

# RECOMMANDATIONS DE CONFIGURATION DES COMMUTATEURS ET PARE-FEUX HIRSCHMANN

---

## GUIDE ANSSI

### 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 Hirschmann** ». Il est téléchargeable sur le site [www.ssi.gouv.fr](http://www.ssi.gouv.fr).

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [12].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

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	09/08/2016	Version initiale
1.1	25/07/2017	Corrections typographiques
1.2	27/10/2017	Mise à jour de l'avertissement
1.3	11/02/2022	Modification du statut du document et mise en forme

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Objectif du guide . . . . .	4
1.2	Convention de lecture . . . . .	4
1.3	Liste des sigles et acronymes . . . . .	5
<b>2</b>	<b>Menaces et objectifs des attaquants</b>	<b>6</b>
<b>3</b>	<b>Administration</b>	<b>7</b>
3.1	Réseau dédié à l'administration . . . . .	7
3.1.1	Port physique dédié à l'administration . . . . .	7
3.1.2	Réseau spécifique . . . . .	7
3.2	Accès aux interfaces d'administration . . . . .	8
3.3	Configuration des interfaces d'administration . . . . .	9
3.4	Gestion des comptes utilisateur . . . . .	9
3.4.1	Utilisation de comptes nominatifs . . . . .	10
3.4.2	Comptes locaux et comptes centralisés . . . . .	10
3.4.3	Configuration d'un annuaire LDAP . . . . .	11
3.4.4	Droits d'accès . . . . .	12
3.5	Désactivation/suppression des comptes par défaut . . . . .	12
3.6	Configuration des outils d'administration . . . . .	12
3.6.1	Le client lourd . . . . .	13
3.6.2	Le client léger . . . . .	13
3.6.3	Administration par SSH . . . . .	14
<b>4</b>	<b>Configuration du réseau</b>	<b>15</b>
4.1	Réduction de la surface d'attaque . . . . .	15
4.2	Cloisonnement des réseaux . . . . .	15
4.2.1	Cloisonnement par VLAN . . . . .	16
4.2.2	Ports en mode <i>trunk</i> . . . . .	16
4.2.3	Ports en mode <i>access</i> . . . . .	17
4.3	Mécanismes de redondance de niveau 2 . . . . .	18
4.3.1	Configuration MRP . . . . .	19
4.3.2	Configuration du STP . . . . .	19
4.4	Sécurisation des ports . . . . .	20
4.4.1	Ports non connectés . . . . .	20
4.4.2	<i>Port security</i> . . . . .	20
4.4.3	Authentification des postes terminaux . . . . .	21
4.4.4	Limitation de débit . . . . .	22
4.4.5	<i>DHCP Snooping</i> et <i>ARP Inspection</i> . . . . .	22
<b>5</b>	<b>Journalisation</b>	<b>23</b>
5.1	Synchronisation horaire et horodatage . . . . .	23
5.2	Journaux locaux . . . . .	23
5.3	Centralisation des journaux . . . . .	24
5.4	Journalisation des actions d'administration . . . . .	24

<b>6 Exploitation des équipements</b>	<b>25</b>
6.1 Supervision des évènements . . . . .	25
6.2 Sauvegarde . . . . .	26
<b>Liste des recommandations</b>	<b>27</b>
<b>Bibliographie</b>	<b>29</b>

# 1

## Introduction

### 1.1 Objectif du guide

Ce document a pour objectif de présenter les bonnes pratiques relatives à la sécurisation des commutateurs et des pare-feux *Hirschmann*. 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 sont plus concises et des explications plus détaillées sont disponibles dans les publications de l'ANSSI suivantes :

- un guide portant sur la sécurité des commutateurs [4];
- un guide portant sur les politiques de filtrage [8];
- un guide portant sur les systèmes d'information d'administration [9].

### 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 :



#### Recommandation à l'état de l'art

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



#### 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 de RSP35 et MSP30 sous HiOS 5.0.00 et de pare-feux Eagle-30 sous HisecOS 2.0.01. Quelques adaptations seront nécessaires pour des modèles ou des versions logicielles différentes. Beaucoup de fonctions étant identiques entre les commutateurs et les pare-feux, il ne sera pas fait de distinction dans ce document. Certaines fonctions de niveau 2 (du modèle OSI) sont cependant portées uniquement par les commutateurs.

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 cette note est que seules les personnes autorisées disposent d'un accès physique aux équipements.

## 1.3 Liste des sigles et acronymes

- **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.
- **RADIUS** : *Remote Authentication Dial-In User Service*. Serveur central d'authentification.
- **VLAN** : *Virtual Local Area Network*. Réseau logique de niveau 2.

# 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 davantage que les infrastructures filaires (brouillage de signal) 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.

### 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.

#### 3.1.1 Port physique dédié à l'administration

Il est préférable d'utiliser un port physique dédié à l'administration d'un commutateur ou un pare-feu lorsque cela est possible, afin de ne pas mélanger les flux de gestion 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.

Les restrictions d'accès aux interfaces d'administration depuis un VLAN dédié se configurent en indiquant comme VLAN ID le numéro du VLAN d'administration ( `Basic Settings` → `Network` → `VLAN ID` ).

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 n'est pas envisageable, une séparation logique, utilisant, par exemple, les VLAN, est envisageable sous réserve de respecter les recommandations du guide de l'ANSSI [9].

Des explications plus approfondies sur les VLAN se trouvent à la section 4.2.

## 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.

Cette adresse doit être statique et se configure dans le menu `Basic Settings` → `Network` → `Ip Address Assignment`. Il est nécessaire de valider le bouton `local`.

Plusieurs services sont disponibles pour administrer les équipements. Ils ne permettent cependant pas d'obtenir le même niveau de sécurité. Seules les protocoles SSH et HTTPS doivent être utilisés, les autres devant être désactivés. Leurs configurations s'effectuent dans le menu `Device Security` → `Management Access` → `Server Assignment`.

R4

### Limiter les services d'administration distante

Il est recommandé d'activer uniquement les services SSH et HTTPS pour l'administration distante des équipements.

Le service `HiDiscovery` permet de faciliter la configuration initiale d'un équipement. Par défaut, ce service est exécuté au démarrage de l'équipement. Il n'est cependant pas sécurisé. Il convient de le désactiver dans le menu `Basic Settings` → `Network` → `HiDiscovery Protocol`.

R5

### Désactiver HiDiscovery

Il est recommandé de désactiver le service `HiDiscovery`.

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 6.1 du présent document.

Enfin, seuls les postes d'administration doivent pouvoir se connecter aux équipements. Ces restrictions d'accès peuvent être réalisées par un pare-feu réseau lorsque qu'un réseau d'administration

dédié est utilisé ou par le biais des ACL locales de l'équipement. Ces dernières se configurent dans le menu `Device Security` → `Management Access` → `IP Access Restriction`, activer les restrictions en explicitant le réseau des postes d'administration pour les services SSH et HTTPS. Les autres services doivent être décochés.

R7

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

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

## 3.3 Configuration des interfaces d'administration

Les configurations par défaut des services d'administration nécessitent d'être ajustées. Le serveur SSH utilise des clés cryptographiques afin de s'authentifier. N'ayant pas d'information sur le mécanisme de génération initial de ces clés, il est plus prudent d'en générer de nouvelles par un outils tiers. Conformément au guide sur OpenSSH [2], seules les clés RSA doivent être utilisées et les clefs DSA doivent être supprimées. Le menu à utiliser est le suivant : `Device Security` → `Management Access` → `Server` → `SSH`.

R8

### Remplacer les clés SSH générées par défaut

Il est recommandé de générer de nouvelles clés RSA et de supprimer les clés DSA existantes.

Le serveur HTTPS est configuré par défaut avec un certificat autosigné. Il convient de le remplacer par un certificat respectant le RGS [11] généré depuis une infrastructure de gestion de clef (IGC) de confiance. Le nom DNS de l'équipement doit être présent dans le *Common name* ou 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 du navigateur client.

R9

### Remplacer le certificat HTTPS par défaut

Il est recommandé de remplacer le certificat usine installé par défaut sur l'équipement par un certificat généré depuis une IGC de confiance.

Afin de s'assurer de la fermeture des sessions des administrateurs, un *timeout* est configuré par défaut à 5 min sur les interfaces WEB (`Device Security` → `Management Access` → `WEB`) et sur les interfaces en ligne de commande (`Device Security` → `Management Access` → `CLI`).

R10

### Conserver une fermeture automatique de session

Il est recommandé de conserver une fermeture de session automatique sur les interfaces d'administration.

## 3.4 Gestion des comptes utilisateur

## 3.4.1 Utilisation de comptes nominatifs

Il est recommandé d'utiliser un compte nominatif pour chaque personne autorisée à se connecter à l'équipement, et ce quels que soient ses privilèges. Cette mesure permet d'assurer la traçabilité de l'ensemble des actions réalisées sur l'équipement.

R11

### 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<sup>1</sup> 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.

## 3.4.2 Comptes locaux et comptes centralisés

Les comptes utilisateurs sont de deux sortes :

- les comptes locaux : gérés dans la configuration locale de l'équipement ;
- les comptes centralisés : gérés dans un annuaire du SI.

L'utilisation de comptes centralisés est la méthode d'administration à privilégier. En effet, la gestion des comptes locaux se révèle très lourde dès lors que le nombre d'administrateurs ou d'équipements du SI devient conséquent.

Dans cette configuration, les comptes nominatifs sont créés dans l'annuaire central. Ces comptes sont utilisés par les administrateurs pour effectuer leurs tâches d'administration quotidiennes. Puis, sur chaque équipement, un compte administrateur local de secours non nominatif (ex : « localadmin »), peut être créé. Celui-ci respecte les recommandations des comptes non nominatifs évoquées au à la section 3.4.1. Ce compte étant un compte de secours, il est préférable de ne pas activer les mécanismes de verrouillage du compte en cas d'échecs multiples d'authentification (*User Lock*).

R12

### Mettre en place une gestion centralisée des utilisateurs

Il est recommandé d'utiliser une gestion centralisée des comptes, à l'exception d'un compte local d'administration « de secours ».

Il est par ailleurs recommandé d'utiliser un annuaire dédié aux comptes d'administration du SI, comme expliqué dans le guide [9] de l'ANSSI relatif à l'administration sécurisée des SI.

1. Se reporter au guide [1].

Si les comptes locaux sont utilisés, il est nécessaire de durcir les configurations comme le nombre d'essai, la taille minimale du mot de passe, la politique de mot de passe, etc. Ces paramètres se trouvent dans le menu *Device Security* → *User Management*.

R13

### Durcir les paramètres des comptes locaux

Pour les comptes locaux, il est recommandé de :

- spécifier une taille minimale de mot de passe ;
- limiter le nombre d'essais possibles (par exemple 3) ;
- spécifier une politique de mot de passe ;
- verrouiller l'utilisateur après plusieurs échecs (à l'exception du compte de secours) ;
- utiliser les algorithmes cryptographiques AES et SHA1 pour le protocole SNMP.

Les méthodes d'authentification utilisées ainsi que leurs priorités se configurent dans le menu *Device Security* → *Authentication List*. Configurer l'authentification souhaitée et désactiver l'ensemble des autres méthodes.

R14

### Désactiver les méthodes d'authentification non utilisées

Il est recommandé de désactiver les méthodes d'authentification non utilisées.

## 3.4.3 Configuration d'un annuaire LDAP



### Information

Dans la version étudiée, l'authentification LDAP n'est pas disponible sur les pare-feux eagle-30.

La configuration d'un annuaire LDAP s'effectue dans le menu *Device Security* → *LDAP* → *Configuration*. Pour activer une connexion sécurisée, il est nécessaire d'importer le certificat d'une autorité de certification de confiance et d'imposer une connexion TLS.

R15

### Utiliser une connexion sécurisée à l'annuaire LDAP

Il est recommandé de se connecter à l'annuaire d'authentification à l'aide du protocole sécurisé LDAPS.

Pour permettre l'interrogation de l'annuaire et en particulier pour la gestion des droits d'accès, un compte de service est utilisé. Ce compte doit avoir le minimum de privilèges sur l'annuaire, il doit être en lecture seule et ne pas avoir accès aux champs relatifs aux mots de passe des utilisateurs.

**R16**

### Utiliser un compte de service

Il est recommandé de se connecter à l'annuaire avec un compte de service ayant un accès limité à celui-ci.

## 3.4.4 Droits d'accès

Chaque administrateur 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). Le menu *Device Security* → *User Management* permet de définir les droits que l'on souhaite affecter aux utilisateurs locaux. Le menu *Device Security* → *LDAP* → *Role Mapping* permet de faire correspondre un groupe LDAP ou un attribut LDAP à un rôle défini sur l'équipement.

**R17**

### Ajuster les droits d'administration

Il est recommandé de ne positionner que les droits strictement nécessaires aux tâches des différents administrateurs.

## 3.5 Désactivation/suppression des comptes par défaut

Deux comptes sont présents en sortie d'usine sur les équipements, il s'agit des comptes « admin » et « user ». Après création des comptes tel qu'indiqué précédemment, ils ne sont plus nécessaires pour administrer l'équipement.

**R18**

### Supprimer les comptes usine

Il est recommandé de supprimer les comptes présents par défaut sur les équipements (« admin » et « user »).

## 3.6 Configuration des outils d'administration

Les outils d'administration se présentent sous deux formes :

- un client lourd, offrant une simplicité de configuration puisqu'il est fourni avec la version de Java nécessaire à son fonctionnement ;
- un client léger (navigateur web), téléchargeant une applique Java.

---

1. vendor-specific attribute

## 3.6.1 Le client lourd



### Attention

La version de Java embarquée dans le client lourd n'est pas à jour.

Le comportement du client peut être modifié pour qu'il utilise le binaire Java du système. Cette modification nécessite de faire pointer la variable `JavaExe` des scripts `AppletLauncher.sh` et `HiView.sh` vers le binaire Java du système.



### Attention

En HTTPS, le client lourd adopte le modèle *Trust On First Use*, également adopté par SSH. Il ne vérifie pas la validité du certificat présenté par l'équipement.

Ces deux points peuvent être corrigés en appliquant les recommandations ci-dessous.

## 3.6.2 Le client léger

Le client léger télécharge une applique Java. Il l'exécute en utilisant la version de Java présente sur le système. Cette version peut ainsi être mise à jour, indépendamment du logiciel fourni par l'éditeur.

Le client s'appuie sur le fonctionnement du protocole HTTPS pour authentifier l'équipement auquel il se connecte. Pour ce faire, il est nécessaire d'avoir importé, dans les magasins des autorités de confiance du navigateur<sup>2</sup> et de Java, le certificat de l'autorité de confiance ayant signé le certificat de l'équipement.



### Information

Dans Java, les magasins de certificats utilisés ne sont pas ceux du système d'exploitation, mais ils sont stockés dans des fichiers de type *keystore*. Par défaut, le magasin de certificats des autorités de certification racines de confiance est stocké dans le fichier `cacerts` du sous dossier `.\lib\security\` d'installation de l'environnement d'exécution Java.

Pour lister les certificats par défaut de ce magasin (en se plaçant au préalable dans le sous dossier `.\lib\security\`), il faut exécuter la commande :

```
keytool -list -keystore cacerts
```

Pour importer un certificat `mon_ac.cer` dans ce magasin, il faut exécuter la commande :

```
keytool -keystore cacerts -importcert -alias mon_ac -file mon_ac.cer
```

Toutefois, au sein d'un système d'information où les environnements d'exécution Java sont télédéployés avec une configuration centralisée, il est possible que le

2. Ceci est nécessaire pour les utilisateurs du client léger uniquement.

chemin de ce magasin ait été changé et qu'un magasin maintenu en central soit installé sur les postes utilisateurs par stratégie de sécurité. Pour plus de détails, il est recommandé de consulter le fichier de configuration `deployment.properties` de Java ainsi que le guide sur le sujet [3].

La vérification de l'intégrité de l'appliquette s'effectue de cette manière :

1. le client léger vérifie la validité du certificat présenté par le serveur HTTPS ;
2. le client léger télécharge l'appliquette Java ;
3. Java vérifie la signature de l'appliquette ;
4. l'appliquette vérifie la validité du certificat présenté par le serveur HTTPS.

Cette vérification d'intégrité suppose en prérequis :

- l'import, dans le magasin du client léger et dans le magasin Java du certificat de l'autorité de confiance ayant signée le certificat serveur ;
- l'import, dans le magasin Java, du certificat de l'autorité de confiance ayant signée l'appliquette.

Si ces imports ont été correctement réalisés, un test de connexion ne doit donner lieu à aucun affichage d'un message d'erreur qui résulterait d'une exception de sécurité liée aux certificats.

Dans un contexte déconnecté, il peut être nécessaire de désactiver la vérification de CRL dans le panneau de configuration de Java.

R19

### Ajouter les autorités de confiance dans les magasins de certificats

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

## 3.6.3 Administration par SSH

Les équipements s'administrent également en SSH. Les clients SSH adoptent par défaut le modèle *Trust On First Use* (le fonctionnement TOFU est expliqué dans la note technique OpenSSH [2]). La confiance envers le serveur SSH est établie lors de la première connexion. Il est important de vérifier l'empreinte affichée par le client et de la comparer avec l'empreinte présente sur le serveur. L'interface HTTPS permet de la visualiser avec le menu `Device Security` → `Management Access` → `Server` → `SSH`.

R20

### 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.



# 4

## Configuration du réseau

### 4.1 Réduction de la surface d'attaque

De manière à réduire la surface d'attaque des équipements, les services réseaux non nécessaires doivent être désactivés. Les menus suivants permettent de configurer le LLDP<sup>3</sup> (Diagnostics → LLDP → Configuration), le MMRP<sup>4</sup> (Switching → MRP-IEEE → MMRP), le MVRP<sup>5</sup> (Switching → MRP-IEEE → MVRP), le *DHCP Relay L2* (Advanced → DHCP Relay L2), un serveur DHCP (Advanced → DHCP Server), les protocoles industriels (Advanced → Industrial Protocol)

R21

#### Désactiver les services non utilisés

Il est recommandé de désactiver l'ensemble des services non utilisés, en particulier :

- LLDP ;
- MMRP ;
- MVRP ;
- DHCP Relay L2 ;
- le serveur DHCP ;
- les protocoles industriels non utilisés.

### 4.2 Cloisonnement des réseaux

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 occurrences de collisions et donc de diminuer les performances.

Le cloisonnement peut être physique ou virtuel.

Le premier est plus sécurisé et plus performant, tous les liens sont dédiés et aucun équipement réseau n'est mutualisé. En revanche, il est plus coûteux et les contraintes physiques ne le permettent pas toujours. Le deuxième ne nécessite que des modifications de configuration. Dans ce cas, les liens physiques et les commutateurs sont mutualisés.

3. Link Layer Discovery Protocol.

4. Multiple MAC Registration Protocol.

5. Multiple VLAN Registration Protocol.



### Attention

Avant de choisir entre cloisonnement physique et logique, 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.

## 4.2.1 Cloisonnement par VLAN

Le cloisonnement virtuel des réseaux locaux est associé au concept de VLAN. Les commutateurs *Hirschmann* permettent un cloisonnement par VLAN. Des bonnes pratiques de configuration doivent être respectées.

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

- mode *trunk* : le port est utilisé pour mutualiser les réseaux virtuels. Le commutateur s'interconnecte avec un autre équipement compatible avec cette mutualisation. La norme 802.1Q est utilisée sur les équipements *Hirschmann*. Les trames Ethernet en provenance ou à destination de ces équipements sont marquées par un *tag* d'identification de réseau à l'exception du VLAN natif comme indiqué dans le guide de recommandations des commutateurs [5];
- 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.

Ces modes ne sont pas directement présents sur les équipements *Hirschmann* comme ceci peut être le cas sur d'autres modèles de commutateurs. C'est bien la configuration qui va être fournie au commutateur qui doit imposer l'un des deux modes. Chacun de ces deux modes a des particularités de configuration. Les paragraphes suivants détaillent les spécificités de ces modes et expliquent comment les configurer.

## 4.2.2 Ports en mode trunk

Quand un port est configuré en mode *trunk* seuls les réseaux explicitement autorisés sont acceptés. Cette discrimination se fait par l'utilisation des marquages (*tags*) ayant des valeurs définies par l'administrateur. Seules des trames marquées avec ces valeurs circulent sur ce port. Le VLAN dit natif<sup>6</sup>, bien que non utilisé, doit être configuré avec un identifiant dédié et permettent ainsi de limiter les conséquences d'une erreur de configuration.

Le menu Switching → VLAN → Port permet de configurer :

- le VLAN natif, à positionner par exemple sur 42 (Port VLAN ID);
- le type de trames autorisées, à positionner sur *Admit Only Vlan Tagged* (Acceptable Frame Type);
- le filtrage, à activer impérativement pour que ces paramètres soient appliqués (Ingress Filtering).

---

6. Une définition plus précise des VLAN natif, par défaut et de quarantaine est donnée dans le guide sur les commutateurs [4].

Le menu `Switching` → `VLAN` → `Configuration` permet d'indiquer les VLAN configurés sur ce port et la méthode de transit des paquets. Sur un port en mode *trunk*, seul le symbole `T` doit être présent. Le VLAN par défaut, le VLAN natif, le VLAN de quarantaine ainsi que l'ensemble des VLAN non autorisés à circuler sur ce port doivent être marqués avec le symbole `-`.

R22

### Configurer les ports de type *trunk* de manière sécurisée

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

- changer l'ID du VLAN natif ;
- imposer uniquement des trames marquées ;
- activer le filtrage ;
- configurer les VLAN autorisés comme marqués ;
- désactiver les VLAN par défaut, natif, de quarantaine ainsi que tous les VLAN non autorisés.

## 4.2.3 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, les prises réseaux sont accessibles librement. La configuration du raccordement doit être imposée par le commutateur, en particulier le VLAN d'appartenance.

Le menu `Switching` → `VLAN` → `Port` permet de configurer :

- le VLAN d'appartenance (`Port VLAN ID`) ;
- le type de trames autorisées, à positionner sur `Admit All` (`Acceptable Frame Type`) ;
- le filtrage, à activer impérativement pour que ces paramètres soient appliqués (`Ingress Filtering`).

Le menu `Switching` → `VLAN` → `Configuration` permet d'indiquer les VLAN configurés sur ce port et la méthode de transit des paquets. Sur un port en mode *access*, un seul VLAN doit être configuré, identique au VLAN ID précédemment configuré, et les trames circulent non marquées. Le symbole `U` doit être utilisé. Le VLAN par défaut, le VLAN natif, le VLAN de quarantaine ainsi que tous les autres VLAN doivent être marqués avec le symbole `-`.

Le raccordement sur ce port n'étant pas de confiance, d'autres menaces sont à prendre en compte. Des mécanismes de sécurité supplémentaires doivent être mis en place afin de :

- s'assurer que l'équipement terminal ne peut interagir avec les protocoles de redondance de niveau 2 (voir le chapitre 4.3) ;
- limiter le nombre d'adresses MAC par port (voir le chapitre 4.4).

**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 le VLAN ID du VLAN autorisé ;
- autoriser la circulation des trames non marquées ;
- activer le filtrage ;
- configurer le VLAN autorisé comme non marqué ;
- désactiver les VLAN par défaut, natif, de quarantaine ainsi que tous les autres VLAN ;
- limiter le nombre d'adresses MAC autorisées par port ;
- empêcher toute interaction avec les protocoles de redondance niveau 2.

## 4.3 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. 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.

**R24**

## 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.

**R25**

## Limiter les ports de redondance

Il est recommandé que seuls les ports de l'équipement membres d'une topologie redondante puissent faire transiter les trames associées.

**R26**

## 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.



### Attention

L'équipement de type pare-feu Eagle-30 ne supporte pas les protocoles de redondance niveau 2 dans la version logicielle testée. Il n'est pas en mesure de comprendre ce type

de trame et de les bloquer. Il ne doit pas participer à une topologie redondante de niveau 2.

### 4.3.1 Configuration MRP

Le protocole MRP<sup>7</sup> se configure lorsqu'une topologie en anneau est mise en œuvre. Le menu L2 Redundancy → MRP permet de configurer les deux ports permettant de faire transiter le protocole de redondance et le VLAN associé.

R27

#### Configurer les ports utilisés pour le MRP

Il est recommandé de configurer les ports utilisés pour faire transiter le MRP en mode *trunk* et d'utiliser un VLAN dédié.

### 4.3.2 Configuration du STP

Le protocole STP<sup>8</sup> s'adapte à toutes les topologies. Lorsque qu'il est désactivé globalement (Spanning Tree → Global), le commutateur laisse passer les trames de contrôle STP : les BPDU. Lorsque le STP est activé globalement, tout port est par défaut membre de la topologie. Le menu Spanning Tree → Port → CIST permet d'activer ou de désactiver le *Spanning Tree* par port. 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 les boucles malencontreuses. Sa désactivation peut se montrer contre-productive. Pour se prémunir des boucles, sans s'exposer aux attaques intrinsèques au protocole, il faut activer la fonction de sécurité *BPDU Guard* sur les ports en mode *access*. Elle permet de désactiver le port lorsque celui-ci reçoit un BPDU. Pour l'activer :

- cocher la case *BPDU Guard* dans le menu Switching → L2-Redundancy → Spanning Tree → Global ;
- expliciter le port comme étant un port en mode *access* (*Admin Edge Port*) et désactiver la détection automatique (*Auto Edge Port*) dans le menu Switching → L2-Redundancy → Spanning Tree → Port → CIST.

Par défaut le port reste bloqué jusqu'à l'intervention d'un administrateur. Il est possible de réactiver le port automatiquement au delà d'un certain délai d'attente :

- cocher la case *Auto Disable* dans le menu Switching → L2-Redundancy → Spanning Tree → Global ;
- configurer le délai de réactivation en modifiant le paramètre *Reset Timer* dans le menu Diagnostics → Port → Auto disable → Port<sup>9</sup>.



#### Information

La réactivation ne pourra être effective que si la cause du problème (apparition de trames BPDU sur un port *access*) est corrigée.

7. Media Redundancy Protocol.

8. Spanning Tree Protocol.

9. Par défaut le temps de réactivation n'est pas limité.

Les BPDUs transitent sur le LAN physique et non dans un VLAN dédié. Cependant, afin d'être cohérent et de maintenir un maximum d'isolation entre les VLAN de données et les trames de contrôle, les liens inter-commutateurs utilisant le protocole STP devraient être uniquement des liens *trunk*.

R28

### 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 conformément à la recommandation R26.

R29

### Activer la fonction de sécurité BPDU Guard sur les ports en mode access

Il est recommandé d'activer la fonction de sécurité *BPDU Guard* sur les ports en mode *access*.

## 4.4 Sécurisation des ports



### Objectif

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

### 4.4.1 Ports non connectés

Les ports non connectés des équipements peuvent constituer des points d'entrée du SI. Sur des commutateurs, ces ports sont souvent en libre accès. Il est important de désactiver tous les ports non utilisés en utilisant le menu *Basic Settings* → *Network* → *Port*. Afin de limiter les erreurs de manipulation lors de l'activation de ces ports, ils sont positionnés dans un VLAN de quarantaine en modifiant le paramètre *VLAN ID* (ex : 666) et le filtrage dans le menu *Switching* → *VLAN* → *Port*.

R30

### Désactiver les ports non utilisés

Il est recommandé de désactiver l'ensemble des ports non utilisés et de les positionner dans un VLAN de quarantaine.

### 4.4.2 Port security

Les équipements, en particulier les commutateurs, doivent se prémunir d'un autre type d'attaque consistant à saturer leurs tables d'adresses MAC. Le point d'entrée à protéger est le port en mode *access*. 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. Ce paramètre se configure dans le menu *Network Security* → *Port Security* et l'activation de *trap SNMP* permet de superviser le déclenchement

d'une telle restriction. Le paramètre *auto disable* permet de désactiver le port suite à une tentative de connexion frauduleuse.

Par défaut, lorsque le port est désactivé automatiquement, une réactivation manuelle est nécessaire. La remontée automatique du port est configurable dans le menu `Diagnostics` → `Port` → `Auto Disable` → `Port`. Le nombre de secondes souhaitées avant la réactivation de celui-ci doit être spécifié.

R31

### Activation de la fonction *port security*

Il est recommandé d'activer la fonction *port security* sur les ports *access*, de limiter le nombre d'adresses MAC dynamiques à 1, d'activer *traps on violation* et, si la procédure de l'installation industrielle le permet, de désactiver automatiquement le port.



### Attention

Lorsqu'un équipement est déconnecté d'un port, le commutateur met, par défaut, trente secondes avant de supprimer l'adresse MAC de cet équipement de sa table. Le remplacement rapide d'un équipement par un autre peut entraîner la désactivation du port.

## 4.4.3 Authentification des postes terminaux

Pour aller plus loin, il est possible d'authentifier les équipements terminaux en utilisant le protocole 802.1X. Ce type d'authentification nécessite d'être configuré à la fois sur le commutateur et sur l'équipement terminal. Un serveur d'authentification est nécessaire, il se configure dans le menu `Device Security` → `Authentication list` → `defaultDot1x8021AuthList`. Un serveur RADIUS est généralement utilisé.

Une configuration globale est à réaliser dans le menu `Network Security` → `802.1X Port Authentication` → `Global`. L'authentification se configure ensuite par port dans le menu `Network Security` → `802.1X Port Authentication` → `Port Configuration`.

R32

### Désactiver certains modes 802.1X

Il est recommandé de ne pas activer les modes :

- *Dynamic VLAN creation* (création automatique de VLAN par messages GVRP<sup>10</sup>) ;
- *Monitor Mode* (authentification optionnelle des équipements terminaux).

R33

### Activer certaines options du 802.1X

Si le 802.1X est utilisé, il est recommandé d'activer :

- *Port initialisation* (réinitialisation du port à chaque déconnexion) ;
- *Port reauthentication* (réauthentification périodique de l'équipement terminal) ;
- *Force Authorized* (authentification de l'équipement terminal).

10. Generic VLAN Registration Protocol.

Pour plus d'informations, se reporter au guide ANSSI [6]).

## 4.4.4 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*, *unknown unicast*. Lors d'un usage classique, ces trames sont peu nombreuses et une limitation de leur nombre n'affecte pas les flux métier. Cette limitation se configure en pourcentage ou en paquets par seconde au travers du menu *Switching* → *Rate Limiter*.

R34

### 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*.



### Attention

Certains protocoles industriels utilisent des trames de type *multicast*. Vérifier leur fonctionnement dans tous les états et modes du système afin de limiter au bon débit.

## 4.4.5 DHCP Snooping et ARP Inspection

Les mécanismes de *DHCP snooping* et d'*ARP Inspection* sont des contre-mesures à la mise en place d'un serveur DHCP illégitime et à l'usurpation d'adresses IP. Ces mécanismes se configurent au moyen des menus *Network Security* → *DHCP Snooping* et *Network Security* → *ARP Inspection*. Il est nécessaire de spécifier le port sur lequel se trouve le serveur DHCP. Les alarmes doivent être remontées et analysées.

R35

### Activer le DHCP snooping et l'ARP inspection

Il est recommandé d'activer les mécanismes de *DHCP snooping* et d'*ARP inspection*.



# 5

## 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.

Les recommandations faites dans cette partie sont une déclinaison de celles mentionnées dans le guide de l'ANSSI relatif à la journalisation [7].

### 5.1 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. Il est recommandé d'activer la synchronisation NTP en utilisant plusieurs serveurs de temps internes au SI. Ces serveurs doivent être synchronisés sur des sources de temps fiables. Les menus à utiliser sont : Time → Basic Setting et Time → Sntp → Client.

R36

### Activer NTP

Il est recommandé d'activer la synchronisation NTP en se basant sur plusieurs serveurs de temps internes.

### 5.2 Journaux locaux

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*.

Les recommandations faites dans cette partie sont une déclinaison de celles mentionnées dans le guide relatif à la journalisation [10].

Les journaux sont sauvegardés localement dans un espace tampon circulaire. Il est possible de le déplacer sur une mémoire externe et d'en augmenter sa taille. Le menu idoine est `Diagnostics` → `Persistent Logging`.

R37

### Augmenter la taille du tampon local

Il est recommandé d'activer la journalisation sur le support externe et d'augmenter la taille de l'espace tampon circulaire en cohérence avec la politique de sécurité.

## 5.3 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. L'envoi vers un serveur *syslog* distant se fait par le menu `Diagnostics` → `Syslog`.

Le niveau de gravité des journaux envoyés est défini par le paramètre *minimum severity*. Les fonctions de sécurité de l'équipement remontent leurs événements en *warning* ou en *error*. L'imputabilité sur les interfaces d'administration, les changements d'état des ports ou les modifications de topologie utilisent la valeur *notice*.

R38

### Activer la centralisation des journaux

Il est recommandé d'activer l'envoi des journaux vers un serveur de centralisation des journaux central et de positionner le paramètre *minimum severity* à *notice*.

## 5.4 Journalisation des actions d'administration

Par défaut, les actions d'administration ne sont pas journalisées. Le menu `Diagnostics` → `Report` → `Global` permet d'activer leur journalisation.

R39

### Activer la journalisation des actions d'administration

Il est recommandé de journaliser les actions d'administration suivantes :

- *Console logging* ;
- *CLI logging* ;
- *Log SNMP set*.

# 6

## Exploitation des équipements

### 6.1 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 *Hirschmann*.

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). Par défaut, différentes versions de ce protocole sont activées dans `Device Security` → `Management Access`.

R40

#### Utiliser le protocole de supervision SNMPv3

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

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, un compte de service en lecture seule doit être configuré. Pour limiter les connexions aux serveurs de supervision, un filtrage doit être réalisé par un pare-feu lorsque qu'un réseau d'administration dédié est utilisé et par le biais des ACL locales à l'équipement. Ces dernières se configurent dans le menu `Device Security` → `Management Access` → `IP Access Restriction`.

R41

#### Dédier un compte à la supervision

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

R42

#### 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.

Un certain nombre de fonctions de sécurité mises en place précédemment (*port security*, violations 802.1X, perte de redondance, etc.), ne journalisent pas les évènements dans `syslog` mais envoient

des *trap* SNMP. Il est important d'activer les *traps* afin d'exploiter les éléments remontés par les fonctions de sécurité. Le serveur de collecte se configure dans le menu `Diagnostics` → `Status Configuration` → `Alarms (Trap)`.

R43

### Activer les traps SNMP

Il est recommandé d'activer les *traps* SNMP.

D'autres éléments doivent également être transmis à la supervision de sécurité. Le menu `Diagnostics` → `Status Configuration` → `Device Status` → `Global` permet de transmettre des informations telles que l'état de la boucle de redondance de niveau 2 ou l'extraction de la mémoire externe. L'ensemble des éléments doit être coché. Il en est de même pour le menu `Diagnostics` → `Status Configuration` → `Security Status` → `Global` qui supervise des éléments en lien direct avec la sécurité, par exemple la réactivation des services dangereux ou la modification de paramètres critiques.

R44

### Activer les traps SNMP complémentaires

Il est recommandé d'activer les *traps* SNMP pour l'ensemble des paramètres présents dans `Device Status` et `Security Status`.

## 6.2 Sauvegarde

Les éléments présents dans la configuration ne sont pas tous sécurisés. Cependant, les équipements permettent de chiffrer la configuration avant de l'exporter (`Basic Settings` → `LoadSave` → `Configuration Encryption` → `Set Password`).

R45

### Chiffrer les sauvegardes

Il est recommandé de chiffrer les sauvegardes réalisées.

# Liste des recommandations

<b>R1</b>	Dédier un port à l'administration	7
<b>R2</b>	Créer un réseau d'administration physiquement dédié	7
<b>R2-</b>	Créer un réseau d'administration logiquement dédié	8
<b>R3</b>	Configurer une adresse IP d'administration statique	8
<b>R4</b>	Limiter les services d'administration distante	8
<b>R5</b>	Désactiver HiDiscovery	8
<b>R6</b>	Ne pas utiliser le protocole SNMP pour l'administration distante	8
<b>R7</b>	Filtrer les connexions à destination de l'interface d'administration	9
<b>R8</b>	Remplacer les clés SSH générées par défaut	9
<b>R9</b>	Remplacer le certificat HTTPS par défaut	9
<b>R10</b>	Conserver une fermeture automatique de session	9
<b>R11</b>	Utiliser des comptes nominatifs d'administration	10
<b>R12</b>	Mettre en place une gestion centralisée des utilisateurs	10
<b>R13</b>	Durcir les paramètres des comptes locaux	11
<b>R14</b>	Désactiver les méthodes d'authentification non utilisées	11
<b>R15</b>	Utiliser une connexion sécurisée à l'annuaire LDAP	11
<b>R16</b>	Utiliser un compte de service	12
<b>R17</b>	Ajuster les droits d'administration	12
<b>R18</b>	Supprimer les comptes usine	12
<b>R19</b>	Ajouter les autorités de confiance dans les magasins de certificats	14
<b>R20</b>	Vérifier l'empreinte SSH de l'équipement	14
<b>R21</b>	Désactiver les services non utilisés	15
<b>R22</b>	Configurer les ports de type <i>trunk</i> de manière sécurisée	17
<b>R23</b>	Configurer les ports de type <i>access</i> de manière sécurisée	18
<b>R24</b>	Maîtriser les membres d'une topologie redondante de niveau 2	18
<b>R25</b>	Limiter les ports de redondance	18
<b>R26</b>	Activer une seule technologie de redondance de niveau 2 par port	18
<b>R27</b>	Configurer les ports utilisés pour le MRP	19
<b>R28</b>	Configurer explicitement le STP	20
<b>R29</b>	Activer la fonction de sécurité <i>BPDU Guard</i> sur les ports en mode <i>access</i>	20
<b>R30</b>	Désactiver les ports non utilisés	20
<b>R31</b>	Activation de la fonction <i>port security</i>	21
<b>R32</b>	Désactiver certains modes 802.1X	21
<b>R33</b>	Activer certaines options du 802.1X	22
<b>R34</b>	Limiter le trafic de diffusion	22
<b>R35</b>	Activer le <i>DHCP snooping</i> et l' <i>ARP inspection</i>	22
<b>R36</b>	Activer NTP	23
<b>R37</b>	Augmenter la taille du tampon local	24

<b>R38</b>	Activer la centralisation des journaux	24
<b>R39</b>	Activer la journalisation des actions d'administration	24
<b>R40</b>	Utiliser le protocole de supervision SNMPv3	25
<b>R41</b>	Dédier un compte à la supervision	25
<b>R42</b>	Filtrer les connexions à destination de l'interface de supervision	25
<b>R43</b>	Activer les <i>traps</i> SNMP	26
<b>R44</b>	Activer les <i>traps</i> SNMP complémentaires	26
<b>R45</b>	Chiffrer les sauvegardes	26

# Bibliographie

- [1] *Recommandations de sécurité relatives aux mots de passe.*  
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.  
<https://www.ssi.gouv.fr/mots-de-passe>.
- [2] *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>.
- [3] *Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows.*  
Note technique DAT-NT-008/ANSSI/SDE/NP v2.0, ANSSI, juillet 2016.  
<https://www.ssi.gouv.fr/recos-securite-poste-java>.
- [4] *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>.
- [5] *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>.
- [6] *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>.
- [7] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation.*  
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.  
<https://www.ssi.gouv.fr/journalisation>.
- [8] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu.*  
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.  
<https://www.ssi.gouv.fr/politique-filtrage-parefeu>.
- [9] *Recommandations relatives à l'administration sécurisée des systèmes d'information.*  
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.  
<https://www.ssi.gouv.fr/securisation-admin-si>.
- [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] *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>.

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





Version 1.3 - 11/02/2022 - ANSSI-BP-033

Licence ouverte / Open Licence (Étalab - v2.0)

ISBN : 978-2-11-167116-4 (papier)

ISBN : 978-2-11-167117-1 (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.gov.fr](http://www.ssi.gov.fr) / [conseil.technique@ssi.gov.fr](mailto:conseil.technique@ssi.gov.fr)

