De manière générale, les ports non connectés des équipements peuvent constituer des points d'entrée du SI depuis l'intérieur. Sur des commutateurs, ces ports sont souvent en libre accès. Afin de limiter les erreurs de manipulation lors de l'activation de ces ports, ils sont positionnés dans un VLAN qui ne sera pas utilisé et différent du VLAN 1, le VLAN par défaut et du VLAN dit natif [13].

R34

Désactiver les ports non utilisés

Il est recommandé de désactiver l'ensemble des ports non utilisés et de les positionner en *access* (symbole `U`), dans un VLAN non utilisé et différent du VLAN 1.

Pour chaque équipement, la désactivation des ports non utilisés s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `Ports`. Sélectionner le port concerné et décocher la case `Port enabled`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `Ports`, onglet `Overview`. Sélectionner le port concerné. A partir de la liste déroulante `Status`, sélectionner le paramètre `disable`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `Ports`, onglet `Overview`. Sélectionner le port concerné. A partir de la liste déroulante `Status`, sélectionner le paramètre `disable`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `Ports`, onglet `Overview`. Sélectionner le port concerné. A partir de la liste déroulante `Status`, sélectionner le paramètre `disable`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `Interfaces` → `Ethernet`, onglet `Configuration`. sélectionner le paramètre `disable`. Valider la saisie en appuyant sur le bouton `Set Values`.

Pour chaque équipement, l'isolation des ports non utilisés dans un VLAN non utilisé s'effectue comme l'affectation d'un port d'accès à un VLAN (voir la section 4.1.2) :

- **pour l'équipement** `X310`, `Switch` → `VLAN`, le VLAN non utilisé doit être marqué « **U** » pour chacun des ports non utilisés ;
- **pour l'équipement** `XB208`, `Layer 2` → `VLAN`, onglet `General`, le VLAN non utilisé doit être marqué « **U** » pour chacun des ports non utilisés ;

13. Une définition plus précise des VLAN natif et VLAN par défaut est donnée dans le guide de recommandation des commutateurs [2].

- **pour l'équipement** `XC216`, `Layer 2 → VLAN`, onglet `General`, le VLAN non utilisé doit être marqué « **U** » pour chacun des ports non utilisés ;
- **pour l'équipement** `XM408`, `Layer 2 → VLAN`, onglet `Port Assignment`, le VLAN non utilisé doit être marqué « **U** » pour chacun des ports non utilisés ;
- **pour l'équipement** `S615`, `Layer 2 → VLAN`, onglet `General`, le VLAN non utilisé doit être marqué « **U** » pour chacun des ports non utilisés.

L'isolation des ports et les affectations des VLAN par port sont illustrées sur la figure 4 ci-dessous. Dans cet exemple, les ports 1 et 2 sont des ports d'accès, respectivement associés aux VLAN Y et Z, le port 3 est un port *trunk* et les ports 4 et 5 ne sont pas utilisés (ils doivent être fermés).

VLAN	Port 1	Port 2	Port 3	Port 4	Port 5
VLAN Y	**U**	**F**	**T**	**-**	**-**
VLAN Z	**F**	**U**	**T**	**F**	**-**
VLAN non utilisé(s)	**F**	**F**	**F**	**U**	**U**

TABLE 4 – Exemple d'affectation des VLAN par port

4.3.2 Port security

Les ports non désactivés ou accessibles à des personnes qui ne sont pas de confiance doivent être protégés contre la connexion de matériel illégitime. En effet, une personne mal intentionnée peut raccorder un équipement illégitime ou brancher un autre commutateur afin d'autoriser la connexion à d'autres équipements.

Deux mécanismes permettent de rendre ces attaques moins évidentes : *port security* et 802.1X. Toutefois, le niveau de sécurité qu'ils apportent n'est pas le même. *Port security* permet seulement de limiter le nombre de machines connectées à une même interface d'accès, tandis que 802.1X apporte en plus un mécanisme de contrôle d'accès au niveau du port, qui peut reposer sur des fonctions cryptographiques robustes. La mise en œuvre de ces fonctionnalités est décrite respectivement dans la présente section ainsi qu'à la section 4.3.3.

Table d'adresses MAC

Un commutateur stocke, de manière temporaire (un rafraichissement est réalisé régulièrement), l'association des adresses MAC des postes clients et du numéro de port physique sur lequel ils sont raccordés. Cette association est enregistrée au sein d'un espace mémoire du commutateur, la table d'adresses MAC).

Lorsque la table d'adresses est saturée, selon les modèles de commutateurs, un comportement anormal et dégradé peut se produire. Ce mode dégradé peut se traduire par :

- un rejet des adresses MAC légitimes au profit d'une adresse MAC d'un attaquant ;
- un rejet de toute nouvelle adresse MAC légitime ;
- une diffusion des trames reçues sur l'ensemble des ports de l'équipement.

Le point d'entrée à protéger est le port en mode *access*. En effet, contrairement aux ports de type *trunk*, les ports *access* sont raccordés directement aux équipements clients. Une seule adresse MAC

devrait être présente sur celui-ci puisqu'un seul équipement doit y être connecté. Le mécanisme appelé *port security* permet de restreindre le nombre d'adresses MAC simultanées autorisées à se connecter sur un port en bloquant les trames provenant d'adresses MAC illégitimes (l'apprentissage nécessite une action de l'administrateur ou de l'opérateur de supervision).

R35

Activer la fonction port security

Sur tous les ports en mode *access*, il est recommandé :

- d'activer la fontion *port security* ;
- de limiter le nombre d'adresses MAC dynamiques à 1.

Attention

L'équipement `S615` ne permet pas la mise en place de filtrage par adresse MAC. Il n'est donc pas possible de restreindre le nombre d'adresses MAC autorisées à se connecter sur un port.

Il y a deux façons d'insérer une ou plusieurs adresses MAC légitimes sur les commutateurs :

- manuellement pour chaque adresse MAC ;
- par apprentissage des adresses MAC reçues par l'équipement.

Pour chaque équipement, l'activation de la fonction et l'insertion des adresses MAC légitimes s'effectuent à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `Unicast Filter (ACL)`, onglet `Filtering`. Appuyer sur le bouton `New Entry`, saisir le VLAN concerné, saisir l'adresse MAC légitime (chaque octet devant être séparé par le caractère « : » ou « - ») et sélectionner le port pour lequel l'adresse MAC saisie précédement sera autorisée (la lettre « M » doit figurer sur le port sélectionné). Valider la saisie en appuyant sur le bouton `Set Values` ; Il est possible de faire appel à la fonction d'apprentissage d'adresse(s) MAC et de ne pas réaliser de saisie manuelle. Ceci peut être réalisé à partir du menu suivant : `Switch` → `Unicast Filter (ACL)` → `Learning`. Appuyer sur le bouton `Start learning` pour démarrer l'apprentissage des adresses MAC et appuyer sur le bouton `Stop learning` après un délai jugé significatif par l'utilisateur afin que l'adresse MAC légitime soit présentée sur le port. La sélection du port pour lequel le filtrage doit s'appliquer s'effectue à partir du menu suivant : `Switch` → `Unicast Filter (ACL)` → `Ports`, cocher la case au niveau du port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour les équipements** `XB208`, `XC216` **et** `XM408`, `Layer 2` → `Unicast`, onglet `Filtering`. Sélectionner le VLAN concerné, saisir l'adresse MAC légitime dans le champ `MAC Address` (chaque octet devant être séparé par le caractère « : » ou « - ») et cocher le port pour lequel l'adresse MAC saisie précédement sera autorisée. Valider la saisie en appuyant sur le bouton `Set Values` ; Il est possible de faire appel à la fonction d'apprentissage d'adresse(s) MAC et de ne pas réaliser de saisie manuelle. Ceci peut être réalisé à partir du menu suivant : `Layer 2` → `Unicast`, onglet `Learning`. Appuyer sur le bouton `Start learning` pour démarrer l'apprentissage des adresses

MAC et appuyer sur le bouton `Stop learning` après un délai jugé significatif par l'utilisateur afin que l'adresse MAC légitime soit présentée sur le port. La sélection du port pour lequel le filtrage doit s'appliquer s'effectue à partir du menu suivant : `Layer 2` → `Unicast`, onglet `Locked Ports`, cocher la case `Setting` au niveau du port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `S615`, il n'est pas possible de mettre en place de règles de filtrage de niveau 2 sur cet équipement.

L'activation des *traps* SNMP permet de superviser le déclenchement d'une telle restriction (se référer au chapitre 8.1).

Trap SNMP

Un *trap* SNMP est un type de message du protocole SNMP. Ce message, qui est émis sans sollicitation du serveur SNMP, est transmis lors d'un évènement sur le client SNMP.

4.3.3 Authentification des équipements terminaux

Pour aller plus loin, il est possible d'authentifier les équipements terminaux en mettant en œuvre le protocole 802.1X. Ce type d'authentification nécessite cependant une configuration à la fois sur le commutateur et sur l'équipement terminal. Un serveur d'authentification RADIUS est également nécessaire.

Pour chaque équipement (appelé *client* dans le guide [3]), l'activation du service s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `IEEE 802.1x` → `Ports`. Sélectionner le numéro du port concerné et cocher la case `802.1x Authenticator`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Security` → `AAA`, onglet `802.1X Authenticator`, dans la colonne `802.1X Auth. Control`, sélectionner le paramètre `Auto` de la liste déroulante pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Security` → `AAA`, onglet `802.1X Authenticator`, dans la colonne `802.1X Auth. Control`, sélectionner le paramètre `Auto` de la liste déroulante pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Security` → `AAA`, onglet `802.1X Authenticator`, dans la colonne `802.1X Auth. Control`, sélectionner le paramètre `Auto` de la liste déroulante pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, cette fonctionnalité n'est pas disponible.

Information

Lorsqu'un administrateur modifie le profil d'un compte utilisateur (suppression des droits par exemple), ce dernier sera autorisé à communiquer sur le réseau tant qu'il ne se sera pas authentifié à nouveau. Il existe une option permettant l'authentica-

tion périodique de l'utilisateur sans action de sa part. Il s'agit de réauthentification périodique.

R36

Durcir la configuration du 802.1X

Si le protocole 802.1X est utilisé, il est recommandé d'activer l'option *Reauthentication* (réauthentification périodique de l'équipement terminal) et de modifier la période d'envoi des trames à 300 secondes.

Pour chaque équipement, la mise en place de ces recommandations R36 s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch → IEEE 802.1x → Ports`. Sélectionner le numéro du port concerné et cocher la case `802.1x Re-Authentication`. Saisir la valeur du délai de retransmission dans le champ `802.1x Tx Period[sec]`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Security → AAA`, onglet `General`, cocher la case `802.1x Reauthentication`. Valider la saisie en appuyant sur le bouton `Set Values` ; `Security → AAA`, onglet `802.1X Authenticator`, dans la colonne `Re-Authentication Timeout`, saisir la valeur « 300 » pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Security → AAA`, onglet `General`, cocher la case `802.1x Reauthentication`. Valider la saisie en appuyant sur le bouton `Set Values` ; `Security → AAA`, onglet `802.1X Authenticator`, dans la colonne `Re-Authentication Timeout`, saisir la valeur « 300 » pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Security → AAA`, onglet `General`, cocher la case `802.1x Reauthentication`. Valider la saisie en appuyant sur le bouton `Set Values` ; `Security → AAA`, onglet `802.1X Authenticator`, dans la colonne `Re-Authentication Timeout`, saisir la valeur « 300 » pour le port concerné. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, cette fonctionnalité n'est pas disponible.

Les commutateurs intègrent les méthodes d'authentification suivantes :

- EAP-MD5 ;
- EAP-PEAP ;
- EAP-TLS ;
- EAP-TTLS.

La méthode EAP-MD5 est vulnérable aux attaques par dictionnaire et ne permet pas d'authentification mutuelle.

R37

Respecter les recommandations du guide 802.1X

Si le 802.1X est utilisé, les recommandations du guide 802.1X [3] doivent être respectées.

4.3.4 Limitation de débit

Certaines trames particulières, destinées à tous les ports d'un même VLAN, peuvent fortement dégrader les performances d'un commutateur car elles sont diffusées sur l'ensemble des ports du VLAN. Il s'agit des trames de type *broadcast*, *multicast* et *unknown unicast*. Lors d'un usage classique, ces trames sont peu nombreuses et une limitation de leur nombre n'affecte pas les flux « métier ».

R38

Limiter le trafic de diffusion

Il est recommandé d'activer les mécanismes de limitation de débit sur les trames de type *broadcast*, de *multicast* et d'*unknown unicast*.

Information

Pour les trames de type *Unicast*, deux options de limitation sont présentes sur les équipements `XB208`, `XC216` et `XM408`.

- `Limit Ingress Unicast (DLF)` : il s'agit des trames dont les adresses MAC ne sont pas connues par l'équipement (non présentes en mémoire) ;
- `Limit Ingress Unicast` : il s'agit des adresses MAC déjà connues par l'équipement (présentent en mémoire).

Pour chaque équipement, la limitation s'effectue au travers du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `Load Limits`. Sélectionner le port concerné en cliquant sur son numéro. Pour les deux parties `Ingress` et `Egress`, à partir de la liste déroulante `Mode`. sélectionner le paramètre `All Frames`. A partir de la liste déroulante `Rate`, sélectionner la limitation souhaitée. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `Rate Control`. Pour le port concerné, cocher l'ensemble des cases des différents types de trames à limiter. Saisir ensuite la limitation globale pour le port en entrée dans le champ `Total Ingress Rate` et en sortie dans le champ `Egress Rate`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, Pour le port concerné, cocher l'ensemble des cases des différents types de trames à limiter. Saisir ensuite la limitation globale pour le port en entrée dans le champ `Total Ingress Rate` et en sortie dans le champ `Egress Rate`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `Rate Control`. Pour le port concerné, cocher l'ensemble des cases des différents types de trames à limiter. Saisir ensuite la limitation globale pour le port en entrée dans le champ `Total Ingress Rate` et en sortie dans le champ `Egress Rate`. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `S615`, il n'est pas possible de mettre en place de règles de filtrage de niveau 2 sur cet équipement.

Attention

Certains protocoles industriels utilisent des trames de type *multicast* (OPC-UA en mode PUB/SUB par exemple). Il est nécessaire de vérifier leur fonctionnement dans tous les états et modes du système afin de limiter au bon débit.

5
VPN IPsec

Les systèmes d'information adoptent généralement une architecture distribuée. Les différentes briques logicielles et matérielles qui les composent sont de plus en plus communicantes, non seulement entre elles mais également avec des systèmes d'information distants et à travers des réseaux non maîtrisés tels qu'Internet.

Tout comme ces différentes briques peuvent être critiques pour un système d'information, les flux de communication qu'elles génèrent entre elles peuvent l'être également. Ces flux regroupent de nombreuses informations sensibles (données d'authentification, informations métier confidentielles, commandes d'installations industrielles, etc.). L'interception ou l'altération de ces informations par des individus potentiellement malveillants représente des risques non négligeables dans un contexte où les cyber attaques sont de plus en plus nombreuses et sophistiquées. La protection de ces flux sensibles est alors primordiale.

Force est pourtant de constater que cette problématique n'est pas toujours bien appréhendée, et que de nombreux flux réseau sensibles ne sont pas protégés comme ils le devraient. IPsec est une suite de protocoles de communication sécurisée permettant la protection des flux réseau. Elle est éprouvée mais souvent mal maîtrisée et reste encore trop peu ou mal employée.

Objectif

Sécuriser les échanges entre l'équipement pare-feu `S615` et un équipement compatible par la mise en place de tunnels VPN IPsec en accord avec les recommandations figurant dans le guide [5].

Les cas d'usage d'un VPN IPsec au travers de l'équipement `S615` peuvent être les suivants :

- connexion entre deux équipements `S615` pour sécuriser une communication distante ;
- connexion entre un équipement `S615` et un autre équipement IPsec (pare-feu par exemple) ;
- connexion entre un équipement `S615` et un automate (type S7-1500 par exemple) ;
- connexion entre un équipement `S615` et un serveur SINEMA.

5.1 Authentification

R39

Utiliser l'authentification mutuelle par certificats

Il est recommandé de mettre en œuvre une authentification mutuelle par certificat des correspondants.

La mise en place de cette recommandation nécessite d'importer les fichiers de certificats et de clefs depuis le menu : `System` → `Load&Save`, onglet `HTTP`. Appuyer sur le bouton `Load` de la ligne `X509Cert` et insérer successivement les éléments suivants :

- le certificat de l'autorité de certification (AC) au format *.PEM ;
- le certificat serveur (équipement distant) au format *.PEM ;
- le certificat de l'équipement local `S615` (incluant la clef privée) au format *.P12. [14]

Information

Avant l'insertion du certificat client, il est nécessaire de renseigner le mot de passe de la clef privée à partir de l'onglet `Passwords` et en insérant le mot de passe de la clef privée, dans le champ `Password` de la ligne `X509Cert`.

L'équipement `S615` affecte de façon automatique le type de certificat lors de son chargement. Les critères de reconnaissance pour cette affectation sont les suivants :

- un certificat au format *.PEM chargé sans la clef au format *.KEY est reconnu comme un certificat distant (certificat serveur) ;
- lorsque la clef privée associée au certificat précédent est chargé, le certificat est reconnu comme appartenant à l'équipement local (certificat client) ;
- l'insertion d'un certificat associé à sa clef privée au format *.P12 est reconnu comme certificat client ;
- Si les champs « Issuer DN » et « Subject DN » sont identiques, le certificat est reconnu comme un certificat AC, en effet il n'y a pas de vérification du champ `CA:TRUE`.

La vérification des certificats importés s'effectue à partir du menu `Security` → `Certificates`.

Attention

SIEMENS met à disposition un outil de génération de certificats. L'outil nommé *Security Configuration Tool* (SCT) permet de générer notamment la clef privée du certificat client à insérer dans l'équipement `S615`. Le mécanisme de génération proposé par l'outil n'étant pas connu, son utilisation n'est pas recommandée. Il convient d'utiliser un certificat respectant les recommandations du RGS ([12], [13] et [14]) généré depuis une IGC de confiance.

14. Il est possible d'insérer le certificat client (équipement `S615` local) ainsi que sa clef privée selon deux fichiers distincts, le certificat au format *.PEM et la clef privée au format *.KEY.

R39 -

Utiliser une clef partagée robuste

Si une authentification par clef partagée est choisie pour un VPN IPsec, il est recommandé de mettre en œuvre les recommandations suivantes :

- le secret doit disposer d'une entropie d'au moins 128 bits [15] (22 caractères aléatoires en utilisant comme source les minuscules, les majuscules et les chiffres) ;
- le secret doit respecter les règles relatives à la génération des mots de passe décrites dans le guide de l'ANSSI [16] ;
- une clef partagée différente doit être utilisée pour chaque tunnel ;
- le secret doit être renouvelé régulièrement, sa cryptopériode doit être définie en fonction de la politique de sécurité de l'organisme.

5.2 Profils de chiffrement

La mise en place de VPN IPsec nécessite l'utilisation de mécanismes cryptographiques. Les tableaux 5 et 6 donnent des exemples de profil de chiffrement compatibles avec les préconisations de l'ANSSI [11] et les valeurs proposées par défaut dans l'équipement. Les cryptopériodes [16] indiquées dans ces tableaux ne sont pas directement issues du RGS mais données à titre indicatif. Elles doivent être définies en fonction de la politique de sécurité de l'organisme.

Paramètre	Valeur recommandée	Valeur par défaut
Encryption	AES 128 GCM	AES 128 GCM 16
Hash	SHA 256	SHA 256
Groupe Diffie-Hellman	Groupe 14 (2048 bits)	Groupe 14
Lifetime	6h (360min)	3h (180min)

TABLE 5 – Exemple de profil de chiffrement IKE compatible avec le RGS

Paramètre	Valeur recommandée	valeur par défaut
Encryption	AES 128 GCM	AES 128 GCM 16
Hash	SHA 256	SHA 256
Groupe Diffie-Hellman (PFS)	Groupe 14 (2048 bits)	Groupe 14
Lifetime	1h (60min)	1h (60min)

TABLE 6 – Exemple de profil de chiffrement IPsec compatible avec le RGS

R40

Utiliser des algorithmes cryptographiques robustes

Il est recommandé d'utiliser au minimum les algorithmes AES 128, SHA 256 et le Groupe *Diffie-Hellman* 14 dans les profils de chiffrement IKE et IPsec. Il est recommandé d'utiliser la version 2 d'IKE.

15. Se référer à l'annexe B1 du RGS pour plus de précisions [15].
16. Durée maximale durant laquelle on accepte de perdre la confidentialité et l'intégrité du trafic si le secret venait à être compromis.

R40 -

Ne pas utiliser le mode Aggressive

Si la version 2 d'IKE ne peut être utilisée pour des raisons de compatibilité avec un équipement ou logiciel distant qui n'intègre pas cette version, la fonctionnalité `Aggressive Mode` ne doit pas être utilisée.

La mise en œuvre d'un tunnel IPsec à partir de l'équipement `S615` s'effectue à partir du menu `Security` → `IPSec VPN`.

1. onglet `General`, cocher la case `Activate IPsec VPN` ;
2. onglet `Remote End`, créer un équipement distant en saisissant son nom dans le champ `Remote End Name` et valider en appuyant sur le bouton `Create`. Dans la colonne `Remote Mode`, sélectionner le paramètre `Standard`. Dans la colonne `Remote Type`, sélectionner le paramètre `Manual`. Insérer l'adresse de l'équipement distant dans le champ `Remote Address` avec le masque de sous-réseau en respectant le format x.x.x.x/x (« 10.1.1.2/32 » par exemple) ainsi que le sous-réseau distant dans le champ `Remote Subnet` avec le masque de sous-réseau en respectant le format x.x.x.x/x (« 192.168.1.0/24 » par exemple). Appuyer sur le bouton `Set Values` pour valider les modifications ;
3. onglet `Connections`, créer une connexion VPN en saisissant son nom dans le champ `Connection Name` et valider en appuyant sur le bouton `Create`. Dans la colonne `Keying Protocol`, sélectionner le paramètre `IKEv2`. Dans la colonne `Remote End`, sélectionner le nom de l'équipement distant créé précédemment à partir de l'onglet `Remote End`. Insérer l'adresse du sous-réseau local dans la colonne `Local subnet` avec le masque de sous-réseau en respectant le format x.x.x.x/x (« 192.168.10.0/24 » par exemple). Appuyer sur le bouton `Set Values` pour valider les modifications ;
4. onglet `Authentication`. Dans la colonne `Authentication`, sélectionner `CA Cert` pour une authentification d'un groupe de machine ou `Remote Cert` pour une authentification avec l'équipement distant. Si l'authentification par groupe de machine est sélectionnée, il est nécessaire de choisir le certificat de l'AC (préalablement inséré comme précisé dans la section 5.1) à partir de la liste déroulante `CA Certificate`. Dans le cas d'une authentification avec l'équipement distant, le certificat de ce dernier est à sélectionner à partir de la liste déroulante `Remote Certificate`. Renseigner l'adresse IP (sans le masque de sous-réseau) de l'équipement local `S615` dans la colonne `Local ID` ainsi que l'adresse de l'équipement distant (sans le masque de sous réseau) dans la colonne `Remote ID`. Appuyer sur le bouton `Set Values` pour valider la configuration ;
5. onglet `Phase 1`, sélectionner les algorithmes recommandés dans le tableau 5 du présent guide. La case `Agressive Mode` ne doit pas être cochée. Appuyer sur le bouton `Set Values` pour valider la configuration ;
6. onglet `Phase 2`, sélectionner les algorithmes recommandés dans le tableau 6 du présent guide. La case `Auto Firewall Rules` ne doit pas être cochée. Appuyer sur le bouton `Set Values` pour valider la configuration.

Lorsque la configuration du VPN est réalisée, le démarrage de ce dernier s'effectue à partir du menu `Security` → `IPSec VPN`, onglet `Connections`, colonne `Operation`, sélectionner le mode de fonctionnement de l'équipement `S615` (`Wait` ou *Start* et valider en appuyant sur le bouton `Set Values`.

L'option `Auto Firewall Rules` permet de créer, sans manipulation de la part de l'utilisateur, les règles permettant d'autoriser les flux du VPN IPSec. Lorsqu'elle est activée, il n'est pas possible de consulter les règles implicitement liées à cette fonctionnalité.

R41

Ne pas utiliser les règles automatiques

Il est recommandé de ne pas utiliser la fonction permettant la création « automatique » de régles pour l'autorisation des flux IPSec.

Attention

Les paramètres suivants doivent être conformes avec l'équipement distant afin que la liaison IPSec puisse s'établir :

- version IKE ;
- Remote Address ;
- Remote Subnet ;
- Local ID ;
- Remote ID ;
- les suites cryptographiques (algorithmes de signature, de chiffrement et groupes Diffie-Hellman).

Information

Il est possible de consulter l'état de la connexion VPN à partir du menu `Information → IPSec VPN`.

5.3 Dead Peer Detection

Le mécanisme de *Dead-Peer-Detection* (DPD) effectue une vérification périodique du bon fonctionnement du tunnel grâce à des échanges de messages chiffrés. Si un correspondant ne répond pas aux requêtes envoyées par son pair, il sera alors considéré comme injoignable et l'émetteur fermera le tunnel de son côté.

Il existe différents modes d'utilisation de ce mécanisme, notamment :

- le mode actif, l'équipement `S615` surveille l'état du correspondant et envoie une réponse sur sollicitation de l'équipement distant ;
- le mode passif, l'équipement `S615` ne surveille pas l'état du correspondant et envoie une réponse uniquement sur sollicitation de l'équipement distant.

R42

Activer le mécanisme de Dead-Peer-Detection

Il est recommandé de mettre en œuvre le mécanisme de *Dead-Peer-Detection* en mode actif si le mode de fonctionnement du DPD est connu des deux côtés ou si les deux extrémités sont maîtrisées.

R42 -

Utiliser le mode DPD passif

Si la présence du mécanisme *Dead-Peer-Detection* sur l'extrémité distante n'est pas connue, il est recommandé d'utiliser le mode passif permettant de répondre lorsque une requête DPD est reçue.

La configuration de ce mécanisme s'effectue à partir du menu `Information` → `IPSec VPN`, onglet `Phase 1`. Activer la fonctionnalité en cochant la case `DPD` (DPD actif) pour le VPN IPSec concerné.

6
Réduction de la surface d'attaque

Objectif

Mettre en œuvre les configurations permettant de réduire la surface d'attaque dans le cadre de la gestion des équipements.

Par défaut, plusieurs services permettant la gestion des équipements sont activés. Or, tout service activé et non utilisé ne sert qu'à un attaquant. Il est donc essentiel de réduire les services démarrés au strict nécessaire.

R43

Désactiver les services non utilisés

Il est recommandé de désactiver ou modifier la configuration des services peu fiables, en particulier :

- LLDP ;
- GVRP ;
- FTP (uniquement pour l'équipement `X310`) ;
- PNIO-DCP ;
- PNIO-CM ;
- le serveur DHCP (pour sa désactivation se reporter à la recommandation R3).

Pour chaque équipement, la désactivation du protocole LLDP s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Switch` → `LLDP`. Pour l'ensemble des ports, appuyer sur le rectangle du port concerné afin qu'aucune flèche ne soit présente. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `Layer 2` → `LLDP`, sur la ligne ligne `All Ports`, sélectionner le symbole « - » du menu déroulant `Setting`. Appuyer sur le bouton `Copy to Table` afin que cette option soit prise en compte sur l'ensemble des ports. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `LLDP`, sur la ligne ligne `All Ports`, sélectionner le symbole « - » du menu déroulant `Setting`. Appuyer sur le bouton `Copy to Table` afin que cette option soit prise en compte sur l'ensemble des ports. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `LLDP`, sur la ligne ligne `All Ports`, sélectionner le symbole « - » du menu déroulant `Setting`. Appuyer sur le bouton `Copy to Table` afin que cette

option soit prise en compte sur l'ensemble des ports. Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `S615`, `Layer 2` → `LLDP`, sur la ligne ligne `All Ports`, sélectionner le symbole « - » du menu déroulant `Setting`. Appuyer sur le bouton `Copy to Table` afin que cette option soit prise en compte sur l'ensemble des ports. Valider la saisie en appuyant sur le bouton `Set Values`.

La désactivation du protocole GVRP s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `VLAN` → `GVRP`, décocher les cases pour l'ensemble des ports. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, Cette équipement n'intègre pas le protocole GVRP ; Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `Layer 2` → `VLAN`, onglet `GVRP`. Décocher la case `GVRP`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `Layer 2` → `VLAN`, onglet `GVRP`. Décocher la case `GVRP`. Valider la saisie en appuyant sur le bouton `Set Values`.
- **pour l'équipement** `S615`, cet équipement n'intègre pas le protocole GVRP.

Pour l'équipement `X310`, la désactivation du protocole FTP s'effectue à partir du menu suivant : `Agent`, décocher la case `FTP`. Valider la saisie en appuyant sur le bouton `Set Values`.

Des protocoles SIEMENS sont intégrés dans les équipements pour en effectuer la configuration et l'administration (hormis sur l'équipement `S615`). Ces protocoles ne disposent d'aucun mécanisme de sécurité et sont donc à proscrire ou, en cas de nécessité d'utilisation (pour des besoins de retro-compatibilité), des modifications de configuration sont à réaliser.

Ces protocoles sont les suivants :

- PNIO-DCP (Profinet IO Discovery and Configuration Protocol) : il s'agit d'un protocole de découverte et de configuration d'équipements. Ce dernier est utilisé par les logiciels SINEMA et TIA PORTAL mais également par l'outil PST (configuration d'adresse IP). En désactivant ce protocole, la découverte des équipements est réalisée par les requêtes ICMP et la configuration au travers de SNMPv3 ;
- PNIO-CM (Profinet IO Context Manager) : Ce dernier est utilisé par le logiciel SINEMA Server. En désactivant ce protocole, la découverte des équipements est réalisée par les requêtes ICMP et la configuration au travers de SNMPv3.

SINEMA server

SINEMA est un logiciel permettant la gestion (inventaire, remontée des alarmes, configuration, topologie du réseau, etc.) des équipements industriels SIEMENS (SIMATIC, SCALANCE, etc.). Pour réaliser ces opérations, le logiciel utilise, entre autres, les protocoles PNIO-DCP et PNIO-CM (généralement configurés sur les ports UDP 34964 et 49155 pour la gamme SCALANCE).

La désactivation du protocole PNIO-DCP s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent`, décocher la case `DCP`. Si l'utilisation de ce protocole est rédhibitoire pour l'installation, il est nécessaire de cocher les options `DCP` et `DCP Read Only`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `Configuration`. Sélectionner le paramètre « - » de la liste déroulante `DCP Server`. Si l'utilisation de ce protocole est rédhibitoire pour l'installation, il est nécessaire de sélectionner le paramètre `Read-Only` de la liste déroulante `DCP Server`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `Configuration`. Sélectionner le paramètre « - » de la liste déroulante `DCP Server`. Si l'utilisation de ce protocole est rédhibitoire pour l'installation, il est nécessaire de sélectionner le paramètre `Read-Only` de la liste déroulante `DCP Server`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `Configuration`. Sélectionner le paramètre « - » de la liste déroulante `DCP Server`. Si l'utilisation de ce protocole est rédhibitoire pour l'installation, il est nécessaire de sélectionner le paramètre `Read-Only` de la liste déroulante `DCP Server`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, La mise en œuvre des protocoles PNIO nécessitent l'utilisation d'une clef « Key Plug ». Dans le cas contraire, le service n'est pas activé.

La désactivation du protocole PNIO-CM s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, Le protocole n'est pas intégré à cet équipement ;
- **pour l'équipement** `XB208`, `System`, onglet `General`. Décocher la case `SINEMA Configuration Interface`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System`, onglet `General`. Décocher la case `SINEMA Configuration Interface`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System`, onglet `General`. Décocher la case `SINEMA Configuration Interface`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, La mise en œuvre des protocoles PNIO nécessitent l'utilisation d'une clef « Key Plug ». Dans le cas contraire, le service n'est pas activé.

7
Journalisation

La journalisation fait partie intégrante de la sécurité des SI. C'est une fonctionnalité indispensable à la détection de comportements anormaux ainsi qu'aux recherches de compromission a posteriori.

Objectif

Mettre en œuvre les bonnes pratiques de configuration et de sécurisation des fonctions de journalisation des équipements conformément au recommandations du guide [10].

7.1 Synchronisation horaire et horodatage

Objectif

Disposer d'une heure fiable et homogène sur tous les équipements.

La mise à l'heure ainsi que l'activation de la synchronisation NTP doivent faire partie des premières actions d'initialisation d'un équipement. En effet, certaines fonctionnalités sont fortement liées à l'heure du système, notamment la journalisation et la gestion des certificats. Il est important de disposer d'une heure juste et synchronisée sur une source de temps fiable.

Attention

La validation du protocole SNTP sur l'équipement `X310` entraine l'utilisation de NTPv1. Il est donc recommandé de ne pas l'utiliser.

R44

Activer NTP

Il est recommandé d'activer la synchronisation NTP sécurisée et d'utiliser une ou plusieurs sources de temps fiables.

Information

La configuration du client NTP sécurisé nécessite la mise en place d'un serveur NTP proposant les fonctionnalités d'authentification des clients NTP. Pour les différents

équipements du présent guide (hormis l'équipement X310, les paramètres à saisir sont les suivants :

- l'algorithme de hashage ;
- l'identifiant de clef. Il s'agit généralement d'un numéro incrémenté à partir de « 1 » et se trouvant dans le fichier de configuration du serveur NTP afin de pouvoir identifier les différentes clefs stockées dans ce dernier ;
- la clef partagée avec le serveur.

Pour chaque équipement, la configuration d'un ou plusieurs serveur(s) NTP sécurisé(s) s'effectue à partir du menu suivant :

- **pour l'équipement** X310, Agent, cocher NTP et décocher SNTP. Menu Agent → Time Config → NTP Client. Insérer la ou les adresse(s) du ou des serveur(s) NTP. Sélectionner le paramètre SHA1 de la liste déroulante Auth. Insérer l'identifiant de la clef dans le champ Key ID, la clef partagée dans le champ Key et cocher la case Enable Secure NTP. Valider la saisie en appuyant sur le bouton Set Values ;
- **pour l'équipement** XB208, System → System Time, onglet NTP Client. Insérer l'adresse du premier serveur NTP dans le champ NTP Server Address. Valider la saisie en appuyant sur le bouton Set Values. Pour insérer des serveurs NTP supplémentaires, séletionner l'index « 2 » de la liste déroulante NTP Server Index et appuyer sur le bouton Create ;
- **pour l'équipement** XC216, System → System Time, onglet NTP Client. Insérer l'adresse du premier serveur NTP dans le champ NTP Server Address, sélectionner le paramètre SHA1 de la liste déroulante hash Algorithm et insérer l'identifiant de la clef dans le champ Key ID et la clef partagée dans les champs Key et Key Confirmation. Valider la saisie en appuyant sur le bouton Set Values. Pour insérer des serveurs NTP supplémentaires, séletionner l'index « 2 » de la liste déroulante NTP Server Index et appuyer sur le bouton Create ;
- **pour l'équipement** XM408, System → System Time, onglet NTP Client. Insérer l'adresse du premier serveur NTP dans le champ NTP Server Address, sélectionner le paramètre SHA1 de la liste déroulante hash Algorithm et insérer l'identifiant de la clef dans le champs Key ID et la clef partagée dans les champs Key et Key Confirmation. Valider la saisie en appuyant sur le bouton Set Values. Pour insérer des serveurs NTP supplémentaires, séletionner l'index « 2 » de la liste déroulante NTP Server Index et appuyer sur le bouton Create ;
- **pour l'équipement** S615, System → System Time, onglet NTP Client. Insérer l'adresse du premier serveur NTP dans le champ NTP Server Address, sélectionner le paramètre SHA1 de la liste déroulante hash Algorithm et insérer l'identifiant de la clef dans le champ Key ID et la clef partagée dans les champs Key et Key Confirmation. Valider la saisie en appuyant sur le bouton Set Values. Pour insérer des serveurs NTP supplémentaires, séletionner l'index « 2 » de la liste déroulante NTP Server Index et appuyer sur le bouton Create. Il est nécessaire d'ajouter une règle afin d'autoriser le transfert du protocole NTP comme indiqué dans la recommandation R5.

7.2 Evènements

Les équipements du présent guide émettent des messages d'évènements (alarmes) répartis selon plusieurs catégories : état des ports, fonctionnement du tunnel IPSec, fonction de routage, proto-

cole Spanning Tree, etc. Si certains services ou fonctionnalités ne sont pas mis en œuvre, il n'est pas nécessaire de conserver l'émission des évènements correspondants.

R45

Désactiver l'émission d'évènements non utiles

Il est recommandé de ne pas activer l'émission de trames d'évènements correpondant à une fonctionnalité non utilisée.

Information

Il est noter que la mise en service d'une fonctionnalité engendrera l'émission d'un *traps* SNMP. Cette information est utile afin de detecter l'activation d'un service par un tiers illégitime souhaitant exploiter une vulnérabilité.

Pour chaque équipement, la configuration des évènements à transmettre s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent` → `Event Config`.
  - décocher l'ensemble des évènements de la colonne `E-Mail`. Les autres colonnes devant être cochées sauf pour les éléments ci-dessous ;
  - décocher `RMON Alarm` si l'agent RMON n'est pas utilisé ;
  - décocher `RM State change` si le protocole MRP n'est pas utilisé ;
  - décocher `Port Auth State Change` si le service 802.1X n'est pas utilisé.

  Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `Events`, onglet `configuration`.
  - décocher l'ensemble des évènements de la colonne `E-Mail`. Les autres colonnes devant être cochées sauf pour les éléments ci-dessous ;
  - décocher `RMON Alarm` si l'agent RMON n'est pas utilisé ;
  - décocher `RM State change` si le protocole MRP n'est pas utilisé ;
  - décocher `802.1X Port Authentication State Change` si le service 802.1X n'est pas utilisé.

  Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `Events`, onglet `configuration`.
  - décocher l'ensemble des évènements de la colonne `E-Mail`. Les autres colonnes devant être cochées sauf pour les éléments ci-dessous ;
  - décocher `RMON Alarm` si l'agent RMON n'est pas utilisé ;
  - décocher `RM State change` si le protocole MRP n'est pas utilisé ;
  - décocher `802.1X Port Authentication State Change` si le service 802.1X n'est pas utilisé ;
  - décocher `FMP Status Change` (*Fiber Monitoring Protocol*) si aucun module optique n'est utilisé.

Valider la saisie en appuyant sur le bouton `Set Values` ;

- **pour l'équipement** `XM408`, `System` → `Events`, onglet `configuration`.
  - décocher l'ensemble des évènements de la colonne `E-Mail`. Les autres colonnes devant être cochées sauf pour les éléments ci-dessous ;
  - décocher `RMON Alarm` si l'agent RMON n'est pas utilisé ;
  - décocher `RM State change` si le protocole MRP n'est pas utilisé ;
  - décocher `MRP Interconnection State change` si le protocole MRP n'est pas utilisé ;
  - décocher `802.1X Port Authentication State Change` si le service 802.1X n'est pas utilisé ;
  - décocher `FMP Status Change` (*Fiber Monitoring Protocol*) si aucun module optique n'est utilisé ;
  - décocher `PoE State change` si cette fonction n'est pas utilisée sur l'équipements ;
  - décocher `CLI Script File` ;
  - décocher `OSPF State Change` et `VRRP State Change` si aucun protocole de routage n'est activé sur cet équipement.

  Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `Events`, onglet `configuration`.
  - décocher l'ensemble des évènements de la colonne `E-Mail`. Les autres colonnes devant être cochées sauf pour les éléments ci-dessous ;
  - décocher `DDNS Client Logs` ;
  - décocher `Digital In`, si l'éntrée « DIN » n'est pas utilisée.

  Valider la saisie en appuyant sur le bouton `Set Values` ;

Information

Pour tous les équipements sauf le `X310`, en plus des éléments cités précédemment, il est recommandé de valider l'option suivante : menu `System` → `Fault Monitoring`, onglet `Power Supply`, cocher les cases `Line 1` et `Line 2`. Ceci permet d'activer la surveillance de la perte d'une des alimentations par envoi de *traps* SNMP ou de *logs*.

7.3 Journaux locaux

Chaque équipement permet de consulter les évènements de manière locale. Ces informations sont consultables à partir du menu suivant :

- **pour l'équipement** `X310`, `System` → `Event Log` ;
- **pour l'équipement** `XB208`, `Information` → `Log Table` ;
- **pour l'équipement** `XC216`, `Information` → `Log Table` ;
- **pour l'équipement** `XM408`, `Information` → `Log Table` ;
- **pour l'équipement** `S615`, `Information` → `Log Table`.

7.4 Centralisation des journaux

La centralisation des journaux est une bonne pratique de sécurité des SI. Elle permet de faciliter l'exploitation des informations qu'ils contiennent. Cela permet aussi de conserver une copie des journaux en cas d'effacement sur la machine qui les a générés.

Les journaux sont composés d'informations réparties selon le niveau de gravité des évènements enregistrés. Les niveaux (par ordre d'importance) sont : *Info*, *Warning* et *Critical*. Par exemple, les évènements concernant les connexions locales ou distantes (au travers du protocole SSH) font partie du niveau de sévérité « Info ». Il en est de même pour les évènements liés à la modification de la configuration ou le changement de topologie du réseau. Le niveau de gravité des journaux est communément appelé *severity level* ou niveau de sévérité.

Attention

Pour l'ensemble des équipements, il n'est pas possible de modifier le niveau de sévérité alloué à un évènement.

R46

Activer le niveau de sévérité « Info »

Il est recommandé de configurer le niveau de sévérité des équipements dans la catégorie *Info*.

La configuration du niveau de sévérité pour l'ensemble des journaux s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, Il n'est pas possible d'effectuer la configuration du niveau de sévérité sur cet équipement ;
- **pour l'équipement** `XB208`, `System` → `Events`, onglet `Severity Filters`. Sélectionner le paramètre `Info` dans la liste déroulante correspondant à la ligne `Syslog`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `Events`, onglet `Severity Filters`. Sélectionner le paramètre `Info` dans la liste déroulante correspondant à la ligne `Syslog`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `Events`, onglet `Severity Filters`. Sélectionner le paramètre `Info` dans la liste déroulante correspondant à la ligne `Syslog`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `Events`, onglet `Severity Filters`. Sélectionner le paramètre `Info` dans la liste déroulante correspondant à la ligne `Syslog`. Valider la saisie en appuyant sur le bouton `Set Values`.

R47

Activer la centralisation des journaux

Il est recommandé d'activer l'envoi des journaux vers un serveur de centralisation des journaux central.

Pour chaque équipement, la configuration d'un serveur *syslog* s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent → Syslog Config`. Insérer l'adresse du serveur *syslog* (cet équipement ne permet pas d'ajouter plus d'un serveur *syslog*) dans le champ `Syslog Server IP Address`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System → Syslog Client`. Insérer l'adresse du serveur *syslog* dans le champ `Syslog Server Address` et cocher la case `TLS` (cette dernière fonctionnalité nécessite la mise en place d'un serveur *syslog* TLS). Appuyer sur le bouton `Create` et cocher ensuite la case `Syslog Client` pour valider la fonctionnalité. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System → Syslog Client`. Insérer l'adresse du serveur *syslog* dans le champ `Syslog Server Address` et cocher la case `TLS` (cette dernière fonctionnalité nécessite la mise en place d'un serveur *syslog* TLS). Appuyer sur le bouton `Create` et cocher ensuite la case `Syslog Client` pour valider la fonctionnalité. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System → Syslog Client`. Insérer l'adresse du serveur *syslog* dans le champ `Syslog Server Address` et cocher la case `TLS` (cette dernière fonctionnalité nécessite la mise en place d'un serveur *syslog* TLS). Appuyer sur le bouton `Create` et cocher ensuite la case `Syslog Client` pour valider la fonctionnalité. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System → Syslog Client`. Insérer l'adresse du serveur *syslog* dans le champ `Syslog Server Address` et cocher la case `TLS` (cette dernière fonctionnalité nécessite la mise en place d'un serveur *syslog* TLS). Appuyer sur le bouton `Create` et cocher ensuite la case `Syslog Client` pour valider la fonctionnalité. Valider la saisie en appuyant sur le bouton `Set Values`.

R47 -

Relever les journaux

Lorsque l'envoi des journaux vers un serveur de collecte n'est pas possible, il est recommandé de mettre à jour les procédures d'exploitation et de maintenance afin d'y intégrer l'opération de relève manuelle.

8
Exploitation des équipements

8.1 Supervision des évènements

Objectif

Mettre en œuvre les configurations permettant de concourir à la sécurisation du système de supervision des évènements générés par les équipements *Scalance*.

La supervision des équipements *Scalance* peut être réalisée à partir du protocole SNMP. Il existe plusieurs versions de ce protocole et les deux versions fréquement utilisées sont SNMPv2c et SNMPv3. La version 3 du protocole SNMP apporte les fonctionnalités d'authentification des équipements et la protection en confidentialité des flux SNMP (mode *AuthPriv*).

Le protocole SNMPv3 est implémenté sur l'ensemble des équipements du présent guide. Le protocole SNMP permet également la configuration des équipements. Compte-tenu de la faiblesse du protocole de chiffrement mis en œuvre dans SNMPv3, celui-ci ne doit pas être utilisé à des fins d'administration (comme indiqué dans la recommandation R6).

R48

Utiliser le protocole de supervision SNMPv3

Il est recommandé d'activer uniquement le protocole SNMPv3 et les fonctions d'intégrité et de chiffrement associées (mode *AuthPriv*) et de désactiver les versions antérieures.

Pour chaque équipement, l'activation du protocole SNMPv3 s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent` → `SNMP`. Décocher la case `SNMPv1/v2c/V3` et cocher le paramètre `SNMPv3 Only`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `SNMP`, onglet `General`. A partir de la liste déroulante `SNMP`, sélectionner le paramètre `SNMPv3`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `SNMP`, onglet `General`. A partir de la liste déroulante `SNMP`, sélectionner le paramètre `SNMPv3`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `SNMP`, onglet `General`. A partir de la liste déroulante `SNMP`, sélectionner le paramètre `SNMPv3`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `SNMP`, onglet `General`. A partir de la liste déroulante `SNMP`, sélectionner le paramètre `SNMPv3`. Valider la saisie en appuyant sur le bouton `Set Values`.

Seuls les serveurs de supervision doivent pouvoir se connecter au service SNMP et n'utiliser que des fonctions de supervision. Afin de limiter l'usage du service SNMP aux fonctions de supervision, il est important d'utiliser un compte en lecture seule sur l'équipement.

R49

Dédier un compte à la supervision

Il est recommandé de créer un compte de service en lecture seule dédié à la supervision.

Attention

Contrairement aux autres équipements, il n'est pas possible de sélectionner le type d'algorithme de chiffrement utilisé pour SNMPv3 sur l'équipement `X310`. En effet, ce dernier propose uniquement le standard 3DES.

L'activation du mode *AuthPriv* et des restrictions d'accès des utilisateurs au travers du protocole SNMP s'effectuent à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent` → `SNMP` → `Groups`. Apppuyer sur le bouton `New Entry`.Insérer un nom de groupe, sélectionner le paramètre `Auth/Priv` depuis la liste déroulante `Security Level` et cocher UNIQUEMENT la case `Read`. Valider la saisie en appuyant sur le bouton `Set Values`. Il est ensuite nécessaire de créer un utilisateur qui pourra accéder uniquement en lecture au service SNMP. A partir du menu `Agent` → `SNMP` → `Users`, appuyer sur le bouton `New Entry`, insérer un nom d'utilisateur et sélectionner le groupe créé précédement. Valider la saisie en appuyant sur le bouton `Set Values`. Sélectionner l'algorithme `SHA` à partir de la liste déroulante `Authentication Algorithm`. Saisir les mots de passe d'authentification et de chiffrement correpondant à cet utilisateur sur le serveur SNMP. Valider la saisie en appuyant sur le bouton `Set Values`;
- **pour les équipements** `XB208`, `XC216`, `XM408` **et** `S615`, `System` → `SNMP`, onglet `v3 Groups`. Insérer un nom de groupe, sélectionner le paramètre `Auth/Priv` depuis la liste déroulante `Security Level` et appuyer sur le bouton `Create`. Cocher ensuite UNIQUEMENT la case `Read` du groupe nouvellement créé. Valider la saisie en appuyant sur le bouton `Set Values`. Il est ensuite nécessaire de créer un utilisateur qui pourra accéder uniquement en lecture au service SNMP. A partir du menu `System` → `SNMP`, onglet `v3 Users`, insérer un nom d'utilisateur dans le champ `User Name` et appuyer sur le bouton `Create`. A partir de la liste déroulante `Group Name`, sélectionner le groupe créé précédement. Sélectionner l'algorithme `SHA` à partir de la liste déroulante `Authentication Protocol`. Sélectionner l'algorithme `AES` à partir de la liste déroulante `Privacy Protocol`. Saisir les mots de passe d'authentification et de chiffrement correpondant à cet utilisateur sur le serveur SNMP. Valider la saisie en appuyant sur le bouton `Set Values`.

Pour limiter les connexions aux serveurs de supervision, un filtrage doit être réalisé par un pare-feu extérieur et par le biais d'ACL locales à l'équipement. Les fonctionnalités ACL sont décrites au chapitre 3.2.

R50

Filtrer les connexions à destination de l'interface de supervision

Il est recommandé de filtrer les accès à destination du service SNMP. Seuls les serveurs de supervision doivent pouvoir s'y connecter.

R51

Activer les traps SNMP

Il est recommandé d'activer les *traps* SNMP et de les centraliser sur un serveur de supervision.

Information

Quel que soit l'équipement du présent guide, l'envoi des *traps* SNMP s'effectue avec la version 1 du protocole, y compris si cette version est désactivée de manière globale pour les requêtes provenant du serveur comme décrit ci-dessous.

Pour chaque équipement, la configuration du serveur de collecte s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `Agent` → `SNMP`, cocher la case `Traps`. Menu `Agent` → `SNMP` → `Trap Config`, insérer l'adresse IP du serveur SNMP et cocher la case `Enable Trap`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XB208`, `System` → `SNMP`, onglet `General`, cocher la case `SNMPv1 Traps`. `System` → `SNMP`, onglet `Traps`, insérer l'adresse du serveur SNMP, appuyer sur le bouton `Create` et cocher la case `Trap`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XC216`, `System` → `SNMP`, onglet `General`, cocher la case `SNMPv1 Traps`. `System` → `SNMP`, onglet `Traps`, insérer l'adresse du serveur SNMP, appuyer sur le bouton `Create` et cocher la case `Trap`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `XM408`, `System` → `SNMP`, onglet `General`, cocher la case `SNMPv1 Traps`. `System` → `SNMP`, onglet `Traps`, insérer l'adresse du serveur SNMP, appuyer sur le bouton `Create` et cocher la case `Trap`. Valider la saisie en appuyant sur le bouton `Set Values` ;
- **pour l'équipement** `S615`, `System` → `SNMP`, onglet `General`, cocher la case `SNMPv1 Traps`. `System` → `SNMP`, onglet `Traps`, insérer l'adresse du serveur SNMP, appuyer sur le bouton `Create` et cocher la case `Trap`. Valider la saisie en appuyant sur le bouton `Set Values`.

R52

Configurer les traps SNMP

Pour l'ensemble des équipements, il est récommandé de configurer les évènements SNMP à transmettre au serveur comme décrit à la section 7.2.

8.2 Sauvegarde et mise à jour

Objectif

Mettre en œuvre les configurations permettant de sécuriser l'import et l'export de fichier de configuration et la mise à jour du firmware.

Firmware

Il s'agit d'un programme intégré dans la mémoire physique de l'équipement permettant la gestion des fonctionnalités de ce dernier. Il est appelé micrologiciel en français.

Les équipements disposent d'une fonctionnalité de mise à jour de configuration ou du système d'exploitation au travers du protocole FTP. Ce protocole ne dispose d'aucun mécanisme de protection.

R53

Mettre à jour par un canal sécurisé

Il est recommandé de ne pas mettre à jour les équipements au travers du protocole TFTP et d'utiliser le protocole HTTPS.

Pour chaque équipement, la mise à jour du firmware s'effectue à partir du menu suivant :

- **pour l'équipement** `X310`, `System → Save & Load HTTP`;
- **pour l'équipement** `XB208`, `System → Load&Save`;
- **pour l'équipement** `XC216`, `System → Load&Save`;
- **pour l'équipement** `XM408`, `System → Load&Save`;
- **pour l'équipement** `S615`, `System → Load&Save`.

Information

Les fichiers de configuration des équipements doivent être sauvegardés et versionnés selon une politique de gestion de configuration globale intégrant notamment le nommage des fichiers (par exemple *AAMMJJ_Nom-eqt_version*).

Liste des recommandations

Annexe A

A.1 Produits pour lesquels le micrologiciel est équivalent

Produits Siemens Scalance			
X310	XB208 et XC216	XM408	S615
XR300	XB205	XM416	M804
XR324	XB213		M812
X300	XB216		M816
X302	XC206		M826
X307	XC208		M874
X308	XC224		M876
X320	XF204		RM1224
	XP208		
	XP216		
	XR324		
	XR326		
	XR328		

Bibliographie

[1] *Recommandations pour un usage sécurisé d'(Open)SSH*.
Note technique DAT-NT-007/ANSSI/SDE/NP v1.2, ANSSI, août 2015.
https://www.ssi.gouv.fr/nt-ssh.

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

[3] *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux*.
Guide ANSSI-BP-043 v1.0, ANSSI, août 2018.
https://www.ssi.gouv.fr/guide-802-1X.

[4] *Recommandations de configuration d'un système GNU/Linux*.
Guide ANSSI-BP-028 v1.2, ANSSI, février 2019.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[5] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[6] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[7] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance.

[8] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[9] *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*.
Guide ANSSI-PA-072 v2.0, ANSSI, mars 2020.
https://www.ssi.gouv.fr/controle-acces-videoprotection.

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

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

[12] *RGS Annexe A1 : Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques*.
Référentiel Version 3.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[13] *RGS Annexe A3 : Politique de certification Type certificats de serveurs applicatifs*.
Référentiel Version 3.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[14] *RGS Annexe A4 : Profils de certificats/LCR/OCSP et algorithmes cryptographiques*.
Référentiel Version 3.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[15] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

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

[17] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

Version 1.0 - 11/02/2022 - ANSSI-BP-094

ISBN : 978-2-11-167118-8 (papier)
ISBN : 978-2-11-167119-5 (numérique)
Dépôt légal : 4 février 2022

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN