

# RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION

---

## GUIDE ANSSI

ANSSI-PA-022  
11/05/2021

### PUBLIC VISÉ :

Développeur

Administrateur

RSSI

DSI

Utilisateur





# Informations



## Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations relatives à l'administration sécurisée des systèmes d'information** ». 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 [28].

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	20/02/2015	Version initiale
2.0	24/04/2018	Prise en compte des retours d'expérience, réorganisation des chapitres & refonte graphique
3.0	11/05/2021	Ajout d'un chapitre sur l'administration par des tiers et l'assistance à distance, mises à jour détaillées en annexe A

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Objectif du guide . . . . .	4
1.2	Organisation du guide . . . . .	4
1.3	Convention de lecture . . . . .	4
<b>2</b>	<b>Les administrateurs, acteurs clés de la sécurité du système d'information</b>	<b>6</b>
2.1	Les administrateurs dans l'écosystème du SI de l'entité . . . . .	6
2.2	Droits et devoirs des administrateurs . . . . .	8
<b>3</b>	<b>Généralités sur le système d'information d'administration</b>	<b>10</b>
3.1	Analyse de risque et objectifs de sécurité . . . . .	10
3.1.1	Analyse de risque . . . . .	10
3.1.2	Objectifs de sécurité . . . . .	10
3.2	Zones de confiance et zones d'administration . . . . .	11
3.3	Produits qualifiés par l'ANSSI . . . . .	12
3.4	Confiance dans le cloisonnement des environnements virtualisés . . . . .	13
<b>4</b>	<b>Poste d'administration</b>	<b>15</b>
4.1	Maîtrise du poste d'administration . . . . .	15
4.2	Architecture du poste d'administration . . . . .	15
4.2.1	Un poste d'administration dédié . . . . .	16
4.2.2	Un poste d'administration multi-niveaux . . . . .	16
4.2.3	Un poste d'administration avec accès distant au SI bureautique . . . . .	17
4.3	Mesures de sécurisation du poste d'administration . . . . .	20
4.3.1	Accès à Internet . . . . .	20
4.3.2	Sécurisation logicielle . . . . .	20
4.3.3	Chiffrement . . . . .	22
<b>5</b>	<b>Réseau d'administration</b>	<b>23</b>
5.1	Protection des ressources d'administration . . . . .	23
5.2	Accès aux ressources administrées . . . . .	24
5.2.1	Sécurisation locale de l'accès aux ressources administrées . . . . .	25
5.2.2	Mise en œuvre d'une interface d'administration dédiée . . . . .	25
5.2.3	Cas d'un réseau étendu . . . . .	27
<b>6</b>	<b>Outils d'administration</b>	<b>29</b>
6.1	Cloisonnement des outils d'administration . . . . .	29
6.1.1	Outils d'administration locaux . . . . .	29
6.1.2	Outils d'administration centralisés . . . . .	29
6.2	Sécurisation des flux d'administration . . . . .	30
6.3	Rupture ou continuité des flux d'administration . . . . .	31
<b>7</b>	<b>Identification, authentification et droits d'administration</b>	<b>33</b>
7.1	Identification . . . . .	33
7.2	Authentification . . . . .	35

7.3 Droits d'administration . . . . .	37
<b>8 Maintien en condition de sécurité</b>	<b>39</b>
<b>9 Sauvegarde, journalisation et supervision de la sécurité</b>	<b>41</b>
9.1 Sauvegarde . . . . .	41
9.2 Journalisation et supervision de la sécurité . . . . .	41
<b>10 Administration à distance et nomadisme</b>	<b>43</b>
<b>11 Systèmes d'échanges sécurisés</b>	<b>46</b>
11.1 Échanges au sein du SI d'administration . . . . .	46
11.2 Échanges en dehors du SI d'administration . . . . .	46
<b>12 Administration par des tiers et assistance à distance</b>	<b>49</b>
12.1 Administration par des tiers . . . . .	49
12.1.1 Qualification PAMS . . . . .	49
12.1.2 Administration ponctuelle à distance par des tiers . . . . .	50
12.2 Assistance à distance . . . . .	54
12.2.1 Utilisation d'un boîtier matériel d'acquisition vidéo . . . . .	55
12.2.2 Mise en œuvre d'une solution logicielle collaborative dédiée . . . . .	55
<b>13 Cas particuliers d'architectures de SI d'administration</b>	<b>57</b>
13.1 Utilisation d'un bastion . . . . .	57
13.2 Possible mutualisation du poste d'administration . . . . .	58
13.3 Une ou plusieurs solutions de poste d'administration ? . . . . .	59
13.4 Administration des ressources d'administration . . . . .	60
13.5 Administration d'un SI déconnecté . . . . .	61
13.6 Administration de ressources dans un <i>cloud</i> public . . . . .	62
<b>Liste des recommandations</b>	<b>63</b>
<b>Annexe A Évolutions du guide</b>	<b>65</b>
A.1 Nouvelles recommandations . . . . .	65
A.2 Mises à jour entre les versions 2.0 et 3.0 . . . . .	65
A.3 Matrice de rétrocompatibilité depuis la version 1.0 vers les versions ultérieures . . . . .	66
<b>Annexe B Aspects juridiques</b>	<b>67</b>
<b>Annexe C Glossaire</b>	<b>70</b>
<b>Bibliographie</b>	<b>72</b>

# 1

## Introduction

### 1.1 Objectif du guide

L'administration d'un SI se traduit par un ensemble de mesures techniques et non techniques visant entre autres à maintenir le SI en condition opérationnelle et de sécurité et à gérer des changements mineurs ou des évolutions majeures.

Ce guide décrit les objectifs de sécurité et les principes d'élaboration d'une architecture technique sécurisée d'administration. Il propose des éléments utiles d'aide à la conception. Il présente quelques cas d'usages concrets mais n'a pas vocation à être exhaustif.

Ce document s'adresse à des lecteurs qui disposent de connaissances minimales pour appréhender les recommandations de sécurité présentées, capables de les adapter à leur contexte et à leurs besoins. Chacun doit s'appuyer également sur la politique de sécurité du système d'information de son entité et sur les résultats d'une analyse de risque pour déterminer les recommandations les plus pertinentes à mettre en œuvre.

### 1.2 Organisation du guide

Ce guide tente d'aborder l'ensemble des thèmes liés à l'administration d'un SI et liste des recommandations dont l'implémentation peut être plus ou moins complexe suivant le contexte de l'entité. L'application linéaire de ce guide ne saurait être adaptée à tous les contextes.

Après une première lecture pour s'appropriier les concepts, il est recommandé d'évaluer le niveau de maturité de l'entité sur le sujet de l'administration d'un SI à l'aide de la liste des recommandations (p. 63). Pour chaque recommandation, préciser si elle est « *respectée* », « *partiellement respectée* » ou « *non respectée* ». Une fois synthétisée, cette analyse peut être le point de départ d'un plan d'actions visant le respect le plus exhaustif possible des recommandations du guide tout en gardant un esprit critique vis-à-vis du contexte d'application.

### 1.3 Convention de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*.

Pour certaines recommandations de ce guide, 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 :

- |             |  |
|-------------|--|
| <b>R</b>    | <b>Recommandation à l'état de l'art</b><br>Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.   |
| <b>R -</b>  | <b>Recommandation alternative de premier niveau</b><br>Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.   |
| <b>R --</b> | <b>Recommandation alternative de second niveau</b><br>Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.  |
| <b>R +</b>  | <b>Recommandation renforcée complémentaire</b><br>Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée en priorité aux entités qui sont matures en sécurité des systèmes d'information. |

La liste récapitulative des recommandations est disponible en page 63.

# 2

## Les administrateurs, acteurs clés de la sécurité du système d'information

Ce chapitre introductif, consacré au rôle d'administrateur, vise à présenter l'ensemble du lexique relatif à l'administration du SI et sert donc de référence pour l'ensemble du document. Il est également un résumé des différentes thématiques abordées.

### 2.1 Les administrateurs dans l'écosystème du SI de l'entité

Un administrateur est non seulement un acteur essentiel du système d'information mais aussi un contributeur majeur pour sa sécurité. Il peut être un salarié de l'entité (on parle d'*administrateur interne*) ou un sous-traitant de l'entité (on parle d'*administrateur externe*), indépendamment du lieu d'activité. De plus, qu'il soit administrateur technique (réseau, système) ou administrateur métier, les besoins d'accès et de privilèges ne sont généralement pas uniformes ; les administrateurs peuvent être regroupés par catégories.

Un administrateur est une ressource critique investie de capacités techniques d'accès aux informations métier de l'entité. En effet, il se distingue des autres utilisateurs par les privilèges qui lui sont accordés sur le système d'information. Il dispose de *droits d'administration* nécessaires à la bonne réalisation d'*actions d'administration*.



#### Actions d'administration

Ensemble des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système participant au SI et susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.

Il est nécessaire de dissocier clairement les différents rôles d'un administrateur sur le SI : un rôle d'utilisateur standard du SI sans privilèges particuliers et un ou plusieurs rôles d'administrateur. Cela se traduit entre autres par la création d'un compte utilisateur standard pour utiliser le SI hors administration et d'un ou plusieurs *comptes d'administration* dédiés aux actions d'administration. L'identification et l'authentification des administrateurs sont les sujets du chapitre 7.

Un poste utilisé pour les actions d'administration, dénommé *poste d'administration*, est un terminal matériel ; il peut être fixe ou portable suivant les besoins. Il est l'objet du chapitre 4.

Un administrateur réalise ses actions grâce à des *outils d'administration*, généralement logiciels, mis à sa disposition sur un poste d'administration ou sur des serveurs dédiés. Un client SSH, une



console centralisée de gestion d'annuaire, un portail Web d'administration de pare-feu sont des exemples d'outils d'administration. Le chapitre 6 aborde ce sujet.

En cas d'accès distant d'un administrateur (ex. : astreinte à domicile, déplacement), on parle d'*administration à distance* dans le chapitre 10. Le cas particulier de l'administration ou l'assistance à distance par des tiers est abordé dans le chapitre 12.

Partie intégrante du SI de l'entité au sens large, le *système d'information d'administration* est le sujet de ce guide. Il inclut toutes les *ressources d'administration* nécessaires pour administrer le SI considéré dont les *postes d'administration*, les *serveurs d'outils d'administration* et les *infrastructures d'administration* nécessaires à son bon fonctionnement (serveurs d'annuaire, DNS, etc.).

Ces ressources sont connectées sur un *réseau d'administration*, réseau de communication faisant transiter les flux internes au SI d'administration et les *flux d'administration* à destination des *ressources administrées*. Ce réseau est évoqué dans le chapitre 5.

La figure 2.1, à titre d'exemple, est un résumé sous forme de représentation fonctionnelle.

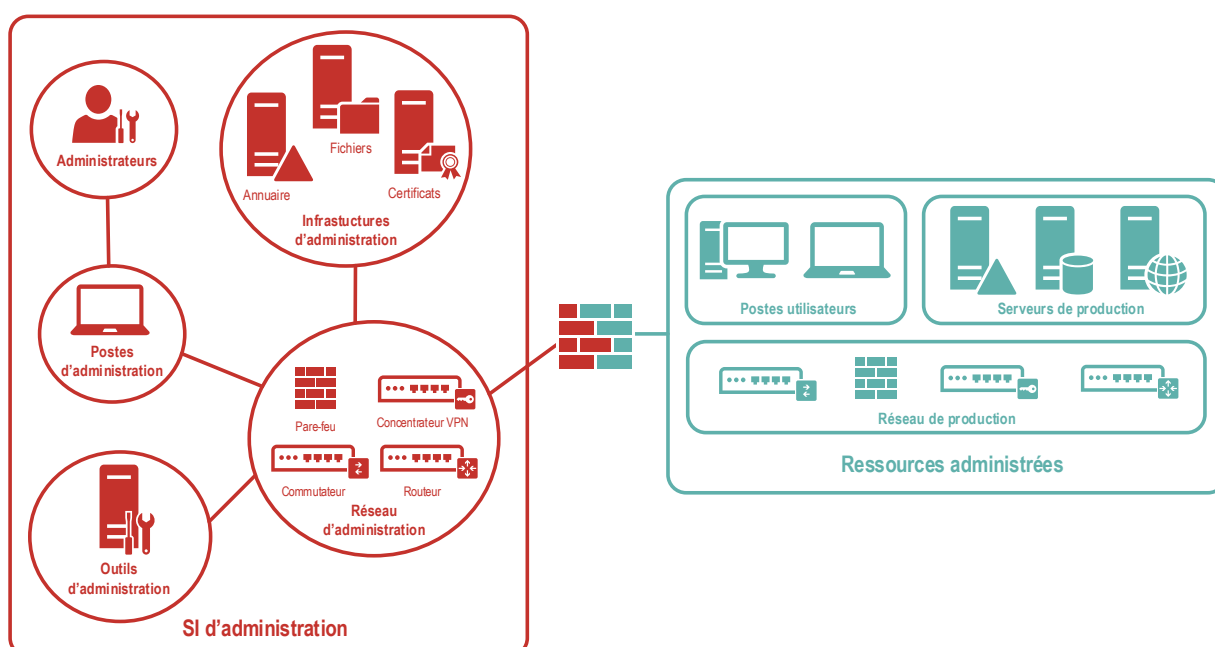


FIGURE 2.1 – Représentation fonctionnelle d'un SI d'administration et de ressources administrées

En périphérie du SI d'administration, un système d'échange sécurisé, illustré par la figure 2.2 et présenté dans le chapitre 11, peut être positionné pour des échanges avec d'autres SI (ex. : un SI bureautique connecté à Internet).

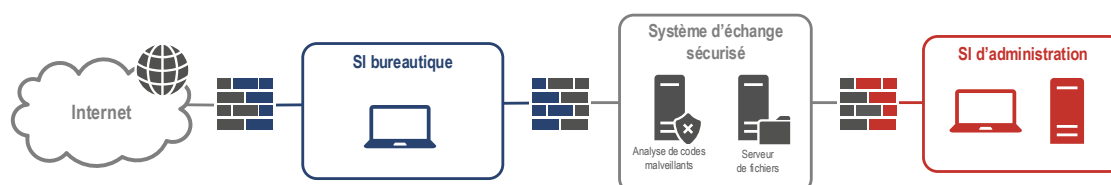


FIGURE 2.2 – Représentation fonctionnelle d'un système d'échange sécurisé

## 2.2 Droits et devoirs des administrateurs

Les fonctions d'administrateur, complexes, doivent s'équilibrer entre un grand pouvoir impliquant de grandes responsabilités et le respect d'obligations précises. En particulier, un administrateur d'un système d'information est tenu à des obligations de loyauté (respect des règles d'éthique), de transparence (respect du règlement intérieur et de la charte informatique) et de confidentialité<sup>1</sup> (respect du secret professionnel). Le non-respect de ces obligations peut donner lieu à des sanctions disciplinaires (allant jusqu'au licenciement pour faute grave), voire des sanctions pénales. L'annexe B traite plus en détail les aspects juridiques, notamment les différents droits et devoirs des administrateurs.

En premier lieu, les droits et obligations des salariés, dont font partie les administrateurs, pour l'utilisation des moyens informatiques doivent être consignés dans une charte informatique annexée au règlement intérieur ou au contrat de travail. L'entité peut prévoir en complément une charte informatique spécifique applicable aux administrateurs. Cette charte doit notamment appeler les administrateurs à la vigilance vis-à-vis des ressources d'administration mises à leur disposition et sur les conduites à tenir en cas de compromission avérée ou suspectée, de perte ou de vol. Pour toute question relative à la sécurité des systèmes d'information (SSI), un administrateur doit pouvoir s'adresser à des référents internes de l'entité, clairement identifiés, techniques ou non techniques.

R1

### Informers les administrateurs de leurs droits et devoirs

Un administrateur doit être informé de ses droits et devoirs, notamment en s'appuyant sur la charte informatique de l'entité.

Il est recommandé d'élaborer une charte informatique spécifique applicable aux administrateurs.

Le rôle d'administrateur nécessite non seulement une confiance forte de l'entité au regard de la criticité de ses actions sur le SI mais également des compétences techniques élevées. Les formations initiale et continue des administrateurs sont indispensables pour garantir la maîtrise de toutes les compétences requises par l'exercice de leurs fonctions.

R2

### Former les administrateurs à l'état de l'art en matière de SSI

En tant que ressource humaine critique pour le SI, un administrateur doit être formé à l'état de l'art, dans ses domaines de compétences et en sécurité des systèmes d'information (ex. : sécurité des systèmes, sécurité des réseaux, infrastructure de gestion de clés).

Le guide d'hygiène informatique de l'ANSSI [13] doit être connu.

Quels que soient l'organisation de l'entité et le partage des responsabilités (entre architectes et administrateurs par exemple), il est essentiel de concevoir et de maintenir à jour la documentation des SI : schémas d'architecture, plans d'adressage IP, matrices de flux, inventaire des comptes privilégiés, etc.

1. Se reporter au guide pour les employeurs et les salariés élaboré par la CNIL [1] dont notamment la fiche n°7 pour les administrateurs.

R3

### Disposer d'une documentation des SI à jour

Les administrateurs doivent disposer de documents reflétant fidèlement l'état courant des SI qu'ils administrent, notamment des cartographies du SI (physique, système, réseau, applications) faisant notamment apparaître clairement les interconnexions avec l'extérieur.

# 3

## Généralités sur le système d'information d'administration

### 3.1 Analyse de risque et objectifs de sécurité

Les ressources d'administration sont des cibles privilégiées par un attaquant. En effet, les droits élevés nécessaires à la réalisation des actions d'administration et les larges accès généralement attribués exposent ces ressources à une menace élevée. Dans de nombreux cas de compromission ou d'intrusion sur ces équipements, l'attaquant prend le contrôle de l'ensemble du SI.

#### 3.1.1 Analyse de risque

Ce guide n'a pas vocation à établir une analyse de risque exhaustive ; ce travail essentiel, propre à chaque système d'information, incombe aux entités en ayant la responsabilité, en liaison avec les responsables de la sécurité des systèmes d'information (RSSI). L'analyse de risque peut être menée avec la méthode EBIOS *Risk Manager* [18] par exemple.

Ainsi, les architectures du SI d'administration peuvent varier en fonction de la criticité du SI administré ou des usages par différentes populations d'administrateurs, chacun ne relevant pas du même niveau de confiance, par exemple entre administrateurs internes et externes.

R4

#### Mener une analyse de risque sur le SI d'administration et son écosystème

Avant toute étude des mesures techniques à mettre en œuvre, une analyse de risque doit être menée en portant une attention particulière sur les besoins de sécurité du SI d'administration et ses interconnexions.

Dans une démarche d'amélioration continue, il est recommandé que l'analyse de risque et la mise en œuvre des mesures induites soient revues au moins une fois par an.

#### 3.1.2 Objectifs de sécurité

Le premier objectif de sécurité des recommandations de ce guide est de protéger le SI d'administration de toute tentative de compromission. En effet, le scénario de compromission le plus fréquent est l'exécution d'un code malveillant sur le poste d'administration – ou sur un poste sur lequel un administrateur s'est connecté avec ses privilèges d'administrateur. Ce code malveillant peut être introduit par le biais d'une navigation Web, par l'ouverture d'une pièce jointe dans un courriel piégé ou à partir d'un support amovible.



## Scénario d'attaque

Un code malveillant peut profiter par exemple des privilèges élevés de la session d'un administrateur pour exécuter des actions telles que :

- le vol des empreintes de mots de passe sur le poste, par exemple par une copie mémoire (ex. : attaque *Pass The Hash* qui permet la réutilisation de ces empreintes pour accéder, sans connaître le mot de passe et donc sans devoir le recouvrer, aux ressources du système d'information);
- l'installation d'un logiciel espion (ex. : cheval de Troie, enregistreur de frappes clavier – *keylogger*);
- l'accès à un serveur de commande et de contrôle<sup>2</sup>;
- la diffusion d'un ver informatique.

Le deuxième objectif de sécurité est de protéger le SI administré des intrusions et compromissions pour lesquelles le SI d'administration serait un vecteur d'attaque. Dans ce cas, on cherche à minimiser les conséquences sur le SI administré d'une compromission du SI d'administration. Du fait des privilèges élevés du SI d'administration sur le SI administré, une action malveillante reste possible mais un cloisonnement adéquat du SI d'administration doit permettre d'éviter une compromission totale du SI administré.

## 3.2 Zones de confiance et zones d'administration

Pour réduire la surface d'exposition aux attaques informatiques et les conséquences en cas de compromission, il est nécessaire de procéder à un découpage du SI administré en zones homogènes dites *zones de confiance* puis d'en déduire des *zones d'administration* au sein du SI d'administration.



### Zone de confiance

Une zone de confiance comprend exclusivement des ressources homogènes; elle est administrée par des administrateurs de même niveau de confiance.

Le découpage du SI administré en zones de confiance peut être déterminé par la combinaison de plusieurs critères d'homogénéité, parmi lesquels :

- de criticité métier (ex. : haute, moyenne, basse);
- organisationnels (ex. : administration interne ou infogérée);
- d'exposition (ex. : à Internet, à des fournisseurs, exclusivement interne);
- réglementaires (ex. : données de santé, données personnelles, données relevant du secret de la défense nationale);
- géographiques (ex. : découpage par pays).

Par défaut, à une zone de confiance correspond une zone d'administration. Les cas de mutualisation sont évoqués dans la section 13.2.

2. Un serveur de commande et de contrôle (C&C) est un ordinateur qui donne des ordres aux équipements infectés par un logiciel malveillant et qui reçoit des informations de ces équipements.

Ce découpage du SI administré (et les conséquences sur le SI d'administration pour la définition des zones d'administration) doit être mené aussi bien en phase de conception initiale qu'avant toute évolution significative du SI administré. Il permet en effet d'alimenter les travaux d'architecture afin que soit traité dans la continuité l'ensemble des besoins d'administration.

Des mécanismes techniques de cloisonnement sont alors mis en œuvre pour matérialiser les zones d'administration : filtrage, chiffrement, authentification, etc. Ainsi, en respectant le principe du moindre privilège, un administrateur donné n'a accès qu'à la ou les zones d'administration dont il a le juste besoin opérationnel, sans possibilité technique d'accéder à une autre zone.

R5

### Définir les zones de confiance du SI administré et déduire les zones d'administration

Avant toute étude d'architecture du SI d'administration, un découpage du SI administré en zones de confiance doit être réalisé. Ce travail permet de déduire un découpage du SI d'administration en zones d'administration.

## 3.3 Produits qualifiés par l'ANSSI

La qualification [27] prononcée par l'ANSSI permet d'attester d'un certain niveau de sécurité et de confiance dans les produits<sup>3</sup> et les prestataires de service. Ce processus permet de s'assurer notamment que des produits remplissent les objectifs de sécurité définis dans des cibles de sécurité préalablement approuvées.

Il est recommandé de recourir à des produits qualifiés pour la protection du SI d'administration même si l'entité n'est soumise à aucun texte réglementaire. Une attention particulière sera portée sur la cible de sécurité qui précise le périmètre qualifié du produit (ex. : le filtrage dynamique des flux IP aux niveaux 3 et 4 pour un pare-feu) ainsi que les hypothèses d'environnement.

R6

### Privilégier l'utilisation de produits qualifiés par l'ANSSI

D'une manière générale, il est recommandé que les matériels et les logiciels utilisés pour protéger le SI d'administration soient qualifiés par l'ANSSI au niveau requis par les besoins de sécurité.

À défaut, il est recommandé qu'ils disposent d'un autre visa de sécurité délivré par l'ANSSI<sup>4</sup>.



### Attention

Il est recommandé d'être toujours attentif aux versions de matériel ou logiciel auxquelles ils s'appliquent ainsi qu'à la définition de la cible de sécurité.

3. La qualification des produits par l'ANSSI comporte trois niveaux : élémentaire, standard et renforcé.

4. Se reporter à <https://www.ssi.gouv.fr/visa-de-securite>.

## 3.4 Confiance dans le cloisonnement des environnements virtualisés

L'emploi des technologies de virtualisation est désormais courant afin de mutualiser les ressources, simplifier les tâches d'exploitation et réduire les coûts. Toutefois, la confiance dans une solution de virtualisation dépend essentiellement de la confiance accordée aux mécanismes de cloisonnement permettant la cohabitation de plusieurs environnements d'exécution sur un même socle physique. Du point de vue de la sécurité, ces mécanismes doivent garantir une étanchéité équivalente à celle d'environnements physiquement distincts.

En pratique, le processus de qualification évoqué dans la section 3.3 est difficilement applicable aux technologies de virtualisation au vu de la complexité de la conception et des développements ainsi que des multiples cas d'intégration.

En conséquence, le principe de précaution doit prévaloir : par défaut, on considère donc que le cloisonnement entre deux environnements virtualisés, hébergés sur un même socle physique, ne garantit pas un niveau de confiance suffisant du point de vue de la sécurité. Ce constat s'applique à tout type de ressource virtualisable, non seulement les serveurs et les ressources de stockage mais également les équipements réseau (routeurs, commutateurs, etc.), les équipements de sécurité (pare-feux, concentrateurs VPN, etc.) ou autres.

Dès lors, la virtualisation sur un même socle physique ne peut être utilisée que pour faire cohabiter des instances d'une même zone de confiance, ayant entre autres :

- les mêmes besoins de sécurité (confidentialité, intégrité, disponibilité) ;
- le même niveau d'exposition, c'est-à-dire accessibles depuis des zones et par des personnes d'un niveau de confiance et de privilège homogène.

Dans le cas présent, le principe de précaution consiste donc à dédier des socles physiques de virtualisation pour l'administration de SI.

À titre d'exemple, un serveur outils et un serveur de fichiers du SI d'administration, s'ils sont virtualisés, peuvent être hébergés sur un même socle physique sous réserve que celui-ci leur soit dédié et qu'il soit par exemple différent de celui utilisé pour des applications métier (cf. figure 3.1).

Dans un autre domaine technique, des équipements virtualisés de routage et de filtrage pour les flux internes au SI d'administration ne doivent pas non plus être mutualisés sur le même socle physique que des équipements virtualisés permettant l'accès aux services de production. De plus, la virtualisation des équipements de sécurité sur des hyperviseurs n'est pas à privilégier dans une infrastructure physique (cf. les raisons techniques dans l'annexe du guide [19]).

R7

### Dédier des socles physiques en cas de virtualisation des infrastructures d'administration

En cas de virtualisation d'infrastructures d'administration, les instances virtuelles correspondantes doivent être déployées sur des socles physiques dédiés, non mutualisés avec d'autres infrastructures virtualisées.



FIGURE 3.1 – Cloisonnement des socles physiques de virtualisation pour des serveurs



### Attention

De manière générale, les produits de virtualisation, complexes, nécessitent une parfaite maîtrise pour garantir un usage sécurisé : configuration du réseau interne, connaissance des flux d'information entre les machines virtuelles, mise en place ciblée de chiffrement authentifié, etc.



# 4

## Poste d'administration

### 4.1 Maîtrise du poste d'administration

En tant que point d'entrée du SI d'administration, le poste de travail de l'administrateur est un composant critique par nature car il dispose d'accès étendus et privilégiés. En outre, il traite généralement des informations sensibles pour le système d'information (configurations, dossiers d'architecture, versions logicielles déployées, mots de passe, etc.) et a la capacité technique d'accéder à des informations métier. Il doit donc faire l'objet d'une sécurisation physique et logicielle afin de restreindre au mieux les risques de compromission.

En premier lieu, il est indispensable que l'entité garde la maîtrise du poste d'administration qu'elle met à disposition des administrateurs, que ceux-ci soient internes ou externes. Toute pratique de type « *Bring Your Own Device* » (BYOD<sup>5</sup>), non recommandée de manière générale, est à proscrire pour un poste d'administration.

R8

#### Gérer et configurer le poste d'administration

Le poste d'administration doit être géré par l'entité – ou à défaut un prestataire mandaté. *En aucun cas* l'utilisation d'un équipement personnel ne doit être tolérée pour l'administration d'un SI.



#### Attention

S'agissant du risque de piégeage matériel, au-delà de maîtriser le processus d'approvisionnement et notamment ses conditions de sécurité, il convient de sensibiliser les administrateurs à la protection physique de leur poste d'administration.

### 4.2 Architecture du poste d'administration

Pour répondre à la dualité des besoins des administrateurs (réalisation des actions d'administration depuis un environnement sécurisé d'une part et accès à un SI bureautique<sup>6</sup> en tant qu'utilisateur d'autre part), trois solutions d'architecture sont envisageables. Elles sont présentées par niveau de sécurité décroissant au regard des objectifs de sécurité fixés :

- un poste d'administration dédié ;
- un poste d'administration multi-niveaux ;
- un poste d'administration avec accès distant à un SI bureautique.

5. Terme français équivalent : AVEC – Apportez votre équipement personnel de communication.

6. On convient de parler de SI bureautique au sens large, c'est-à-dire tout ce qui n'est pas le SI d'administration.

## 4.2.1 Un poste d'administration dédié

La solution qui offre la meilleure garantie du point de vue sécurité consiste à utiliser deux postes physiquement distincts (cf. figure 4.1), respectivement pour les actions d'administration et pour les autres usages (ex. : accès aux services bureautiques, accès à Internet).

R9

### Utiliser un poste d'administration dédié

La principale mesure de sécurité consiste à dédier un poste de travail physique aux actions d'administration. Ce poste doit être distinct du poste permettant d'accéder aux ressources conventionnelles accessibles sur le SI de l'entité (ressources métier, messagerie interne, gestion documentaire, Internet, etc.).

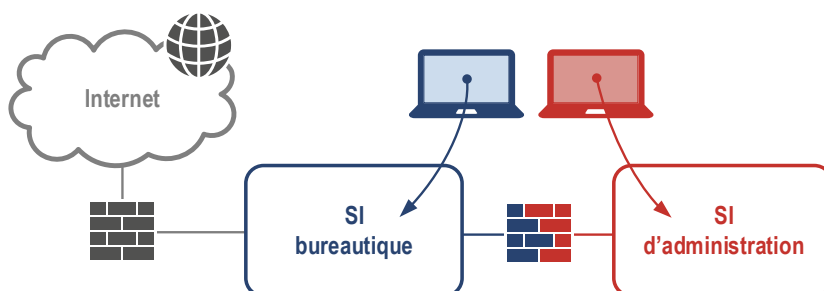


FIGURE 4.1 – Poste d'administration dédié

## 4.2.2 Un poste d'administration multi-niveaux

Le principe d'un poste multi-niveaux consiste à disposer de plusieurs environnements logiciels (généralement deux) sur un même poste physique grâce à l'emploi des technologies de virtualisation ou de conteneurisation. CLIP OS est un exemple de système multi-niveaux *open source*.

Des mécanismes de durcissement du noyau et de cloisonnement permettent d'isoler ces environnements pour réduire les risques de compromission du niveau de sensibilité haute ou de fuite d'information depuis le niveau de sensibilité haute (ici, le SI d'administration) vers le niveau de sensibilité basse (ici, le SI bureautique).

Cette solution (cf. figure 4.2) offre un niveau de sécurité moindre qu'une séparation physique. Dans ce cas exclusif du poste d'administration dérogeant à R7, elle doit impérativement faire l'objet d'une évaluation de confiance des mécanismes d'isolation et de cloisonnement. En effet, l'emploi de cette solution, si elle n'est pas de confiance, peut donner un faux sentiment de sécurité. Il est par ailleurs préférable que ces mécanismes soient gérés au niveau du système, et non par une application utilisateur (cf. figures 4.3 et 4.4).

R9 -

### Utiliser un poste d'administration multi-niveaux

À défaut d'un poste d'administration physiquement dédié, l'emploi de technologies de virtualisation ou de conteneurisation pour obtenir un système multi-niveaux peut être envisagé, dans la mesure où le cloisonnement des environnements est réalisé par des mécanismes évalués comme étant de confiance au niveau système.

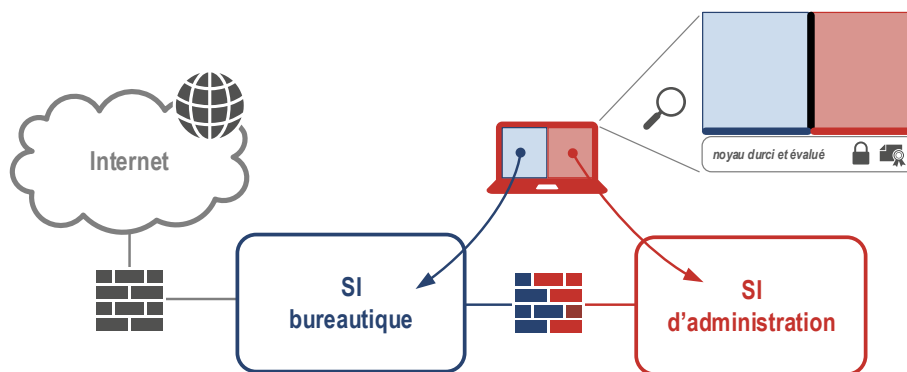


FIGURE 4.2 – Poste d'administration multi-niveaux

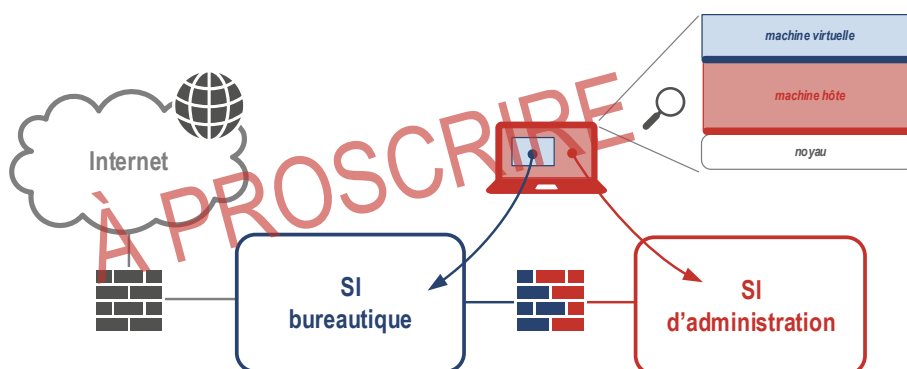


FIGURE 4.3 – Poste d'administration hébergeant une machine virtuelle bureautique

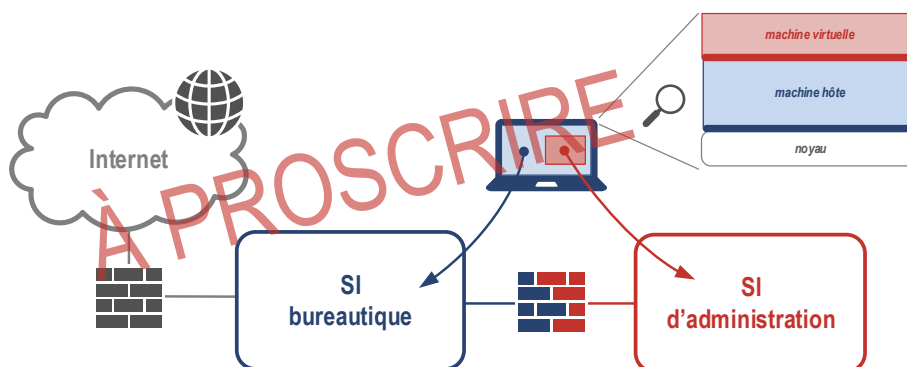


FIGURE 4.4 – Poste bureautique hébergeant une machine virtuelle d'administration

### 4.2.3 Un poste d'administration avec accès distant au SI bureautique

Une dernière solution, d'un niveau de sécurité moindre, consiste en l'emploi au quotidien d'un poste d'administration physique permettant un accès au SI bureautique par connexion à distance (cf. figure 4.5).

Dans cette architecture, la surface d'attaque du SI d'administration est en effet augmentée par l'utilisation d'un client de connexion à distance exécuté sur le poste d'administration. En cas de

compromission du serveur de connexion à distance situé dans le SI bureautique, un attaquant pourrait alors remonter le canal de communication établi pour compromettre le poste d'administration.

Cette pratique nécessite dans tous les cas une maîtrise plus forte de l'interconnexion entre les deux SI.



### Attention

Il est à noter que la solution inverse, qui consiste à accéder depuis un poste bureautique à un poste d'administration par connexion à distance, est à proscrire (cf. figure 4.6).

En effet, le poste bureautique ayant potentiellement accès à Internet, sa compromission pourrait permettre à un attaquant d'espionner les actions effectuées depuis le poste (frappes clavier, copies d'écran), en particulier les connexions initiées vers le poste d'administration (ex. : adresse IP, mot de passe).

Un attaquant pourrait alors rejouer ces connexions et, par rebond, accéder aux outils d'administration puis au SI administré.

De plus, l'utilisation d'un logiciel de connexion à distance nécessite des précautions de configuration qui visent à restreindre les fonctions d'échange entre le système local (administration) et le système distant (bureautique). Faute d'évaluation à la date de rédaction de ce document, les mécanismes d'échange des logiciels de connexion à distance ne peuvent pas être, *a priori*, considérés comme étant de confiance.

De manière non exhaustive, les fonctions d'échange d'informations à désactiver sont :

- les fonctions avancées de copier/coller (en complément de l'activation d'un contrôle sur le volume ou le format) ;
- le partage d'écran ;
- la fonction de prise en charge des périphériques (USB, imprimantes, etc.) ;
- les partages réseaux.

Dès lors, la mise en place d'un système d'échange sécurisé, détaillé dans le chapitre 11, peut être nécessaire.

Dans ce cas dérogatoire d'architecture, il est impératif que :

- un filtrage des flux de connexion à distance vers le réseau bureautique soit effectué par un pare-feu ;
- l'authentification sur le poste d'administration soit réalisée en utilisant l'annuaire du SI d'administration ;
- l'authentification sur l'environnement bureautique soit réalisée en utilisant l'annuaire du SI bureautique.

## Utiliser un poste d'administration avec accès distant au SI bureautique

À défaut d'un poste d'administration physiquement distinct du poste bureautique ou d'un système multi-niveaux de confiance, une solution d'un niveau de sécurité moindre peut consister à ce que les administrateurs :

- utilisent un poste physique pour les actions d'administration ;
- accèdent, par connexion à distance uniquement, à leur environnement bureautique (physique ou virtuel, par exemple : *Virtual Desktop Infrastructure*) depuis ce poste d'administration.

Dans ce cas, les fonctions permettant un échange d'informations entre les deux environnements doivent être désactivées.



### Attention

Il est à noter que cette solution est déconseillée pour l'administration d'infrastructures critiques (ex. : hyperviseurs, annuaires).

Par ailleurs, pour être en mesure de réagir dans les meilleurs délais en cas de crise, il est recommandé de disposer d'une procédure pour désactiver l'accès distant au SI bureautique depuis les postes d'administration.

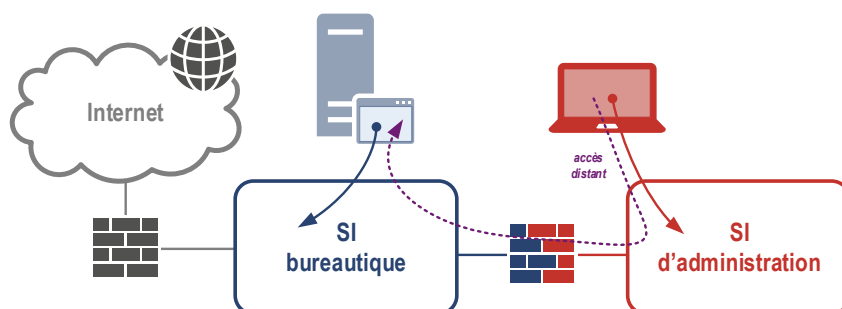


FIGURE 4.5 – Poste d'administration physique avec accès distant à un environnement bureautique virtualisé

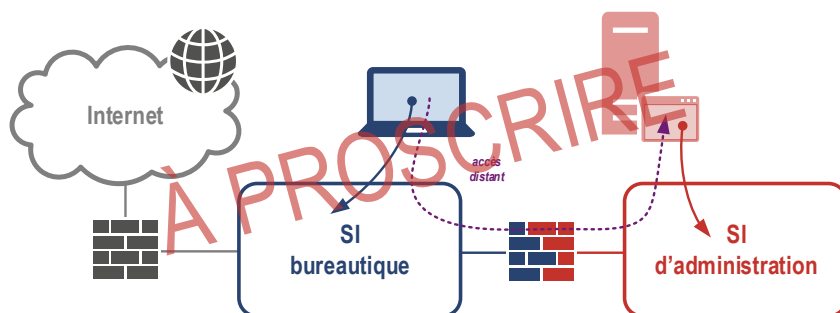


FIGURE 4.6 – Poste bureautique physique avec accès distant à un environnement d'administration virtualisé



## Information

En complément de la présentation de ces trois solutions d'architecture du poste d'administration, la section 13.3 aborde la cohabitation de plusieurs solutions.

# 4.3 Mesures de sécurisation du poste d'administration



## Information

Toutes les recommandations suivantes s'appliquent quelle que soit la solution d'architecture choisie précédemment pour le poste d'administration.

## 4.3.1 Accès à Internet

L'accès à Internet augmente significativement la surface d'exposition aux attaques informatiques et favorise un grand nombre de vecteurs d'attaque : navigation Web, courriel, ouverture de fichiers ou exécution de programmes téléchargés, etc. Ainsi, il est très difficile de garantir l'intégrité d'un poste ayant accès à Internet.

**R10**

## Bloquer tout accès à Internet depuis ou vers le poste d'administration

Le poste d'administration ne doit *en aucun cas* avoir accès à Internet. Cette recommandation inclut en particulier la navigation Web et l'usage de messageries électroniques connectées à Internet, même si ces services sont filtrés par des passerelles sécurisées d'accès Internet.

Par conséquent, l'accès à Internet et aux comptes de messagerie électronique ne peut être autorisé qu'à partir des environnements bureautiques, eux-mêmes soumis à un filtrage au travers des passerelles d'accès Internet de l'entité.

S'agissant de la récupération sur Internet des mises à jour de sécurité du poste, la mise en œuvre de serveurs relais est détaillée dans le chapitre 8. Les autres échanges depuis ou vers Internet sont traités dans le chapitre 11 sur les systèmes d'échange.

## 4.3.2 Sécurisation logicielle

Pour réduire les risques de compromission du poste d'administration, la maîtrise et le durcissement de son socle logiciel et de sa configuration sont impératifs.

Des actions de configuration doivent être menées pour la sécurité du système d'exploitation. Pour cela, il est recommandé de se référer aux guides de sécurité proposés par les éditeurs. Ces derniers décrivent des configurations adaptées à leurs solutions et constituent une première étape dans la sécurisation du socle. L'ANSSI publie également des guides à cet effet, par exemple sur Linux [5], Applocker [10] ou Windows 10 [9] [8].

## Durcir le système d'exploitation du poste d'administration

Les guides de sécurisation des socles des éditeurs doivent être appliqués. Au minimum, les points suivants doivent être traités :

- la désactivation des services inutiles ;
- l'application de droits restreints au juste besoin opérationnel ;
- l'activation et la configuration du pare-feu local pour interdire toute connexion entrante et limiter les flux sortants au juste besoin ;
- le durcissement des configurations systèmes (par exemple pour Windows : GPO, Applocker, SRP ou, pour Linux : SELinux, AppArmor, durcissement du noyau) ;
- l'activation de l'ensemble des mécanismes de mise à jour dans le respect des recommandations du chapitre 8 dédié au maintien en condition de sécurité.

Les administrateurs ne doivent pas pouvoir modifier la configuration du poste d'administration. Pour cela, ils ne doivent pas être intégrés au groupe local « administrateurs » du poste. La majeure partie des actions d'administration est généralement réalisée à partir des navigateurs Web, d'outils de type clients lourds ou en ligne de commande (ex. : ssh) et ne nécessite donc pas de privilèges particuliers sur le poste.

Cette mesure remplit un double objectif : prévenir une erreur humaine qui entraînerait un abaissement du niveau de sécurité du poste et limiter les conséquences de l'exécution d'un code malveillant.

## Restreindre les droits d'administration sur le poste d'administration

Par défaut, les administrateurs ne doivent pas disposer des droits d'administration sur leur poste d'administration. Ces droits doivent être attribués uniquement aux administrateurs en charge de l'administration des postes d'administration.

De façon à restreindre significativement la surface d'exposition du système, il convient d'utiliser uniquement des logiciels – ainsi que leurs mises à jour – préalablement validés suivant un processus de contrôle défini. Pour cela, des vérifications cumulables sur les fichiers binaires ou de configuration à installer peuvent être :

- techniques : analyse antivirus, analyse en bac à sable, vérification de signature électronique, traçabilité à l'aide d'un condensat (*hash*), etc. ;
- organisationnelles : contrôle de la source de téléchargement, de l'émetteur, etc.

La mise à disposition des outils auprès des administrateurs pourra être effectuée à l'aide d'outils de « télédistribution » (ou « télédéploiement »), d'un site Web ou via un partage réseau dédié, ceux-ci étant accessibles uniquement sur le SI d'administration.

R13

### Limiter les logiciels installés sur le poste d'administration

Il est recommandé de n'installer sur le poste d'administration que les logiciels et les outils utiles aux actions d'administration. Pour ce faire, il est nécessaire :

- de dresser et maintenir la liste des outils d'administration utiles ;
- de mettre en œuvre un processus de validation et de distribution des outils d'administration suivant des critères techniques et organisationnels.

## 4.3.3 Chiffrement

Le disque dur du poste d'administration peut contenir des données sensibles, utiles à l'accès au système d'information. La perte ou le vol du poste est préjudiciable car pouvant mener à une compromission de ces données.

R14

### Chiffrer l'ensemble des périphériques de stockage utilisés pour l'administration

Il est recommandé de procéder au chiffrement complet de l'ensemble des périphériques de stockage (disques durs, périphériques de stockage amovibles, etc.) utilisés pour les actions d'administration.



### Attention

Les ordinateurs portables sont en particulier plus exposés aux risques de perte ou de vol. Dans le cadre du nomadisme (cf. chapitre 10), cette recommandation revêt un caractère indispensable.

Les dispositifs de chiffrement utilisés doivent garantir un certain niveau de robustesse et être adaptés à la sensibilité des données à protéger. De tels dispositifs sont au catalogue des produits qualifiés par l'ANSSI.

De plus, l'utilisation du chiffrement implique la mise au point d'un processus lié au cycle de vie des secrets (ex. : initialisation, stockage, récupération en cas de perte).



# 5

## Réseau d'administration

Le réseau d'administration se définit comme le réseau de communication sur lequel transitent les flux internes au SI d'administration et les flux d'administration à destination des ressources administrées. Ce réseau doit faire l'objet de mesures de sécurisation spécifiques en phase avec l'analyse de risque et les objectifs de sécurité décrits dans la section 3.1.

### 5.1 Protection des ressources d'administration

À l'instar de la recommandation sur les postes d'administration, la mise en œuvre d'un réseau d'administration physiquement dédié aux ressources d'administration offre un niveau de sécurité maximal pour se prémunir d'une compromission du SI d'administration et garantir un cloisonnement fort avec tout autre réseau potentiellement connecté à Internet.

Pour éviter le branchement d'équipements indésirables sur ce réseau d'administration dédié (ex. : postes bureautiques, postes personnels), une authentification réseau est recommandée en complément, par exemple par l'implémentation du protocole 802.1X en suivant les recommandations du guide de l'ANSSI [11].

R15

#### Connecter les ressources d'administration sur un réseau physique dédié

Les ressources d'administration (ex. : postes d'administration, serveurs outils) doivent être déployées sur un réseau physiquement dédié à cet usage.

Le cas échéant, il est recommandé que les postes d'administration s'authentifient pour accéder au réseau d'administration.

Si l'application stricte de cette recommandation est techniquement impossible (ex. : sur un réseau étendu) ou disproportionnée par rapport aux besoins de sécurité, une alternative d'un niveau de sécurité moindre peut être envisagée sur la base d'un réseau logique dédié.

R15 -

#### Connecter les ressources d'administration sur un réseau VPN IPsec dédié

À défaut d'un réseau physique dédié, les ressources d'administration doivent être déployées sur un réseau logique dédié à cet usage en mettant en œuvre des mécanismes de chiffrement et d'authentification de réseau, à savoir le protocole IPsec. En complément, des mécanismes de segmentation logique (VLAN) et de filtrage réseau sont recommandés pour limiter l'exposition du concentrateur VPN IPsec aux seuls postes d'administration.

Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

Un regroupement des ressources d'administration par zone de confiance permet de mettre en place un cloisonnement pertinent et les mesures de filtrage réseau idoines au sein du SI d'administration. En outre, afin de garantir le cloisonnement du SI d'administration vis-à-vis de l'extérieur, un filtrage périmétrique doit également être assuré. Dans le cadre du maintien en condition de sécurité, celui-ci doit faire l'objet d'une procédure régulière de révision. De cette façon, les règles de filtrage obsolètes, inutiles ou trop permissives sont supprimées ou, à défaut, désactivées.

**R16**

### Appliquer un filtrage interne et périmétrique au SI d'administration

Quelle que soit la solution de réseau retenue, un filtrage réseau entre zones de confiance doit être mis en œuvre au sein du SI d'administration. Par ailleurs, toutes les interconnexions avec le SI d'administration doivent être identifiées et filtrées. Une matrice de flux, limitée au juste besoin opérationnel, doit être élaborée et revue régulièrement afin d'assurer la traçabilité et le suivi des règles de filtrage.



### Information

L'ANSSI publie des recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu [15] et pour son nettoyage [17].

La figure 5.1 illustre les recommandations R16 et R15 (schéma de gauche), R16 et R15- (schéma de droite). L'illustration de R15-, à droite, ne représente que des postes d'administration connectés en VPN IPsec (cas classique de déploiement d'un client VPN). Cependant il est tout à fait envisageable de connecter d'autres ressources d'administration de la même manière.

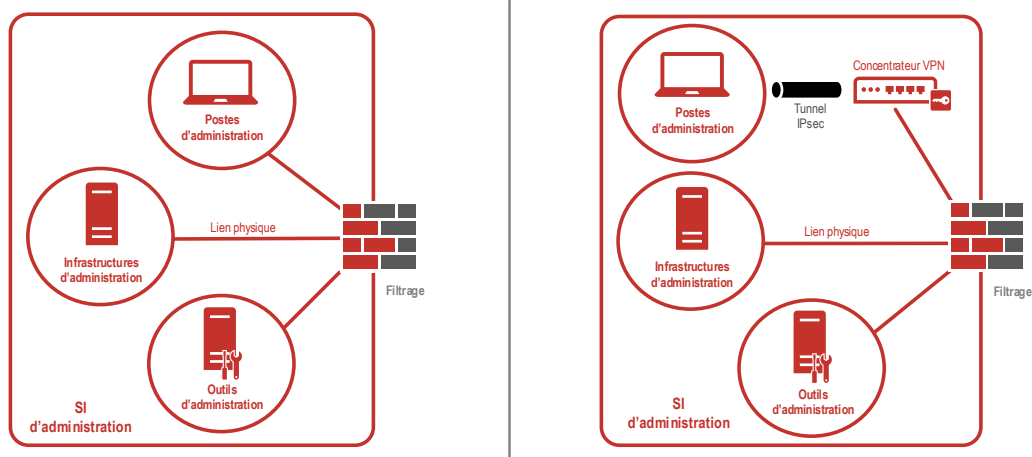


FIGURE 5.1 – Réseaux d'administration avec fonction de filtrage

## 5.2 Accès aux ressources administrées

L'accès aux ressources administrées doit être maîtrisé, non seulement au niveau local grâce à des configurations applicatives sur ces ressources, mais aussi au niveau réseau par des mesures complémentaires de blocage ou de filtrage réseau dans une démarche de défense en profondeur.

## 5.2.1 Sécurisation locale de l'accès aux ressources administrées

Afin de filtrer au plus près l'accès à une ressource administrée, il est recommandé de mettre en œuvre un filtrage local, par exemple à l'aide d'un pare-feu applicatif avec une matrice des flux limitée au strict besoin opérationnel. En particulier, seules des ressources d'administration identifiées peuvent accéder aux services d'administration. Par exemple, le service de production d'un serveur Web est accessible sur le port TCP/443 (HTTPS) par l'ensemble de ses clients légitimes et son service d'administration est accessible sur le port TCP/22 (SSH) par les ressources d'administration identifiées pour ce besoin.

R17

### Appliquer un filtrage local sur les ressources administrées

Pour maîtriser les accès au plus près des ressources administrées, il est recommandé de leur appliquer un filtrage local correspondant au juste besoin opérationnel.



### Information

Certains systèmes, par exemple des systèmes de gestion de contenu ou le service Active Directory de Microsoft, ne distinguent pas le port d'écoute des services de production et d'administration (même port TCP). Dans ce cas de figure, l'application de R17 est toujours nécessaire mais non suffisante. La sécurité de l'administration au niveau de la ressource administrée repose de façon ultime sur la configuration applicative du service (ex : contrôle d'accès, gestion des droits) et sa robustesse ; cela doit être traité avec attention mais n'est pas l'objet de ce guide.

## 5.2.2 Mise en œuvre d'une interface d'administration dédiée

Dès lors qu'elle est techniquement réalisable au niveau d'une ressource administrée, la séparation des interfaces de production et d'administration est recommandée. Cette mesure garantit non seulement un filtrage local plus spécifique (ex. : un service d'administration n'est autorisé que sur l'interface d'administration) mais aussi une disponibilité accrue de la ressource administrée en cas de déni de service sur l'interface de production.

Une séparation en interfaces réseau physiques offre un niveau de sécurité maximal et permet ainsi de dissocier les équipements de filtrage réseau respectivement sur les réseaux de production et d'administration. À défaut, une séparation en interfaces réseau virtuelles est recommandée.

Si cette séparation n'est techniquement pas réalisable sur un système, alors l'application des mesures locales, dont la recommandation R17, doit être d'autant plus stricte.

R18

## Dédier une interface réseau physique d'administration

Il est recommandé de dédier une interface réseau physique d'administration sur les ressources administrées en s'assurant des pré-requis suivants :

- les services logiques permettant l'exécution des actions d'administration doivent être en écoute uniquement sur l'interface réseau d'administration prévue à cet effet ;
- les fonctions internes du système d'exploitation ne doivent pas permettre le routage d'informations entre les interfaces réseau de production et l'interface réseau d'administration d'une même ressource. Elles doivent être désactivées (ex. : désactivation d'*IPForwarding*).

R18 -

## Dédier une interface réseau virtuelle d'administration

À défaut d'une interface réseau physique d'administration, il est recommandé de dédier une interface réseau virtuelle d'administration sur les ressources administrées. Les mêmes pré-requis que R18 s'appliquent.



## Information

Certains constructeurs proposent des interfaces de gestion à distance (ex. : Cisco IMC, Dell RAC, HP iLO) permettant un accès à la couche basse de l'équipement. Dès lors, si elles sont utilisées, elles doivent être considérées comme des interfaces réseau d'administration spécifiques et raccordées au réseau d'administration. En fonction de l'analyse de risque et de l'organisation des équipes d'administration, ces interfaces peuvent être raccordées dans une zone différente de l'administration des couches plus hautes.

Il est nécessaire de s'assurer qu'il n'est pas possible pour un attaquant, ayant pris le contrôle d'une ressource administrée, d'utiliser l'interface réseau d'administration pour rebondir sur les ressources d'administration. En conséquence, seuls les flux initialisés depuis les postes ou les serveurs d'administration vers les ressources administrées doivent être autorisés par défaut. Les remontées des journaux d'événements depuis les ressources administrées (ex. : client syslog) vers le SI d'administration peuvent constituer une exception.

R19

## Appliquer un filtrage entre ressources d'administration et ressources administrées

La recommandation R16 doit être appliquée rigoureusement entre les ressources d'administration et les ressources administrées.

De même, il est nécessaire de s'assurer qu'il n'est pas possible pour un attaquant, ayant pris le contrôle d'une ressource administrée, d'utiliser l'interface réseau d'administration pour rebondir sur les autres ressources administrées. Par conséquent, toute communication entre les ressources administrées doit être interdite à travers le réseau d'administration. Dans ce cadre, il est possible d'avoir recours à :

- un filtrage réseau sur la base d'une « micro-segmentation » (une ressource administrée = un sous-réseau), cette pratique pouvant néanmoins représenter une certaine complexité opérationnelle ;
- l'utilisation de la fonctionnalité de VLAN privé (*Private VLAN* ou PVLAN) au niveau des commutateurs (cf. le guide ANSSI [7]).

R20

### Bloquer toute connexion entre ressources administrées à travers le réseau d'administration

Une mesure de blocage ou de filtrage réseau doit être mise en œuvre entre les ressources administrées afin d'interdire toute tentative de compromission par rebond à travers les interfaces réseaux d'administration.

## 5.2.3 Cas d'un réseau étendu

Dans le cas d'architectures multi-sites ou de réseaux étendus, les ressources d'administration peuvent être éloignées des ressources administrées. Les flux d'administration transitent alors potentiellement par un réseau de transport tiers<sup>7</sup>. Dans ce cas, il est nécessaire de protéger les flux d'administration en confidentialité, en intégrité et en authenticité.

R21

### Protéger les flux d'administration transitant sur un réseau tiers

Si les flux d'administration circulent à travers un réseau tiers ou hors de locaux avec un niveau de sécurité physique adéquat (ex. : portion de fibre noire traversant l'espace public), ceux-ci doivent être chiffrés et authentifiés de bout en bout jusqu'à atteindre une autre zone du SI d'administration ou une ressource à administrer. Dans ce cas, un tunnel IPsec doit être établi.

Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

Les figures 5.2 et 5.3 illustrent respectivement l'accès aux ressources administrées dans le cas d'un réseau local et d'un réseau étendu.

7. Un réseau de transport est dit *tiers* dès lors qu'il n'est pas maîtrisé par l'entité (ex. : Internet ou un réseau d'opérateur de télécommunications).

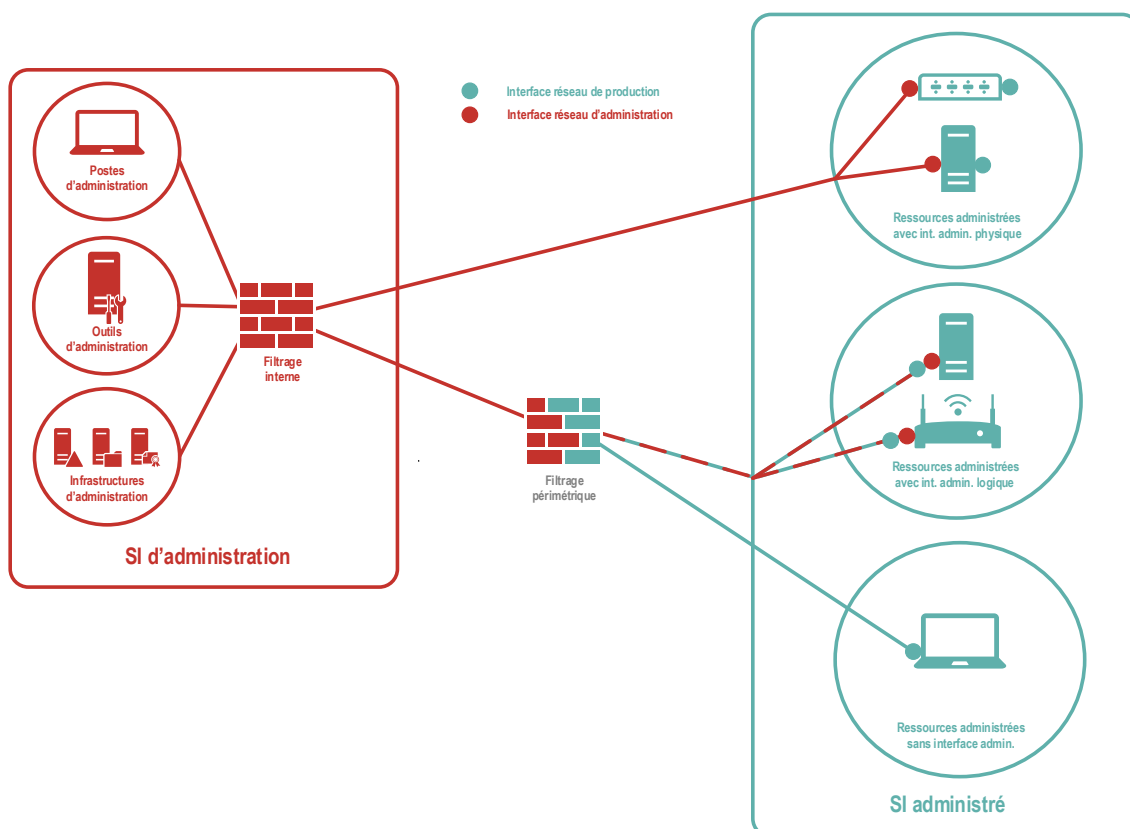


FIGURE 5.2 – Administration, sur un réseau local, à travers des interfaces d'administration dédiées (physiques ou logiques) ou une interface de production

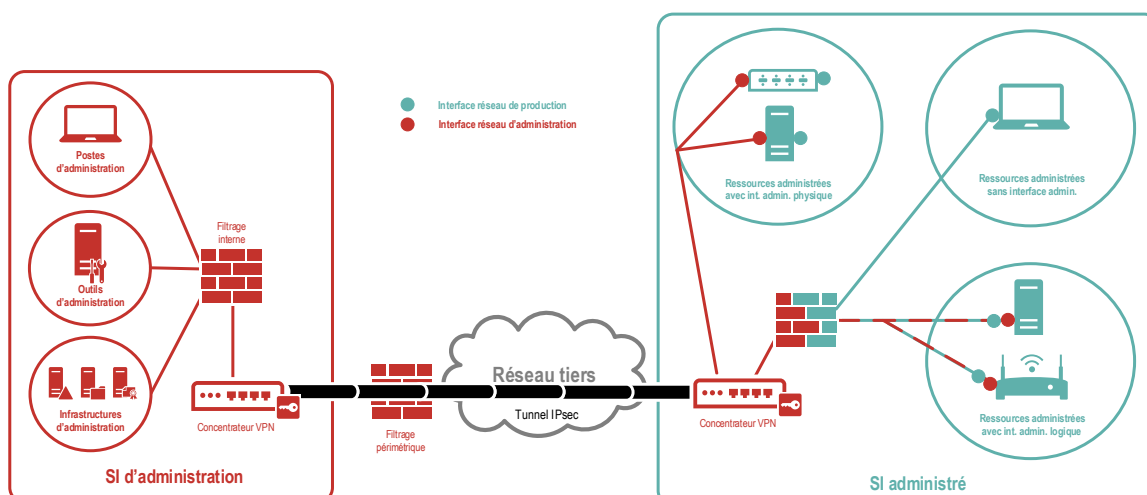


FIGURE 5.3 – Administration, sur un réseau étendu, à travers des interfaces d'administration dédiées (physiques ou logiques) ou une interface de production

# 6

## Outils d'administration

Les outils d'administration, logiciels permettant la réalisation d'actions d'administration, sont mis à disposition des administrateurs, soit localement sur leur poste d'administration soit de façon déportée et centralisée sur des serveurs. Des mesures spécifiques à leur protection contre des tentatives de compromission ou des usages illicites doivent être mises en œuvre. Le cas particulier des outils d'administration d'un *cloud* public est abordé dans la section 13.6.

### 6.1 Cloisonnement des outils d'administration

Dans la continuité des principes de réduction de surface d'attaque décrits dans la section 3.2, la principale mesure vise à cloisonner les outils d'administration par zone d'administration. Pour rappel, à une zone d'administration du SI d'administration correspond une ou plusieurs zones de confiance du SI administré.

#### 6.1.1 Outils d'administration locaux

Dans le cas d'outils d'administration locaux au poste d'administration, le cloisonnement par zone d'administration est difficilement applicable. Il est rappelé que ces outils doivent être déployés en fonction du strict besoin opérationnel conformément à R13.

#### 6.1.2 Outils d'administration centralisés

Dans le cas d'outils d'administration centralisés, la mise en œuvre de serveurs dédiés par zone d'administration permet la mise en œuvre du cloisonnement recherché et facilite la mise à jour des outils.

R22

#### Déployer les outils d'administration sur des serveurs dédiés par zone d'administration

Les outils d'administration doivent être déployés par zone d'administration en fonction du juste besoin opérationnel. Cette mesure peut se traduire par la mise en œuvre de serveurs outils dédiés, intégrant par exemple les outils d'administration proposés par des éditeurs ou des équipementiers (ex. : client lourd ou service Web interagissant avec les ressources administrées).

Les recommandations de sécurisation logicielle des postes d'administration (R10, R11, R12, R13, R14) doivent être appliquées, dès que possible, aux serveurs outils d'administration.

En complément, la mise en œuvre de mécanismes de cloisonnement réseau physique ou de segmentation réseau logique (ex. : VLAN) et de filtrage (ex. : pare-feu) doivent garantir les seules

connexions légitimes depuis les postes d'administration vers les serveurs outils d'administration. Cette pratique contribue, en outre, à restreindre les risques de compromission, par rebond, d'une zone vers une autre.

R23

### Appliquer un filtrage entre les postes d'administration et les serveurs outils d'administration

La recommandation R16 doit être appliquée rigoureusement entre les postes d'administration et les serveurs outils d'administration en autorisant uniquement les flux à l'initiative des postes d'administration.

## 6.2 Sécurisation des flux d'administration

Quelles que soient les mesures de cloisonnement retenues, les flux d'administration requièrent des protocoles utilisant des mécanismes de chiffrement et d'authentification (ex. : SSH, HTTPS, SFTP). L'objectif consiste à renforcer la confidentialité, l'intégrité et l'authenticité des flux d'administration.

R24

### Utiliser des protocoles sécurisés pour les flux d'administration

Il est recommandé d'utiliser systématiquement, dès lors qu'ils existent, des protocoles et des outils d'administration utilisant des mécanismes de chiffrement et d'authentification robustes (cf. RGS [22]), en privilégiant les protocoles sécurisés standardisés et éprouvés (ex. : TLS ou SSH).

Le cas échéant, les protocoles non sécurisés doivent être explicitement désactivés ou bloqués.



### Attention

Certains outils peuvent mettre en avant l'emploi de mécanismes de sécurité mais leur implémentation peut ne pas être conforme à l'état de l'art. Il convient donc de s'assurer par exemple des traces éventuelles générées par ces outils (ex. : condensat de mot de passe) et de vérifier le chiffrement de l'ensemble des informations.

Certains protocoles ou outils d'administration sont obsolètes et ne mettent pas en œuvre ces mécanismes cryptographiques. Dans ce cas, l'emploi de VPN IPsec, depuis le serveur outils ou le poste d'administration jusqu'au plus proche de la ressource administrée, permet de pallier ces carences.

R24 -

### Protéger le cas échéant les flux d'administration dans un tunnel VPN IPsec

À défaut d'interfaces d'administration dédiées ou d'outils d'administration permettant le chiffrement et l'authentification de bout en bout, les flux d'administration doivent être protégés par la mise en œuvre d'un tunnel VPN IPsec, avec authentification mutuelle par certificats, depuis le serveur outils ou le poste d'administration vers les ressources administrées. Ce tunnel VPN IPsec doit être établi au plus près de la ressource d'administration et de la ressource administrée.



## 6.3 Rupture ou continuité des flux d'administration

Les actions d'administration imposent entre autres des exigences de traçabilité et de confidentialité. Suivant l'expression des besoins de sécurité élaborée dans le cadre de l'analyse de risque, il peut être souhaité soit d'assurer une rupture des échanges entre le poste d'administration et la ressource administrée, soit de garantir l'établissement de bout en bout d'une authentification puis d'une session. Les paragraphes suivants illustrent les deux cas d'usage : avec ou sans rupture protocolaire.

La figure 6.1 présente le cas d'usage de la mise en œuvre de rebonds dans une zone d'administration permettant d'appliquer un certain nombre de traitements tels le filtrage des connexions, l'authentification des administrateurs sur un portail frontal, un contrôle d'accès ou encore la journalisation des actions effectuées et des commandes exécutées par les administrateurs. De plus, lorsque le protocole d'administration d'une ressource est peu ou pas sécurisé, le recours à une rupture protocolaire peut être souhaitable en complément de R24.

R25

### Étudier la mise en œuvre d'une rupture protocolaire des flux d'administration

Pour la traçabilité des accès ou des actions d'administration, ou pour pallier des faiblesses de sécurité des protocoles d'administration, il est recommandé d'étudier la mise en œuvre d'une rupture protocolaire des flux d'administration.

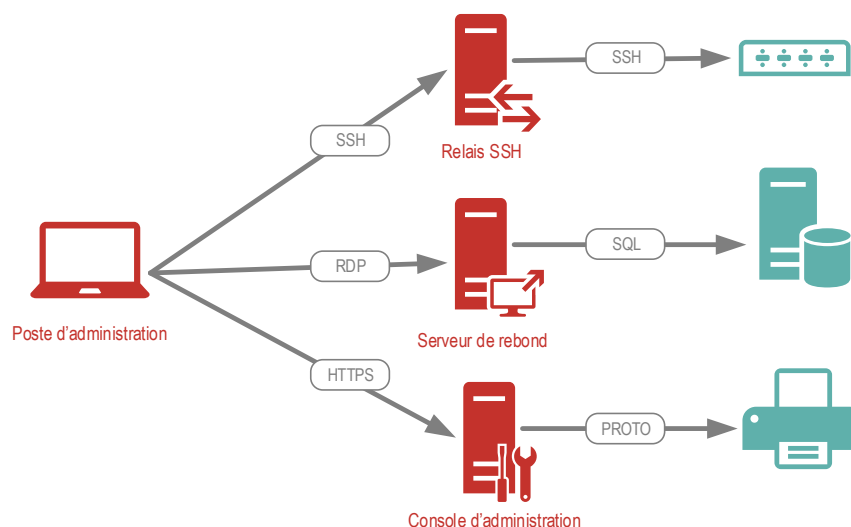


FIGURE 6.1 – Administration avec rupture protocolaire



### Information

La section 13.1 traite plus en détails les problématiques d'architecture liées aux bastions d'administration.

Pour l'autre cas d'usage, sans rupture protocolaire, l'objectif consiste à ne pas rompre la session sécurisée, reposant sur des mécanismes cryptographiques de confiance (cf. figure 6.2).

## Renoncer à la rupture protocolaire pour les besoins en confidentialité

L'absence de rupture protocolaire doit être privilégiée en cas de besoin fort de confidentialité des flux d'administration et après une analyse de risque complémentaire. Le cas échéant, les protocoles utilisés doivent d'autant plus être sécurisés et configurés à l'état de l'art conformément à R24.

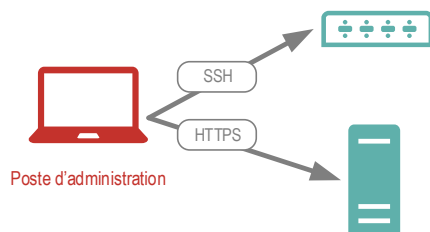


FIGURE 6.2 – Administration sans rupture protocolaire

# 7

## Identification, authentification et droits d'administration

### 7.1 Identification

Il est indispensable de dissocier les rôles sur le SI, en particulier pour un administrateur : simple utilisateur ou administrateur avec des droits privilégiés octroyés sur les ressources administrées. De plus, un administrateur peut intervenir sur plusieurs domaines techniques. En conséquence, des comptes distincts doivent être créés et utilisés selon le rôle (utilisateur ou administrateur) ainsi que des comptes d'administration distincts par domaine technique.

En toute logique, et pour éviter tout rejeu d'un secret potentiellement compromis, les secrets (ex. : code PIN, mot de passe, clé privée) associés doivent être différents entre comptes.

R27

#### Utiliser des comptes d'administration dédiés

L'administrateur doit disposer d'un ou plusieurs comptes d'administration dédiés, distincts de son compte utilisateur. Les secrets d'authentification doivent être différents suivant le compte utilisé.

Les identifiants et secrets associés aux comptes d'administration font partie des premières cibles d'une attaque informatique. Le vol de ces informations simplifie grandement la compromission d'un système d'information et la rend plus silencieuse. Les annuaires contribuant à identifier et authentifier les administrateurs sur les ressources administrées sont des éléments critiques. Leur prise de contrôle par un attaquant permet en effet de disposer de l'ensemble des privilèges sur le SI administré.

R28

#### Protéger l'accès aux annuaires des comptes d'administration

Le ou les annuaires contenant les comptes d'administration doivent être protégés en confidentialité et en intégrité et ne pas être exposés sur des environnements de moindre confiance.

Dans le cas général, il est recommandé de déployer un ou plusieurs annuaires dédiés, au sein du SI d'administration, pour gérer les comptes d'administration et le contrôle d'accès aux ressources administrées.

Dans le cas spécifique d'un SI administré reposant sur Microsoft Active Directory, il est recommandé en premier lieu d'adopter un modèle de gestion des comptes à privilèges (ex. : modèle en trois *Tiers*) pour cet annuaire et de sécuriser sa configuration (cf. les points de contrôle Active Directory [4]).

Des mesures techniques complémentaires restreignant l'emploi des comptes d'administration sur les postes de travail doivent être mises en œuvre.

R29

### Réserver les comptes d'administration aux seules actions d'administration

Les comptes d'administration doivent être utilisés *exclusivement* pour des actions d'administration. En particulier, aucun compte d'administration ne doit être utilisé pour des actions bureautiques ou l'ouverture de sessions de travail sur des postes autres que ceux réservés aux actions d'administration.

Par défaut, les comptes natifs d'administration, dits *built-in* (ex. : root, admin), présents sur les équipements lors de l'installation ne doivent pas être utilisés. Leur utilisation doit rester exceptionnelle et restreinte à un nombre d'administrateurs très limité. En effet, ces comptes ne permettent pas d'imputer de manière précise les actions effectuées sur les équipements. Cela rend aussi impossible la mise en œuvre d'un contrôle d'accès pertinent aux outils d'administration et la ségrégation des droits. Seule la création de comptes individuels d'administration peut répondre à ces besoins.

R30

### Utiliser par défaut des comptes d'administration individuels

Des comptes d'administration individuels doivent être attribués à chaque administrateur.

Les comptes natifs d'administration ne doivent pas être utilisés pour les actions courantes d'administration et les secrets associés ne doivent être accessibles qu'à un nombre très restreint de personnes.



### Information

L'attribution de comptes individuels fait classiquement l'objet d'une convention de nommage. Si, par exemple, Camille MARTIN dispose de l'identifiant `cmartin` pour son compte utilisateur, deux options possibles pour l'identifiant de son compte administrateur sont :

- un identifiant directement dérivé du compte utilisateur : `adm-cmartin` ;
- un identifiant pseudonymisé (mais toujours individuel) : `adm-0x2a`.

Cette deuxième méthode, plus contraignante d'un point de vue opérationnelle car nécessitant le maintien à jour d'une table de correspondances, permet de complexifier pour les attaquants l'identification des administrateurs à cibler (ex. : actions d'hameçonnage, attaque sur le compte utilisateur).

Afin de détecter au plus tôt les signes d'une éventuelle compromission et appliquer les mesures conservatoires et correctives, il est impératif d'auditer l'usage des comptes d'administration. L'annexe A du guide [14] décrit les éléments à auditer. Les modalités concernant la journalisation et la supervision de la sécurité sont traitées dans la section 9.2.

**R31**

### Journaliser les événements liés aux comptes d'administration

Les mécanismes d'audit des événements concernant les comptes d'administration doivent être mis en œuvre. En particulier, les journaux suivants doivent être activés :

- ouvertures et fermetures de session ;
- échecs d'authentification et verrouillage des comptes ;
- gestion des comptes ;
- gestion des groupes de sécurité.

Les comptes d'administration doivent être suivis rigoureusement dans le temps : création, suppression ou modification depuis un environnement sécurisé. Les privilèges associés doivent être ajustés autant que de besoin.

**R32**

### Prévoir un processus de gestion des comptes d'administration

Un processus organisationnel et technique de gestion des comptes d'administration et des privilèges associés doit être mis en œuvre et intégrer une procédure de contrôle et de révision régulière.

Sur l'aspect organisationnel, ce processus doit être suffisamment résilient pour pallier l'absence d'un ou plusieurs acteurs. Les entités opérationnelles doivent être associées en phase de conception et sont ensuite responsables de son application.

Sur l'aspect technique, les comptes d'administration ne doivent pas être créés, modifiés ou supprimés automatiquement depuis un outil exposé sur un SI bureautique.

## 7.2 Authentification

L'authentification permet de s'assurer de l'identité d'un administrateur ou d'un compte de service d'administration avant d'autoriser son accès aux ressources administrées. Pour définir le type d'authentification à mettre en œuvre, le référentiel général de sécurité (RGS), et notamment les annexes B1, B2 et B3, décrivent en détail les mécanismes cryptographiques et d'authentification.

**R33**

### Se référer au RGS pour choisir les mécanismes d'authentification

En phase de conception ou de révision des architectures d'administration, il convient de se référer aux annexes B1, B2 et B3 du RGS [22] afin de mettre en conformité les mécanismes d'authentification utilisés.

Les comptes natifs d'administration (ex. : root, admin) possèdent généralement un mot de passe par défaut, consultable dans la documentation papier ou sur Internet. Il convient donc de les modifier dès l'installation.

**R34**

### Modifier les mots de passe par défaut des comptes natifs

Les mots de passe par défaut des comptes natifs d'administration doivent être modifiés au moment de l'installation de l'équipement ou du service. De préférence, les nouveaux mots de passe sont distincts par équipement et conservés au séquestre.

Les administrateurs peuvent être contraints d'utiliser un grand nombre de secrets, ce qui rend le respect des bonnes pratiques (ex. : complexité, aléa, renouvellement) difficile à maintenir dans le temps. Malgré la mise en œuvre d'annuaire d'authentification centralisée, il se peut que le nombre de mots de passe résiduels reste important à cause d'équipements ou logiciels incompatibles avec ces solutions d'authentification. Leur stockage dans un fichier, en clair ou avec un chiffrement faible, doit néanmoins être proscrit.

R35

### Stocker les mots de passe dans un coffre-fort de mots de passe

Il est recommandé d'utiliser un coffre-fort de mots de passe disposant d'un visa de sécurité pour stocker de manière sécurisée les mots de passe sur le SI d'administration. Ainsi, les mots de passe peuvent être, autant que possible, distincts, longs et aléatoires.

Différents facteurs contribuent à la robustesse de l'authentification. Ils sont à prendre en compte pour le choix des mécanismes d'authentification et se distinguent de la manière suivante :

- ce que je sais (ex. : un mot de passe, un code PIN) ;
- ce que je suis (ex. : une empreinte digitale, un iris) ;
- ce que je possède (ex. : une carte à puce).

Une authentification est dite *multi-facteurs* dès lors qu'au moins deux facteurs différents sont utilisés. En informatique, il est courant de combiner les facteurs *ce que je sais* et *ce que je possède*.



### Attention

L'authentification multi-facteurs n'apporte de réelle sécurité que si, de façon cumulative :

- l'authentification par simple mot de passe est rendue impossible ;
- les facteurs proviennent de canaux indépendants (ex. : certificat stocké sur une carte à puce et code PIN mémorisé).

R36

### Privilégier une authentification double facteur pour les actions d'administration

Pour les actions d'administration, il est recommandé d'utiliser une authentification comportant au minimum deux facteurs.

Pour le facteur *ce que je possède*, l'usage de matériels d'authentification de type carte à puce ou jeton (*token*) USB (ex. : jeton FIDO) est courant et recommandé. Ces matériels sont porteurs d'une partie des éléments secrets contribuant au processus d'authentification. L'autre facteur peut se matérialiser par exemple par un code PIN.

Les éléments d'authentification sont généralement des certificats électroniques de type x.509. Cette technologie nécessite la génération de certificats et induit la notion de confiance dans la chaîne de certification et dans l'infrastructure de gestion de clés (IGC). En effet, si l'usage de certificats paraît plus robuste que le mot de passe, sa robustesse repose en grande partie sur la confiance dans

le cycle de vie de la certification (génération, signature, stockage, révocation) et, par conséquent, dans le prestataire assurant ces services.

R37

### Utiliser des certificats électroniques de confiance pour l'authentification

L'usage de certificats électroniques comme élément contribuant à l'authentification est recommandé.

Il convient d'acquérir ces certificats auprès d'un prestataire de services de certificats électroniques (PSCE) qualifié par l'ANSSI ou de déployer une infrastructure de gestion de clés conforme aux exigences du RGS [22] encadrant ce domaine.

L'authentification des administrateurs peut être locale ou distante sur les ressources d'administration ou les ressources administrées. Il convient d'éviter la « sédimentation » des comptes créés dans le temps, qui rendrait complexe la gestion de leur cycle de vie. Quelle que soit la solution retenue (ex. : annuaire LDAP distant, certificats SSH locaux), une gestion centralisée de l'authentification doit être mise en œuvre pour favoriser le suivi des comptes et le respect de la politique de sécurité (ex. : renouvellement des secrets d'authentification, verrouillage ou révocation). Il est primordial que l'entité soit en mesure de réagir rapidement en cas de compromission, suspectée ou avérée, d'un compte d'administration, en bloquant son utilisation sur un maximum de ressources.

R38

### Mettre en œuvre une gestion centralisée de l'authentification

Une gestion centralisée de l'authentification doit être mise en œuvre en lieu et place d'une gestion exclusivement locale sur les ressources d'administration ou les ressources administrées.

## 7.3 Droits d'administration

L'annuaire des comptes d'administration sert notamment à configurer les droits pour restreindre l'accès à l'administration des ressources administrées ou aux outils d'administration. Un administrateur ne doit pouvoir accéder et administrer que les ressources pour lesquelles il y est autorisé. De plus, cet annuaire doit être lui-même protégé de toute modification intempestive et de tout accès non contrôlé sur les attributs critiques, tels les champs de type *mot de passe*.

R39

### Respecter le principe du moindre privilège dans l'attribution des droits d'administration

Les droits d'administration doivent être mis en œuvre sur l'annuaire des comptes d'administration en respectant le principe du moindre privilège.

Dans le cas spécifique des droits les plus privilégiés sur l'annuaire lui-même, seuls des administrateurs du SI d'administration peuvent en disposer.

Pour faciliter la gestion des droits d'administration (ajout, modification et suppression), il est recommandé de créer des groupes. Un groupe contient, en fonction du juste besoin opérationnel, l'ensemble des comptes d'administration devant disposer de droits d'administration homogènes sur une ou plusieurs ressources administrées. Les droits sur ces ressources sont ainsi octroyés aux groupes et non aux comptes.

R40

## Attribuer les droits d'administration à des groupes

Les droits d'administration doivent être préférentiellement attribués à des groupes de comptes d'administration plutôt qu'unitairement à des comptes d'administration.

De plus, des politiques de sécurité sont à définir et à déployer pour assurer le contrôle d'accès aux outils d'administration. Cela consiste à maîtriser les accès des différentes catégories d'administrateurs au travers de profils de compte d'administration. Parmi les éléments à définir, il convient au minimum de prévoir :

- les privilèges des comptes : il faut attribuer aux différents comptes (administrateurs, services, systèmes) les privilèges strictement nécessaires pour exécuter les actions d'administration sur les équipements ou les services identifiés ;
- les autorisations d'accès aux outils : des règles de contrôle d'accès doivent être définies de façon à préciser les modalités d'accès aux outils d'administration tels les horaires, le type d'authentification, les actions autorisées ou interdites, etc. ;
- le cas échéant, la politique de mot de passe : longueur minimale et maximale, délais d'expiration, nombre de tentatives de connexion avant verrouillage du compte, historique, etc.

R41

## Déployer des politiques de sécurité

Il est recommandé de déployer des politiques de sécurité dans le but de définir les privilèges de chaque compte d'administration, de contrôler l'accès aux outils d'administration en fonction du juste besoin opérationnel et de renforcer l'authentification.



# 8

## Maintien en condition de sécurité

De par son caractère critique, un SI d'administration doit particulièrement respecter le principe de maintien en condition de sécurité (MCS). Ce dernier consiste en la mise en œuvre de l'ensemble des mesures, techniques ou non, visant à maintenir voire améliorer le niveau de sécurité d'un SI d'administration tout au long de son cycle de vie.

R42

### Réaliser scrupuleusement le MCS du SI d'administration

Le MCS de l'ensemble des éléments constituant le SI d'administration doit être assuré périodiquement et dans des délais raisonnables, notamment par l'application des mises à jour de sécurité. À cette fin, il est recommandé de mener une veille technologique.

Les mises à jour doivent être réalisées de préférence au travers de dépôts relais internes à l'entité (cf. figure 8.1) :

- dédiés au SI d'administration ;
- isolés d'Internet par une passerelle de type DMZ<sup>8</sup> ;
- mettant en œuvre des filtrages par liste d'autorisations (liste exclusive de sites Web correspondant aux sites éditeurs ou constructeurs autorisés) ;
- vérifiant, dans la mesure du possible, l'intégrité et l'authenticité des fichiers téléchargés.

R43

### Mettre en place des serveurs relais pour la récupération des mises à jour

Pour la récupération des mises à jour (ex. : correctifs de sécurité ou signatures antivirales), il est recommandé de mettre en œuvre, au sein d'une DMZ, des serveurs relais dédiés au SI d'administration.

Seuls les flux initialisés depuis ces dépôts relais vers Internet doivent permettre le téléchargement des mises à jour. Des mécanismes de filtrage par liste d'autorisations permettent de restreindre l'accès aux seules sources officielles.

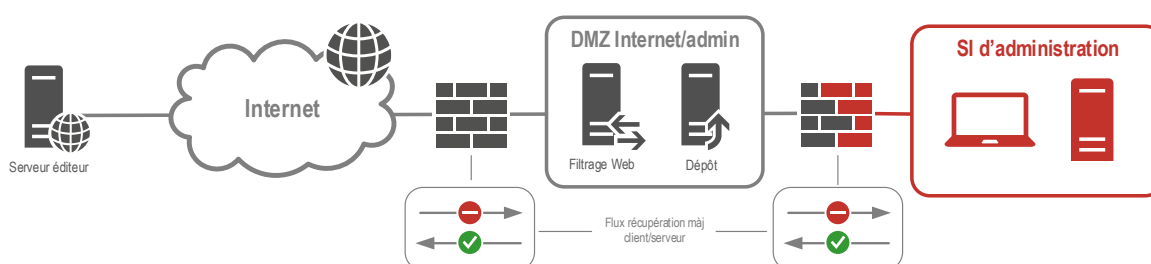


FIGURE 8.1 – Architecture de récupération et mise à disposition des mises à jour

8. DMZ : cf. le glossaire en annexe C.

Enfin, pour éviter toute régression de service suite à la mise en œuvre d'un correctif technique ou de sécurité, il convient de valider au préalable leur bon fonctionnement. Des procédures de déploiement ainsi que de retour arrière doivent être élaborées. Cette pratique nécessite généralement de disposer d'une plate-forme de qualification.

**R44**

### Valider les correctifs de sécurité avant leur généralisation

Il est recommandé que les administrateurs procèdent à la qualification des correctifs de sécurité avant leur mise en production et leur généralisation.

Une procédure d'urgence doit également être prévue pour réagir en cas de crise nécessitant l'application d'un correctif de sécurité au plus vite.

# 9

## Sauvegarde, journalisation et supervision de la sécurité

### 9.1 Sauvegarde

Comme pour tout SI, il est primordial de définir une politique de sauvegarde du SI d'administration, ceci afin de pouvoir rétablir le service suite à un incident ou à une compromission. Pour cela, les éléments à sauvegarder, le lieu de sauvegarde et les droits d'accès qui y sont associés doivent être clairement identifiés. Les sauvegardes doivent être réalisées régulièrement. Enfin, les procédures de restauration doivent être documentées et testées.

R45

#### Définir une politique de sauvegarde du SI d'administration

Pour permettre de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission, une politique de sauvegarde doit être définie et appliquée pour le SI d'administration.

Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue.

### 9.2 Journalisation et supervision de la sécurité

La journalisation des événements techniques, dont ceux liés à la sécurité, et leur analyse régulière permettent de détecter une éventuelle compromission du SI. L'archivage de ces informations permet les investigations numériques pour comprendre comment une intrusion a été possible.

Les besoins de journalisation du SI administré et du SI d'administration doivent donc être pris en compte dans l'étude de conception du SI d'administration. Une zone d'administration doit être dédiée aux services de journalisation (cf. figure 9.1). En effet, pour assurer une analyse pertinente des journaux d'événements, leur intégrité doit être garantie depuis leur génération jusqu'à leur lieu de stockage. En cas d'intrusion, les attaquants voudront effacer ou modifier les traces générées pour que leur présence ne soit pas détectée. Afin de couvrir ce risque, au-delà du cloisonnement des services de journalisation, il est nécessaire de restreindre les accès à ces informations aux seules personnes ayant le besoin d'en connaître.

R46

#### Dédier une zone d'administration à la journalisation

Il est recommandé de dédier une zone d'administration à la journalisation du SI administré et du SI d'administration. Le cas échéant, un contrôle d'accès spécifique doit être mis en place.

La création d'une zone d'administration dédiée à la journalisation impose naturellement que l'ensemble des journaux soit remonté de manière centralisée (cf. figure 9.1). Cela contribue par ailleurs à rendre la corrélation des journaux plus efficace.

R47

## Centraliser la collecte des journaux d'événements

L'architecture doit prévoir la transmission des journaux d'événements de manière centralisée, depuis les équipements vers les services de journalisation.

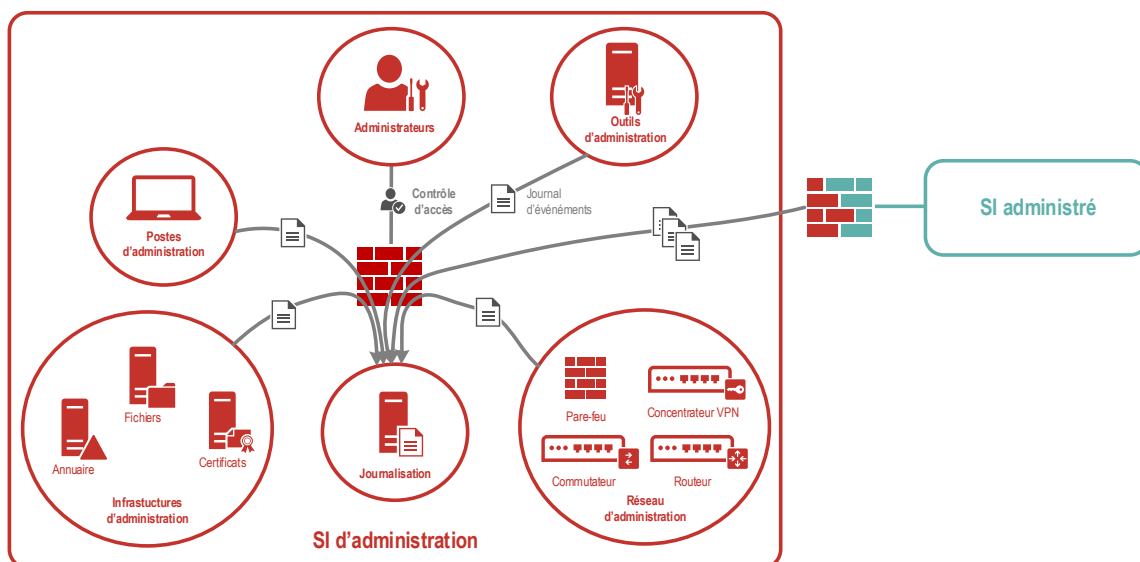


FIGURE 9.1 – Représentation fonctionnelle de la journalisation au sein du SI d'administration

i

## Information

En complément, il est recommandé de s'approprier le guide afférent de l'ANSSI [14] et d'en appliquer les principes et les recommandations.

Pour aller plus loin sur la remontée des journaux d'événements et la supervision de sécurité, le référentiel d'exigences PDIS [25] (Prestataire de détection des incidents de sécurité) constitue un guide de bonnes pratiques.

# 10

## Administration à distance et nomadisme

Pour différentes raisons (opérationnelles, budgétaires, etc.) et afin d'assurer une continuité de l'administration des SI, quasiment en tout lieu et en tout temps, les entités se dotent de moyens d'accès à distance pour leurs administrateurs. L'administration à distance par des tiers, lors du recours à une prestation d'infogérance, est traitée spécifiquement dans le chapitre 12.

On convient dans ce guide de parler de *nomadisme* pour l'utilisation d'un poste d'administration dans un lieu extra-professionnel (lieu public, domicile, etc.) et d'*administration à distance* de manière plus générale pour tout accès au SI en dehors du réseau local de l'entité. Ainsi l'administration à distance couvre non seulement le nomadisme mais également l'utilisation d'un poste d'administration depuis des locaux distants d'un centre de données.

Afin de ne pas affaiblir le niveau de sécurité du SI d'administration, il convient de fournir des moyens de connexion sécurisés à ces administrateurs qui agissent en dehors du périmètre géographique de l'entité.



### Attention

La mise en œuvre d'administration à distance nécessite une plus forte maîtrise du poste d'administration et de sa configuration. En effet, cette pratique augmente sensiblement les risques de compromission du SI, en particulier en cas de vol ou de perte du poste.

Les mesures de sécurité décrites dans la section 4.3 doivent donc être obligatoirement et *intégralement* mises en œuvre sur le poste d'administration utilisé dans le cadre de l'administration à distance, y compris le chiffrement des périphériques de stockage.

Dans le cadre du nomadisme, le poste d'administration peut faire l'objet d'indiscrétions et les informations affichées à l'écran peuvent être lues à l'insu de l'administrateur. En complément de la vigilance de l'administrateur qui veille à utiliser son poste d'administration dans un environnement sûr, l'administrateur doit utiliser un filtre écran de confidentialité.

R48

### Installer un filtre de confidentialité sur le poste d'administration nomade

Le poste d'administration nomade doit être doté d'un filtre écran de confidentialité afin de limiter la portée des informations affichées dès lors qu'il y a une possible exposition à des regards tiers.

Au vu des techniques d'attaques et des protocoles de communication actuels, l'usage du chiffrement IP et le respect des principes d'authentification mutuelle sont recommandés. La technologie VPN IPsec permet de répondre à ce besoin. Comparativement à la technologie TLS, pour laquelle

certaines implémentations proposent aussi l'établissement de VPN, la surface d'attaque des solutions IPsec est plus faible et les échanges pour le renouvellement de clés plus robustes.

R49

### Utiliser un tunnel VPN IPsec pour la connexion du poste d'administration à distance

Un tunnel VPN IPsec doit être mis en œuvre entre le poste d'administration nomade, ou le site distant, et le SI d'administration.

Tous les flux entrants et sortants doivent transiter à travers ce tunnel. Toute configuration de type *split tunnelling*<sup>9</sup> est à proscrire strictement.

Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.



### Attention

Dans le cas d'un poste d'administration nomade, l'accès au concentrateur VPN IPsec à travers Internet constitue la seule exception à la recommandation R10 et nécessite un filtrage local strict conformément à R11. De plus, le profil VPN doit être configuré avec l'adresse IP du concentrateur (et celle de son éventuelle instance de secours) pour éviter toute ouverture de flux DNS publics vers Internet.

Dans le cadre de l'utilisation d'un client VPN IPsec logiciel, les utilisateurs du poste d'administration ne doivent pas être en capacité de modifier la configuration réseau ni, *a fortiori*, de débrayer les mécanismes d'accès distant par VPN. Ceci permet de s'assurer qu'aucune erreur d'utilisation ou action malveillante ne mènera à détourner l'usage du poste d'administration pour accéder directement à un autre réseau (p. ex. Internet) que celui de l'entité.

R50

### Empêcher toute modification de la configuration VPN du poste d'administration

L'utilisateur du poste d'administration ne doit pas être en mesure de modifier sa configuration réseau pour débrayer ou détourner les mécanismes d'accès distant par VPN.



### Information

Dans ce cas précis, l'utilisation d'un portail captif pour bénéficier d'une connexion Internet peut être problématique. Ce cas d'administration à distance, probablement depuis un lieu public, devant théoriquement être exceptionnel, il est alors recommandé d'utiliser le partage de connexion Internet d'un téléphone mobile de confiance.

Par ailleurs, il est recommandé de dédier un concentrateur VPN pour l'accès à distance au SI d'administration, distinct de celui utilisé pour l'accès à distance des utilisateurs aux autres SI. Pour obtenir un niveau de confiance suffisant, ce concentrateur VPN doit être physiquement dédié.

9. Le *split tunnelling* est un concept de réseau informatique consistant à donner accès simultanément à deux réseaux (ex. : réseau local et réseau distant à travers un tunnel IPsec).

Enfin, suivant le niveau de confiance accordé aux différentes catégories d'administrateurs (ex. : internes ou externes, de SI critiques ou non critiques), il est recommandé de dédier un concentrateur VPN par catégorie d'administrateurs. Cette mesure doit être en cohérence avec le cloisonnement interne des zones d'administration auxquelles ces concentrateurs VPN sont connectés.

R51

### Dédier un concentrateur VPN IPsec physique pour l'administration à distance

Pour l'administration à distance, un concentrateur VPN IPsec physiquement dédié doit être déployé en périphérie du SI d'administration, en frontal du réseau non maîtrisé (ex. : Internet, partenaires).



#### Attention

Il est important de s'assurer du respect de la recommandation R21 si des flux d'administration traversent un réseau tiers en sortie du concentrateur VPN dédié pour l'accès à distance.

La figure 10.1 représente les cas d'administration à distance dont le nomadisme.

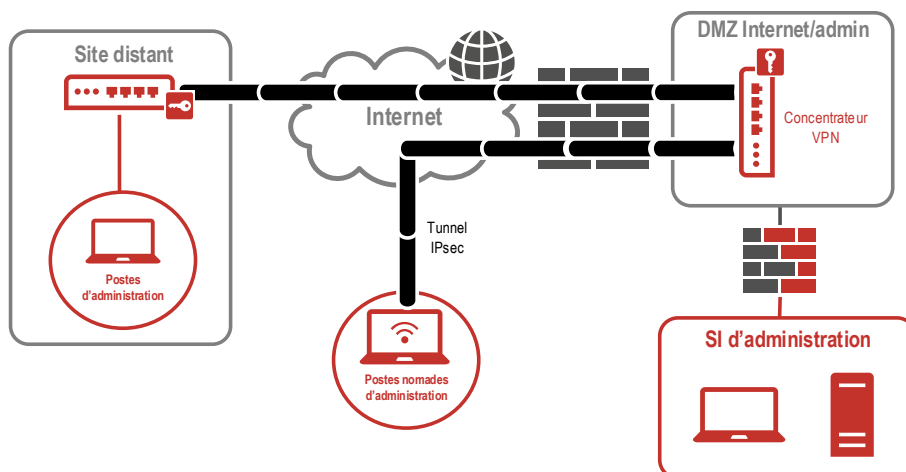


FIGURE 10.1 – Administration à distance et nomadisme

# 11

## Systèmes d'échanges sécurisés

Afin de pallier les risques liés à l'usage de supports de stockage amovibles (ex. : clé USB) sur le poste d'administration, des systèmes d'échanges sécurisés doivent être proposés. Afin de distinguer les exigences de sécurité suivant les usages, on convient de parler de :

- *système d'échange interne* pour les échanges au sein du SI d'administration ;
- *système d'échange externe* pour les échanges entre le SI d'administration et un SI bureautique (éventuellement connecté à Internet).

Quels qu'ils soient, il est primordial que ces dispositifs ne fragilisent pas les moyens de protection du SI d'administration et soient intégrés au périmètre de l'analyse de risque. Il est également nécessaire d'établir précisément la liste des besoins en matière d'échange (type d'informations, volumétrie, fréquence).

R52

### Déployer des systèmes d'échanges sécurisés

Afin de répondre aux besoins fonctionnels d'échanges internes et externes au SI d'administration, il est nécessaire de mettre en place des systèmes d'échanges sécurisés.

## 11.1 Échanges au sein du SI d'administration

Dès lors que les administrateurs souhaitent partager entre eux des informations liées à ce rôle (ex : configurations, captures d'écran), il convient de mettre à disposition des moyens dédiés au sein du SI d'administration, en tant qu'infrastructures d'administration.

Par exemple, une messagerie dédiée au SI d'administration, asynchrone ou instantanée, peut être mise en place sous réserve qu'elle n'ait, conformément à la recommandation R10, aucune interconnexion avec Internet, de manière directe ou indirecte. Il peut s'agir plus basiquement d'un serveur de fichiers.

R53

### Dédier le système d'échange interne au SI d'administration

Le système d'échange interne au SI d'administration doit être déployé au sein des infrastructures d'administration du SI d'administration sans aucune interconnexion avec d'autres SI.

## 11.2 Échanges en dehors du SI d'administration

Malgré l'interdiction d'accès à Internet depuis les postes d'administration prescrite par la recommandation R10, les administrateurs peuvent avoir besoin d'échanger des informations (ex. : en-



voi de journaux, récupération de correctifs) avec des correspondants extérieurs (ex. : éditeurs, équipementiers).

Un système d'échange externe (cf. figure 11.1) doit alors être mis en place et peut par exemple se composer de pare-feux et de services client/serveur (ex. : SCP, SFTP) avec une ou plusieurs interconnexions. Dans ce cas, les flux doivent être autorisés de la façon suivante :

- depuis un poste d'administration (client) vers le système d'échange externe (serveur) ;
- depuis un poste bureautique (client) vers le système d'échange externe (serveur).

On garantit ainsi qu'aucun flux direct n'est autorisé entre le SI bureautique et le SI d'administration.

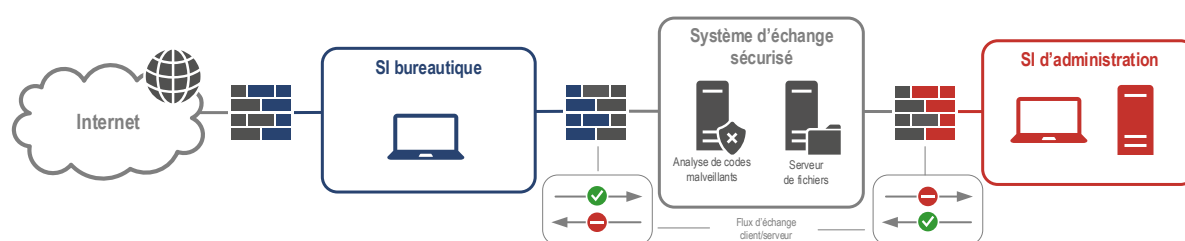


FIGURE 11.1 – Représentation fonctionnelle d'un système d'échange externe



### Information

Pour des besoins d'échanges simples de texte, un serveur *pastebin* (ou gestionnaire d'extraits de texte et de code source) peut se substituer ou s'ajouter à un serveur de fichiers au sein du système d'échange externe.

Le système d'échange externe doit par ailleurs autoriser seulement les protocoles de transfert de données et interdire toute possibilité d'ouvrir des sessions de travail. Par exemple, dans le cas du service SSH, celui-ci doit être configuré pour autoriser uniquement des commandes de transferts de fichiers de type SCP (*Secure Copy*) ou SFTP (*SSH File Transfer Protocol*). Les recommandations du guide afférent de l'ANSSI [6] sont applicables.

R54

### N'autoriser que des protocoles de transfert vers le système d'échange externe

Seuls les services et les protocoles permettant le transfert de données doivent être autorisés *vers* le système d'échange externe ; les flux doivent toujours être à l'initiative des clients situés en dehors du système d'échange. *En aucun cas*, il ne doit être possible d'accéder à une session de travail par le biais du système d'échange externe.

L'accès à un système d'échange externe depuis le SI bureautique doit être réservé strictement aux postes et aux utilisateurs ayant le besoin de transférer des informations vers le SI d'administration. Cela réduit la probabilité qu'une autre machine, plus exposée et potentiellement compromise, puisse déposer des fichiers malveillants sur le système d'échange externe. Cette restriction peut être réalisée par la mise en œuvre d'un filtrage et d'un contrôle d'accès au système d'échange externe.

R55

### limiter au strict besoin opérationnel l'accès au système d'échange externe

Il est recommandé de restreindre l'accès au système d'échange externe du SI d'administration uniquement aux postes et aux utilisateurs qui en ont le besoin.

Afin de ne pas compromettre son ou ses comptes d'administration, il est essentiel qu'un administrateur s'authentifie sur le système d'échange externe avec un compte référencé dans un annuaire dédié ou positionné dans le SI bureautique et *en aucun cas* avec un compte référencé dans un annuaire du SI d'administration.

R56

### Ne pas s'authentifier avec un compte d'administration sur le système d'échange externe

Les administrateurs ne doivent pas s'authentifier avec un compte d'administration sur le système d'échange externe considéré comme de moindre confiance par rapport au SI d'administration.

Pour limiter les risques de fuite ou de compromission des données échangées, un système d'échange externe ne doit pas stocker durablement les fichiers transférés.

R57

### Ne pas stocker de données de manière permanente dans un système d'échange externe

Les données échangées ne doivent pas être stockées de manière permanente sur un système d'échange externe. Dès que leur transfert est effectif ou à défaut dans un délai raisonnable (ex. : 24 h), elles doivent être supprimées.

Enfin, les mécanismes de filtrage de contenu et de protection contre les codes malveillants doivent être systématiquement déployés. Cette mesure vise à protéger les ressources d'administration des risques de compromission par exécution de code malveillant, qui aurait été véhiculé par des fichiers ou des binaires dont l'origine n'est pas de confiance.

R58

### Analyser le contenu des données échangées par le système d'échange externe

Toutes les données transitant par le système d'échange externe doivent être soumises systématiquement à une analyse de contenu à la recherche de codes malveillants.

# 12

## Administration par des tiers et assistance à distance

Pour l'administration de son ou de ses SI, une entité peut faire appel à des tiers (appelés génériquement *prestataires* par la suite) : constructeurs d'équipements, éditeurs de logiciels, intégrateurs en début de projet, etc. Les besoins d'accès aux SI peuvent être réguliers (p. ex. dans le cadre d'un contrat d'infogérance) ou ponctuels (p. ex. dans le cadre d'un contrat de support). L'accès au SI de l'entité, généralement à distance, constitue alors un risque majeur de compromission, d'autant plus si certaines ressources de ces prestataires, comme leurs postes de travail, ne sont pas maîtrisées ou mutualisées entre clients. L'existence de ce risque est avérée avec des attaques réelles appartenant à la famille des attaques de la chaîne d'approvisionnement<sup>10</sup> (ou *supply chain attacks*, en anglais).

De plus, en cas de panne, la priorité est généralement donnée au rétablissement du service, parfois au détriment de la sécurité des conditions d'accès au SI (ex. : prise en main d'un poste d'administration via Internet, mise à disposition d'un accès réseau élargi ou d'un compte à privilèges supérieurs aux besoins). Il est donc primordial d'anticiper ces besoins et de fixer un cadre avant que la panne survienne.

Dans ce chapitre, on distingue volontairement :

- l'administration par des tiers (section 12.1) qui consiste à donner un accès, généralement à distance, à des prestataires pour la réalisation d'actions d'administration ;
- l'assistance à distance (section 12.2) qui consiste à donner un accès à distance pour assister un administrateur interne dans la réalisation de ses actions d'administration, par exemple grâce à un partage d'écran du poste d'administration, sans capacité technique de réaliser des actions d'administration.

### 12.1 Administration par des tiers

#### 12.1.1 Qualification PAMS

Afin d'évaluer la qualité des prestations d'infogérance, un référentiel d'exigences [26] a été élaboré par l'ANSSI. Celui-ci vise à apporter aux entités clientes les garanties nécessaires, tant en matière de sécurité que de confiance à accorder aux prestataires qui les réalisent.

Cette qualification, valorisée par un visa de sécurité ANSSI, permet d'identifier facilement les prestataires d'administration et de maintenance sécurisées fournissant une qualité de service à la hauteur des enjeux de sécurité actuels.

---

10. Lire à ce sujet le document du CERT-FR [2].

Une prestation PAMS répond, dans de bonnes conditions de sécurité, aux besoins d'administration par des tiers, qu'elle soit régulière ou ponctuelle, dans les locaux de l'entité ou à distance. C'est donc la solution à privilégier.

R59

### Recourir à une prestation d'infogérance qualifiée d'un PAMS

Dans le cas d'un contrat d'infogérance pour l'administration ou la maintenance d'un SI, il est recommandé d'avoir recours à un prestataire d'administration et de maintenance sécurisées qualifié et de contractualiser avec lui une prestation qualifiée <sup>11</sup>.

## 12.1.2 Administration ponctuelle à distance par des tiers

Pour des accès ponctuels au SI par des administrateurs tiers (p. ex. dans le cadre d'un contrat de support), dans le cas où l'entité aurait recours à une prestation qui n'est pas qualifiée PAMS, les recommandations suivantes visent à proposer des moyens d'accès alternatifs.



### Attention

Les mesures proposées ici permettent uniquement de réduire le risque de compromission du SI d'administration de l'entité depuis le poste de travail d'un administrateur tiers, non maîtrisé par l'entité.

Il est donc bien entendu que ces cas d'usage doivent constituer des exceptions et être intégrés à l'analyse de risque du SI d'administration. Cette section et les recommandations associées ne constituent *en aucun cas* une alternative à l'ensemble des recommandations précédentes, notamment pour l'administration réalisée par des administrateurs internes.

Tout d'abord, il s'agit d'intégrer au contrat liant les parties, des clauses standard aux contrats d'infogérance (cf. le guide de l'ANSSI sur l'infogérance [12]). Une description de la solution technique d'accès à distance au SI de l'entité, conforme aux recommandations de cette section, est recommandée.

R60

### Intégrer au contrat d'infogérance les exigences de sécurité d'accès à distance

Afin de disposer d'un cadre juridique, il est recommandé de rédiger, au sein du contrat liant les parties, les exigences de sécurité imposées au prestataire, et idéalement intégrer la description de la solution technique d'accès à distance au SI de l'entité.

Il est recommandé de s'appuyer sur le référentiel d'exigences PAMS [26].

Dans le cas où le poste de travail d'un administrateur tiers est fourni, administré et géré par le prestataire, ce dernier est responsable de sa protection physique et logique. Ce poste de travail ne peut pas être considéré comme de confiance pour l'entité. Il est toutefois recommandé de prévoir contractuellement une sécurisation à l'état de l'art des postes de travail des administrateurs tiers et une capacité d'effectuer des contrôles, par des audits ou l'utilisation d'un outil de contrôle de conformité.

11. Un prestataire qualifié garde la faculté de réaliser des prestations en dehors du périmètre pour lequel il est qualifié, mais ne peut, dans ce cas, se prévaloir de la qualification sur ces prestations.

R61

## Imposer une sécurisation à l'état de l'art des postes de travail des administrateurs tiers

Le prestataire doit s'engager à sécuriser physiquement les postes de travail des administrateurs tiers se connectant au SI d'administration de l'entité et se conformer :

- aux mesures de sécurisation de la section 4.3 ;
- aux pratiques d'hygiène informatique [13] dont :
  - > être à jour (système d'exploitation et logiciels),
  - > activer un pare-feu local,
  - > disposer d'une solution de protection du poste de travail (analyse antivirus et comportementale).



### Attention

Malgré les engagements contractuels pris, il n'y a pas, pour l'entité, de totale maîtrise de la sécurité du SI sur lequel est géré le poste de travail des administrateurs tiers. Le prestataire peut être la cible d'un attaquant souhaitant rebondir sur un SI de l'entité de manière discrète, sous couvert d'un accès légitime. Il n'est donc pas exclu qu'un poste de travail ayant fait l'objet d'un effort de sécurisation se trouve impliqué dans une chaîne de compromission du SI du prestataire.

Face à ce risque que le poste distant soit un vecteur d'attaque, il est nécessaire de prendre des mesures défensives au niveau du SI de l'entité. En premier lieu, grâce à des équipements physiques, une chaîne d'accès à distance doit être dédiée pour les administrateurs tiers.

R62

## Dédier une chaîne d'accès à distance pour les administrateurs tiers

Pour l'accès à distance des administrateurs tiers, il est recommandé de dédier une chaîne d'accès, distincte notamment de celle des administrateurs disposant de moyens d'accès maîtrisés. En particulier, les équipements (ex. : concentrateurs VPN, serveurs de rebond) doivent être physiquement dédiés et ne pas être mutualisés avec des équipements utilisés par d'autres populations (utilisateurs, administrateurs internes).

Dans la mesure du possible, les équipements de filtrage et de commutation sont physiquement dédiés, en priorité les équipements périmétriques. À défaut, un cloisonnement logique est réalisé.

Dans le cadre d'un accès à distance, il convient de sécuriser le canal de communication, généralement à travers Internet. Comme pour le nomadisme des administrateurs internes (cf. chapitre 10), la mise en œuvre de tunnels VPN est requise et l'utilisation de VPN IPsec est toujours recommandée par rapport à celle de VPN TLS. Le protocole TLS reste, dans le cas de l'administration par des tiers uniquement, une solution palliative davantage interopérable mais d'un niveau de sécurité moindre.

**R63**

### Utiliser un tunnel VPN IPSec pour la connexion du poste de travail des administrateurs tiers

Un tunnel VPN IPSec doit être mis en œuvre pour la connexion entre les postes de travail des administrateurs tiers et le concentrateur VPN de l'entité dédié aux administrateurs tiers. Les recommandations du guide IPSec de l'ANSSI [16] doivent être suivies.

**R63 -**

### Utiliser un tunnel VPN TLS pour la connexion du poste de travail des administrateurs tiers

À défaut d'utiliser IPSec, il est recommandé d'utiliser TLS pour établir le tunnel VPN entre les postes de travail des administrateurs tiers et le concentrateur VPN de l'entité dédié aux administrateurs tiers. Le cas échéant, une configuration à l'état de l'art avec le suivi des recommandations du guide TLS [20] doit être mise en œuvre. En particulier, toute version inférieure à TLS 1.2 ne doit pas être supportée.

Afin d'assurer une traçabilité précise des accès et des actions d'administration puis d'appliquer au mieux le principe du moindre privilège, l'utilisation de comptes dédiés aux administrateurs tiers est un pré-requis. En complément, le cloisonnement de ces comptes d'accès dans un annuaire dédié peut être envisagé pour réduire l'exposition des autres annuaires de l'entité.

**R64**

### Dédier des comptes d'accès et des comptes d'administration aux administrateurs tiers

Des comptes d'accès dédiés (pour l'accès VPN notamment), ainsi que des comptes d'administration dédiés (pour l'accès aux ressources administrées) doivent être créés pour les administrateurs tiers. L'utilisation de comptes individuels est à privilégier par rapport à l'utilisation de comptes génériques. Ces comptes doivent être intégrés à la procédure de gestion du cycle de vie des comptes. L'utilisation par les administrateurs tiers de comptes par défaut ou de comptes d'autres utilisateurs est à proscrire.

**R65 +**

### Dédier un annuaire aux comptes d'accès des administrateurs tiers

Afin de réduire l'exposition des annuaires utilisés par les autres services de l'entité, il est recommandé, de manière complémentaire à R64, de dédier un annuaire aux comptes d'accès des administrateurs tiers.

Afin d'éviter tout accès et toute action d'administration en dehors des périodes légitimes, il est nécessaire de prévoir un processus organisationnel permettant d'activer exclusivement à la demande les comptes des administrateurs tiers.

**R66**

### Activer à la demande les comptes des administrateurs tiers

Les comptes des administrateurs tiers doivent être désactivés par défaut et activés à la demande, en priorité les comptes d'accès VPN. Si un compte est actif au-delà d'un délai maximal cohérent avec les interventions (p. ex. 24 h), une procédure automatique de désactivation doit être déclenchée ou une alerte doit être levée.

Afin d'éviter notamment le rejeu d'un couple identifiant et mot de passe qui aurait été récupéré par un attaquant, une authentification double facteur est recommandée. Si le second facteur est un jeton physique et qu'il est complexe de gérer son cycle de vie avec les prestataires en raison de l'éloignement géographique ou du changement régulier des administrateurs tiers, ce jeton peut éventuellement être conservé par l'entité. Le cas échéant, un processus organisationnel doit être prévu pour les interventions (ex. : un appel téléphonique entre l'entité et l'administrateur tiers pour valider l'authentification avec le second facteur une fois le mot de passe saisi).

Pour répondre différemment au risque, des mots de passe temporaires peuvent être utilisés par exemple.

R67

### Renforcer l'authentification des administrateurs tiers

Pour renforcer l'authentification des administrateurs tiers, l'utilisation d'un second facteur d'authentification, éventuellement conservé par l'entité, est recommandée. En alternative, il est recommandé de générer un mot de passe non trivial et temporaire par session : les mots de passe des comptes des administrateurs tiers sont renouvelés avant chaque nouvelle connexion et expirent au terme d'une durée inférieure à la journée.

Au-delà des mesures de sécurisation des ressources administrées dans le cadre de l'administration courante, la mise en œuvre en DMZ d'un rebond (poste ou serveur) durci, dédié à l'administration par des tiers, permet une rupture protocolaire. De plus, la possibilité de supprimer ce rebond après utilisation réduit le risque d'une attaque persistante,

R68

### Mettre en œuvre un rebond éphémère en coupure de la terminaison VPN et du SI administré

Il est recommandé de mettre en œuvre un rebond (poste ou serveur) durci en coupure de la terminaison VPN et du SI administré. Il est recommandé que ce rebond soit éphémère, par exemple sous forme de machine virtuelle générée uniquement pour la durée de l'intervention, et hébergée sur un hyperviseur dédié. Ce rebond peut être une instanciation d'un poste d'administration de l'entité. De plus, il est recommandé que ce rebond soit dédié par prestataire et minimaliste du point de vue logiciel.

Il est recommandé d'assurer un contrôle d'accès sur les ressources administrées, conforme au strict besoin opérationnel, et d'assurer une traçabilité exhaustive, textuelle ou vidéo, des actions accomplies par les administrateurs tiers.

R69

### Mettre en œuvre un contrôle d'accès strict et une traçabilité pour les administrateurs tiers

Les accès des administrateurs tiers doivent être restreints au strict besoin opérationnel à l'aide d'un contrôle d'accès. Ces accès et les actions accomplies par les administrateurs tiers doivent être tracés.



## Information

Certaines solutions permettent de mettre en œuvre des sessions de travail dites « *four-eyes* » (ou « quatre yeux » en français) pour permettre le contrôle visuel, en temps réel, par un administrateur interne, des actions réalisées par un administrateur tiers. Ces sessions peuvent être enregistrées et constituer des éléments de traçabilité vidéo.

Un exemple d'architecture est proposé sur la figure 12.1.

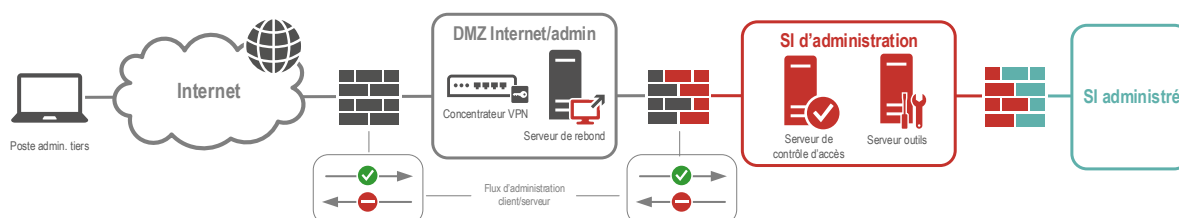


FIGURE 12.1 – Exemple d'architecture d'administration à distance par des tiers

## 12.2 Assistance à distance

Dans le cas de l'assistance à distance, une personne experte, ne disposant pas d'un poste d'administration, assiste à distance un administrateur interne avec un partage d'écran du poste d'administration. Dans ce cas, aucune action d'administration n'est possible depuis le poste de travail distant.

Deux solutions sont alors envisageables : l'utilisation d'un boîtier matériel d'acquisition vidéo unidirectionnelle depuis le poste d'administration vers un poste bureautique connecté à une solution collaborative accessible sur Internet, ou la mise en œuvre en DMZ d'une solution logicielle collaborative accessible sur Internet et dédiée à ce strict besoin opérationnel.

Quelle que soit la solution retenue, durant l'assistance, l'administrateur interne doit prendre garde à ne pas afficher d'informations sensibles (ex. : mots de passe) sans rapport avec l'assistance.



## Attention

Il existe de nombreuses solutions d'assistance voire de prise en main à distance, parfois gratuites, et souvent simples à déployer en installant exclusivement un agent logiciel sur le poste de la personne aidante d'une part et sur le poste de la personne aidée d'autre part. Ces solutions sont à proscrire pour une utilisation depuis une ressource d'administration dans la mesure où, dans ce cas :

- la ressource d'administration doit accéder ou être exposée directement sur Internet ;
- la négociation des clés de chiffrement utiles à la sécurisation des échanges est généralement réalisée sur les infrastructures du prestataire de la solution et ne garantit donc pas un canal fiable en cas de compromission de ce prestataire.



## 12.2.1 Utilisation d'un boîtier matériel d'acquisition vidéo

Dans le contexte d'une assistance à distance, une solution consiste à exporter l'affichage d'un poste d'administration sur un poste bureautique ayant accès à Internet et à une solution collaborative intégrant le partage d'écran. L'utilisation d'un boîtier matériel d'acquisition vidéo (VGA ou HDMI vers USB) unidirectionnelle entre les deux postes garantit une rupture protocolaire.

Un exemple d'architecture est proposé sur la figure 12.2.

Les échanges audio (ou visio) entre personnes peuvent se faire par téléphone ou grâce à la solution collaborative accessible depuis le poste bureautique.

**R70**

### Utiliser un boîtier matériel d'acquisition vidéo pour l'assistance à distance

Pour les besoins d'assistance à distance, il est recommandé d'utiliser, le temps de l'intervention, un boîtier matériel dédié d'acquisition vidéo unidirectionnelle pour permettre un export d'affichage depuis un poste d'administration vers un poste bureautique.

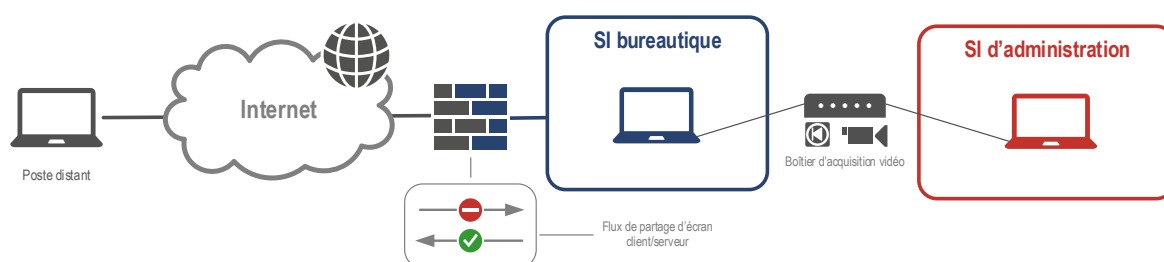


FIGURE 12.2 – Utilisation d'un boîtier matériel d'acquisition vidéo unidirectionnelle pour l'assistance à distance

## 12.2.2 Mise en œuvre d'une solution logicielle collaborative dédiée

Pour les besoins d'assistance à distance, il est également possible de prévoir une infrastructure de partage d'écran, centralisée et dédiée. Dans ce cas, cette infrastructure assurant la rupture protocolaire est déployée en DMZ : le serveur de partage d'écran est accessible par le poste d'administration d'une part et par le poste de travail distant d'autre part, ce serveur est protégé de façon *ad hoc* dès lors qu'il est exposé sur Internet (p. ex derrière un serveur mandataire inverse).

Un exemple d'architecture est proposé sur la figure 12.3.

Le partage d'écran peut être un sous-ensemble des fonctionnalités d'une solution collaborative plus complète. Le recours à un produit qualifié par l'ANSSI et une configuration limitant strictement l'usage au partage d'écran sont donc recommandés le cas échéant.

## Mettre en œuvre une solution logicielle dédiée pour l'assistance à distance

Pour les besoins d'assistance à distance, il est recommandé de mettre en œuvre en DMZ une infrastructure dédiée de partage d'écran. Le cas échéant, toutes les fonctions interactives vis-à-vis du poste d'administration (ex. : prise de contrôle distante) doivent être désactivées de sorte qu'aucune action d'administration ne puisse être réalisée depuis le poste de travail distant.

Les recommandations R64, R65+, R66, R67 et R69 doivent s'appliquer dans ce contexte d'assistance à distance.

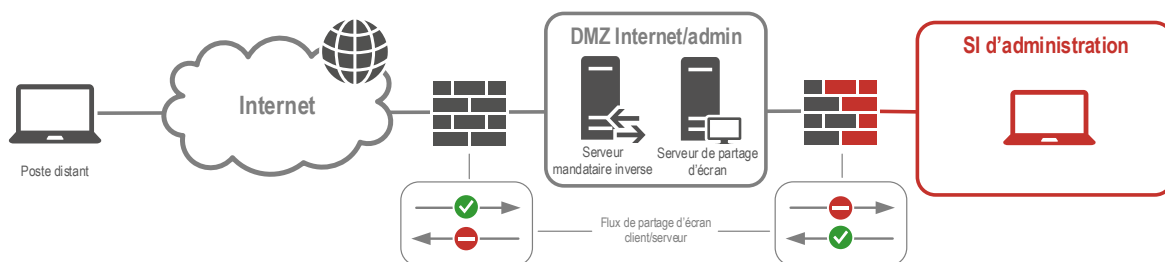


FIGURE 12.3 – Utilisation d'une solution logicielle dédiée pour l'assistance à distance

# 13

## Cas particuliers d'architectures de SI d'administration

Inspiré de cas pratiques rencontrés, ce chapitre propose des indications de mise en œuvre découlant des recommandations de ce guide ; il met aussi en garde sur des pratiques non souhaitables.

### 13.1 Utilisation d'un bastion

Il existe sur le marché des produits nommés *bastions d'administration* ou plus simplement *bastions*. Il s'agit d'une déclinaison du rebond, tel qu'introduit dans la section 6.3. Ces équipements concentrent généralement plusieurs fonctions de sécurité, comme par exemple la gestion centralisée de l'authentification, la traçabilité, le renouvellement automatique des secrets.



#### Attention

Comme tout produit de sécurité, de surcroît disposant d'un nom commercial pouvant procurer un sentiment de sécurité, il convient d'être vigilant sur son choix, son déploiement et son exploitation.

Le déploiement d'un bastion pour les actions d'administration ne se substitue évidemment pas à l'ensemble des recommandations de ce document, notamment le cloisonnement du SI d'administration et la sécurisation du poste d'administration décrite dans le chapitre 4. En effet, le bastion constitue une ressource d'administration critique dans la mesure où il concentre potentiellement à un instant des secrets d'authentification des comptes d'administration ou des journaux liés aux actions d'administration. Il ne doit donc pas être exposé sur un SI de faible niveau de confiance, un SI bureautique par exemple.

Dès lors que le niveau de confiance dans les différentes fonctions de l'équipement est satisfaisant – à travers un processus de qualification de l'ANSSI par exemple – et qu'un équipement de rebond est jugé pertinent dans l'architecture du SI d'administration, celui-ci doit être déployé au sein du SI d'administration, dans la zone d'infrastructures d'administration (cf. figure 13.1).



#### Attention

La solution qui consisterait à déployer un bastion comme moyen d'interconnexion d'un SI bureautique et d'un SI d'administration est à proscrire (cf. figure 13.1). Cela procurerait un faux sentiment de sécurité alors qu'en réalité le bastion, porte d'entrée unique vers le SI d'administration, constituerait une opportunité d'attaque considérable depuis un poste bureautique accédant à Internet.



FIGURE 13.1 – Intégration d'un bastion dans un SI d'administration

## 13.2 Possible mutualisation du poste d'administration

Pour des raisons budgétaires ou opérationnelles, il peut être souhaitable de mutualiser un poste d'administration pour différentes zones d'administration et ainsi administrer différentes zones de confiance voire différents SI d'une même entité, par exemple : des pare-feux d'une zone interne et des pare-feux d'une zone exposée à Internet, des équipements réseau (administration réseau) et des hyperviseurs (administration système), une zone d'hébergement de niveau usuel et une zone d'hébergement de niveau Diffusion Restreinte au sens de l'II 901 [23].



### Information

Les principes proposés pour la mutualisation du poste d'administration peuvent être appliqués dans le contexte d'une même entité finale mais ils ne conviennent pas à un contexte multi-clients pour un infogérant. De plus, ils sont non exhaustifs et doivent être en phase avec l'analyse de risque menée, conformément à R4.



### Attention

La mutualisation du poste d'administration ne doit pas affaiblir les cloisonnements, physiques ou logiques, mis en œuvre entre les zones de confiance au sein du ou des SI administrés.

Pour rappel (cf. chapitre 6), un poste d'administration peut disposer d'outils d'administration installés localement ou, de manière non exclusive, accéder à des serveurs outils d'administration.

Un administrateur peut disposer d'un poste d'administration unique pour l'administration de différentes zones de confiance, aux conditions suivantes :

- la sécurisation du poste d'administration doit être en phase avec les besoins de sécurité de la zone de confiance administrée la plus exigeante (ex. : un poste d'administration physiquement dédié conforme à R9 pour administrer un SI critique peut servir à l'administration d'un SI standard);
- le poste d'administration peut servir pour l'administration des zones de confiance de différentes sensibilités (ex. : non sensible et sensible, voire non sensible et Diffusion Restreinte au sens de l'II 901 [23]) mais en aucun cas des SI de différentes classifications au sens de l'IGI 1300 [3];
- les serveurs outils accessibles depuis le poste d'administration ne doivent pas être mutualisés pour l'administration de deux zones de confiance distinctes (en d'autres termes, un serveur outils reste dédié à une unique zone de confiance et cloisonné dans une zone d'administration);

- les éventuels outils locaux au poste d'administration permettant un accès direct aux ressources administrées doivent être cloisonnés afin d'éviter tout rebond entre deux ressources administrées de deux zones de confiance distinctes à travers le poste d'administration (en d'autres termes, sur un poste d'administration mutualisé, les environnements d'exécution d'outils d'administration locaux de deux zones de confiance distinctes doivent être distincts, par exemple par l'utilisation de la conteneurisation);
- l'accès aux différentes zones de confiance depuis le SI d'administration doit respecter le cloisonnement, physique ou logique, entre zones de confiance (en d'autres termes, deux pare-feux physiques ou un pare-feu configuré avec deux DMZ sont déployés en périphérie du SI d'administration, pour respecter le cloisonnement des zones de confiance).

Les figures 13.2 et 13.3 représentent le cas de mutualisation d'un poste d'administration de deux zones de confiance distinctes, respectivement d'un niveau de confiance homogène ou hétérogène.

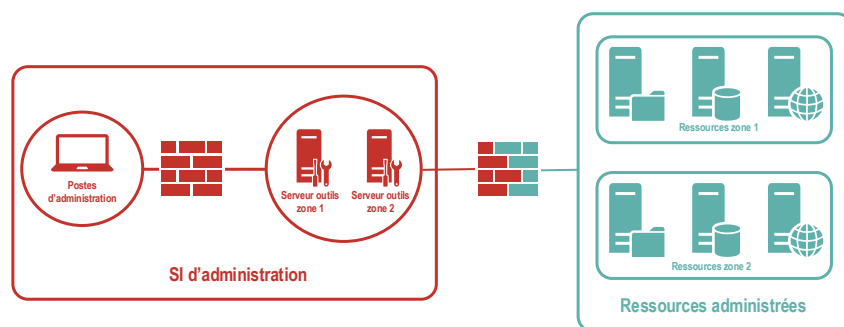


FIGURE 13.2 – Mutualisation du poste d'administration pour deux zones de confiance homogène

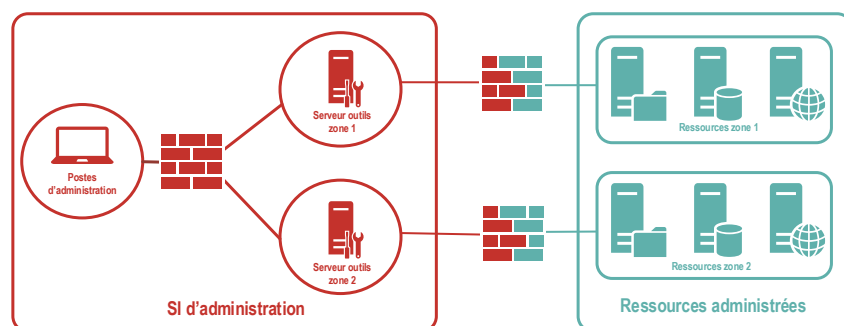


FIGURE 13.3 – Mutualisation du poste d'administration pour deux zones de confiance hétérogène

## 13.3 Une ou plusieurs solutions de poste d'administration ?

Le poste d'administration est un point clé de l'architecture du SI d'administration. Trois solutions d'un niveau de sécurité décroissant sont proposées dans le chapitre 4. Pour des raisons opérationnelles il peut sembler préférable de ne retenir qu'une seule de ces solutions.

Toutefois, pour certaines entités, une solution unique, nivelée par le bas du point de vue de la sécurité, peut répondre à l'ensemble des besoins fonctionnels mais être insuffisante pour couvrir les risques de l'administration des équipements ou des SI les plus critiques. À l'inverse, une solution

unique nivelée par le haut peut être disproportionnée pour des SI moins sensibles ou inadaptée pour des SI très complexes.

Dans ce cas, il est souhaitable de faire cohabiter deux solutions (ex. : un poste dédié conforme à R9 et un poste avec accès distant au SI bureautique conforme à R9-). Pour simplifier la maintenance, les postes d'administration peuvent alors bénéficier d'un socle de durcissement commun et l'accès à distance au SI bureautique est réservée, en option, à certains d'entre eux (cf. figure 13.4).



### Attention

Il convient de respecter la contrainte suivante : *in fine* un outil d'administration ne peut être utilisé, ou une ressource ne peut être administrée, que par un seul type de poste d'administration.

Dès lors, il est nécessaire de construire deux chaînes d'accès distinctes du SI d'administration et s'assurer d'un cloisonnement logique ou physique entre celles-ci. Par exemple, pour un cloisonnement logique, il est recommandé :

- dans le cas d'un réseau d'administration physique, d'utiliser un VLAN distinct par type de poste d'administration ;
- dans le cas d'un réseau d'administration logique à base de VPN IPsec, de déployer un profil VPN distinct par type de poste d'administration.

Ainsi, un filtrage à base de pare-feu permet ensuite de restreindre l'accès aux serveurs outils ou aux ressources administrées conformément au message d'avertissement *infra*, tout en permettant un accès partagé à certaines infrastructures d'administration (ex. : annuaire, serveurs de mise à jour).

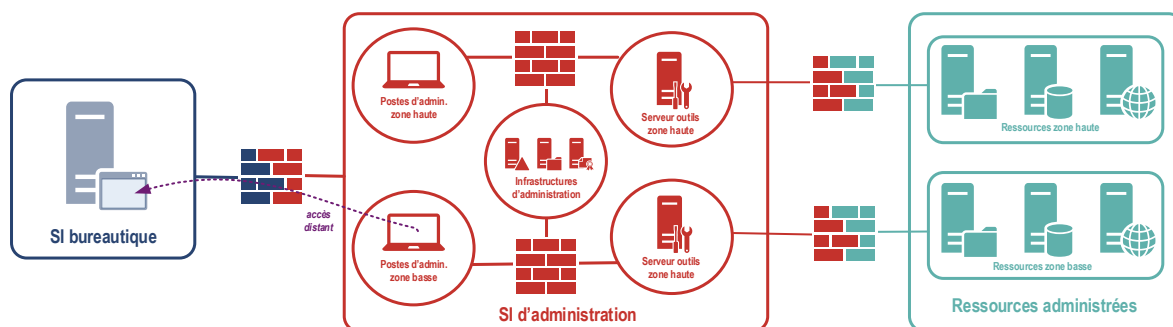


FIGURE 13.4 – SI d'administration intégrant deux solutions de poste d'administration

## 13.4 Administration des ressources d'administration

Quelles que soient les mesures prises pour la sécurisation de l'administration d'un SI, la question de l'administration des ressources d'administration est inéluctable. Il est important que ces ressources (ex. : les postes d'administration, les serveurs outils d'administration) soient elles-mêmes administrées de manière sécurisée.

Pour cela, il est recommandé :

- soit de réaliser une administration locale dans le cas d'un « petit » SI d'administration disposant de seulement quelques ressources d'administration ;
- soit de déployer une zone d'administration dans le cas des SI d'administration plus importants, en mettant en œuvre des mesures de cloisonnement et de filtrage adéquates.

Dans ce cas d'usage, les postes d'administration utilisés doivent être d'un niveau de sécurité au moins équivalent à ceux servant à l'administration courante. Ils sont susceptibles d'utiliser des infrastructures d'administration partagées (ex. : un annuaire pour l'authentification) mais accèdent, dès que possible, à des interfaces dédiées pour l'administration des ressources du SI d'administration conformément à R18 ou R18- (cf. figure 13.5).

Par ailleurs, il est recommandé d'appliquer strictement le principe du moindre privilège aux comptes d'administration des administrateurs du SI d'administration.

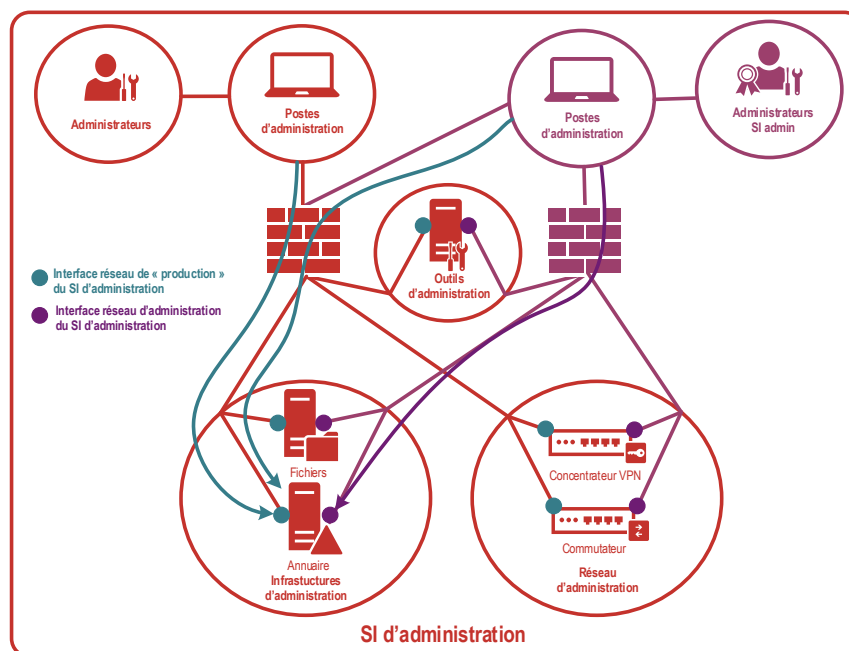


FIGURE 13.5 – Administration des ressources d'administration

## 13.5 Administration d'un SI déconnecté

Les recommandations du guide s'appliquent aussi à l'administration d'un SI déconnecté. Même s'ils peuvent sembler préservés des menaces extérieures, le SI déconnecté et son SI d'administration doivent être maintenus en condition opérationnelle et de sécurité. La récupération des mises à jour est le principal point d'attention.

Si le SI est déconnecté pour des raisons réglementaires (ex. : classifié de défense) ou de criticité et non pour des raisons de connectivité (ex. : absence de desserte), il peut être envisagé, sous certaines conditions, de construire une passerelle d'échanges. Pour cela, les besoins de sécurité spécifiques du SI déconnecté (ex. : confidentialité ou disponibilité) doivent être pris en compte. En particulier, la conception de la passerelle doit intégrer les contraintes réglementaires afférentes qui peuvent être beaucoup plus strictes que celles du système de récupération de mises à jour décrit sur la figure 8.1. À titre d'exemple, une passerelle d'interconnexion entre deux SI non-classifié et classifié

doit reposer sur des produits agréés et faire l'objet d'une homologation spécifique [3]. La conception d'une telle passerelle dépasse donc largement le cadre du présent document.

À défaut, une procédure de type *air gap* avec l'utilisation d'un support amovible dédié aux échanges entre un SI tiers connecté et le SI d'administration du SI déconnecté est possible. Une détection préalable de codes malveillants doit être réalisée et une vérification d'intégrité peut être réalisée à l'occasion du chargement des fichiers sur le SI d'administration du SI déconnecté.

## 13.6 Administration de ressources dans un cloud public

Dans le cas où tout ou partie du SI de l'entité est hébergé dans un *cloud* public, il convient d'adapter l'accès aux outils d'administration, généralement exposés uniquement sur Internet. Cette section n'a pas vocation à être exhaustive sur le sujet mais vise à donner quelques pistes de mise en œuvre en cohérence avec le référentiel d'exigences [26] pour les prestataires d'administration et de maintenance sécurisées (PAMS).

D'une part, les mesures de sécurité, sous maîtrise du fournisseur *cloud*, doivent être mises en œuvre autant que possible pour l'accès aux outils d'administration (API ou interface Web) : filtrage sur les adresses IP source, authentification double facteur, journalisation renforcée, interconnexion à travers un tunnel IPsec.

D'autre part, pour l'entité, ce cas d'usage ne remet pas en cause le besoin d'intégrité du poste d'administration ; l'utilisation d'un poste d'administration dédié et l'interdiction par défaut de l'accès à Internet depuis ce poste restent recommandées. Pour l'accès aux outils d'administration exposés exclusivement sur Internet, afin d'assurer une rupture protocolaire, une infrastructure de postes de rebond virtualisés et dédiés peut être mise en œuvre au sein d'une zone dédiée du SI d'administration. Ces postes de rebond sont accessibles uniquement aux postes d'administration, par connexion à distance dont les fonctions d'échange sont désactivées ; ils sont distincts des postes bureautiques de la recommandation R9-. De plus, ces postes de rebond accèdent à Internet, suivant le strict besoin opérationnel de l'administration de ressources dans le *cloud* public, à travers une DMZ, conformément aux recommandations du guide d'interconnexion d'un SI à Internet [21] : utilisation d'un serveur mandataire, authentification, liste d'autorisations d'adresses IP ou Web dédiées à l'administration de ressources dans le *cloud* public. Les postes de rebond virtualisés sont supprimés et réinstanciés régulièrement (p. ex. quotidiennement) pour réduire le risque d'une attaque persistante.

La figure 13.6 illustre un exemple de cette architecture.

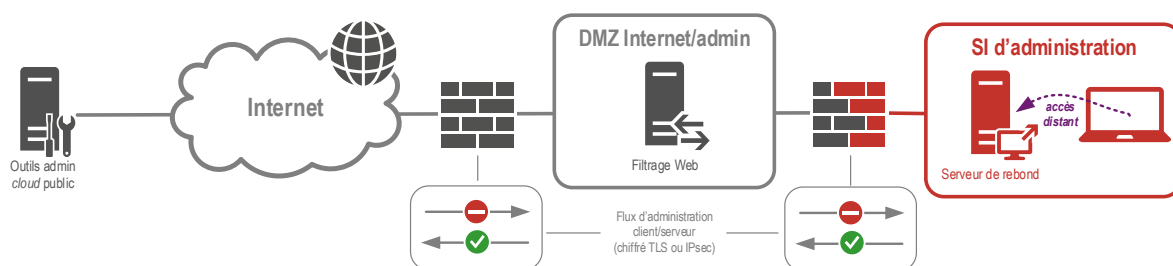


FIGURE 13.6 – Administration de ressources dans un *cloud* public



# Liste des recommandations

<b>R1</b>	Informer les administrateurs de leurs droits et devoirs	8
<b>R2</b>	Former les administrateurs à l'état de l'art en matière de SSI	8
<b>R3</b>	Disposer d'une documentation des SI à jour	9
<b>R4</b>	Mener une analyse de risque sur le SI d'administration et son écosystème	10
<b>R5</b>	Définir les zones de confiance du SI administré et déduire les zones d'administration	12
<b>R6</b>	Privilégier l'utilisation de produits qualifiés par l'ANSSI	12
<b>R7</b>	Dédier des socles physiques en cas de virtualisation des infrastructures d'administration	14
<b>R8</b>	Gérer et configurer le poste d'administration	15
<b>R9</b>	Utiliser un poste d'administration dédié	16
<b>R9-</b>	Utiliser un poste d'administration multi-niveaux	17
<b>R9- -</b>	Utiliser un poste d'administration avec accès distant au SI bureautique	19
<b>R10</b>	Bloquer tout accès à Internet depuis ou vers le poste d'administration	20
<b>R11</b>	Durcir le système d'exploitation du poste d'administration	21
<b>R12</b>	Restreindre les droits d'administration sur le poste d'administration	21
<b>R13</b>	Limiter les logiciels installés sur le poste d'administration	22
<b>R14</b>	Chiffrer l'ensemble des périphériques de stockage utilisés pour l'administration	22
<b>R15</b>	Connecter les ressources d'administration sur un réseau physique dédié	23
<b>R15-</b>	Connecter les ressources d'administration sur un réseau VPN IPsec dédié	23
<b>R16</b>	Appliquer un filtrage interne et périmétrique au SI d'administration	24
<b>R17</b>	Appliquer un filtrage local sur les ressources administrées	25
<b>R18</b>	Dédier une interface réseau physique d'administration	26
<b>R18-</b>	Dédier une interface réseau virtuelle d'administration	26
<b>R19</b>	Appliquer un filtrage entre ressources d'administration et ressources administrées	26
<b>R20</b>	Bloquer toute connexion entre ressources administrées à travers le réseau d'administration	27
<b>R21</b>	Protéger les flux d'administration transitant sur un réseau tiers	27
<b>R22</b>	Déployer les outils d'administration sur des serveurs dédiés par zone d'administration	29
<b>R23</b>	Appliquer un filtrage entre les postes d'administration et les serveurs outils d'administration	30
<b>R24</b>	Utiliser des protocoles sécurisés pour les flux d'administration	30
<b>R24-</b>	Protéger le cas échéant les flux d'administration dans un tunnel VPN IPsec	30
<b>R25</b>	Étudier la mise en œuvre d'une rupture protocolaire des flux d'administration	31
<b>R26</b>	Renoncer à la rupture protocolaire pour les besoins en confidentialité	32
<b>R27</b>	Utiliser des comptes d'administration dédiés	33
<b>R28</b>	Protéger l'accès aux annuaires des comptes d'administration	34
<b>R29</b>	Réserver les comptes d'administration aux seules actions d'administration	34
<b>R30</b>	Utiliser par défaut des comptes d'administration individuels	34
<b>R31</b>	Journaliser les événements liés aux comptes d'administration	35
<b>R32</b>	Prévoir un processus de gestion des comptes d'administration	35
<b>R33</b>	Se référer au RGS pour choisir les mécanismes d'authentification	35

<b>R34</b>	Modifier les mots de passe par défaut des comptes natifs	36
<b>R35</b>	Stocker les mots de passe dans un coffre-fort de mots de passe	36
<b>R36</b>	Privilégier une authentification double facteur pour les actions d'administration	36
<b>R37</b>	Utiliser des certificats électroniques de confiance pour l'authentification	37
<b>R38</b>	Mettre en œuvre une gestion centralisée de l'authentification	37
<b>R39</b>	Respecter le principe du moindre privilège dans l'attribution des droits d'administration	37
<b>R40</b>	Attribuer les droits d'administration à des groupes	38
<b>R41</b>	Déployer des politiques de sécurité	38
<b>R42</b>	Réaliser scrupuleusement le MCS du SI d'administration	39
<b>R43</b>	Mettre en place des serveurs relais pour la récupération des mises à jour	39
<b>R44</b>	Valider les correctifs de sécurité avant leur généralisation	40
<b>R45</b>	Définir une politique de sauvegarde du SI d'administration	41
<b>R46</b>	Dédier une zone d'administration à la journalisation	42
<b>R47</b>	Centraliser la collecte des journaux d'événements	42
<b>R48</b>	Installer un filtre de confidentialité sur le poste d'administration nomade	43
<b>R49</b>	Utiliser un tunnel VPN IPsec pour la connexion du poste d'administration à distance	44
<b>R50</b>	Empêcher toute modification de la configuration VPN du poste d'administration	44
<b>R51</b>	Dédier un concentrateur VPN IPsec physique pour l'administration à distance	45
<b>R52</b>	Déployer des systèmes d'échanges sécurisés	46
<b>R53</b>	Dédier le système d'échange interne au SI d'administration	46
<b>R54</b>	N'autoriser que des protocoles de transfert vers le système d'échange externe	47
<b>R55</b>	Limiter au strict besoin opérationnel l'accès au système d'échange externe	48
<b>R56</b>	Ne pas s'authentifier avec un compte d'administration sur le système d'échange externe	48
<b>R57</b>	Ne pas stocker de données de manière permanente dans un système d'échange externe	48
<b>R58</b>	Analyser le contenu des données échangées par le système d'échange externe	48
<b>R59</b>	Recourir à une prestation d'infogérance qualifiée d'un PAMS	50
<b>R60</b>	Intégrer au contrat d'infogérance les exigences de sécurité d'accès à distance	50
<b>R61</b>	Imposer une sécurisation à l'état de l'art des postes de travail des administrateurs tiers	51
<b>R62</b>	Dédier une chaîne d'accès à distance pour les administrateurs tiers	51
<b>R63</b>	Utiliser un tunnel VPN IPSec pour la connexion du poste de travail des administrateurs tiers	52
<b>R63-</b>	Utiliser un tunnel VPN TLS pour la connexion du poste de travail des administrateurs tiers	52
<b>R64</b>	Dédier des comptes d'accès et des comptes d'administration aux administrateurs tiers	52
<b>R65+</b>	Dédier un annuaire aux comptes d'accès des administrateurs tiers	52
<b>R66</b>	Activer à la demande les comptes des administrateurs tiers	53
<b>R67</b>	Renforcer l'authentification des administrateurs tiers	53
<b>R68</b>	Mettre en œuvre un rebond éphémère en coupure de la terminaison VPN et du SI administré	53
<b>R69</b>	Mettre en œuvre un contrôle d'accès strict et une traçabilité pour les administrateurs tiers	53
<b>R70</b>	Utiliser un boîtier matériel d'acquisition vidéo pour l'assistance à distance	55
<b>R71</b>	Mettre en œuvre une solution logicielle dédiée pour l'assistance à distance	56

# Annexe A

## Évolutions du guide

### A.1 Nouvelles recommandations

Les recommandations suivantes font leur apparition dans la version 2.0 du guide :

R2, R3, R4, R8, R27, R34, R40, R45, R50, R53, R56.

Les recommandations suivantes font leur apparition dans la version 3.0 du guide :

R59, R60, R61, R62, R63, R63-, R64, R65+, R66, R67, R68, R69, R70, R71.

### A.2 Mises à jour entre les versions 2.0 et 3.0

Outre l'ajout du nouveau chapitre 12 et des modifications de forme notamment sur les figures, le guide a fait l'objet de mises à jour mineures de fond entre les versions 2.0 et 3.0 :

- section 3.4 : précision sur la virtualisation des équipements de sécurité qui n'est pas à privilégier, avec renvoi vers le guide [19] pour la justification technique ;
- section 4.2.2 : CLIP OS est cité comme exemple de système multi-niveaux ;
- section 4.2.3 : complément sur l'utilisation des fonctions avancées de copier/coller dans l'architecture de la recommandation R9-- ;
- section 6.3 : reformulation de la recommandation R25 pour inciter à une étude préalable des besoins de rupture protocolaire ;
- section 7.1 : précision sur les annuaires des comptes d'administration (recommandation R28) et sur les journaux à activer (recommandation R31) ;
- section 7.2 : le jeton FIDO est cité comme exemple de second facteur d'authentification, reformulation de la recommandation R38 et du paragraphe la précédant ;
- section 9.1 : dans la recommandation R45, la sauvegarde hors ligne des éléments critiques devient plus prescriptive.
- section 11.2 : ajout d'une bulle d'information pour évoquer la possibilité de déployer un serveur *pastebin* en complément d'un serveur de fichiers pour les échanges sécurisés entre SI bureau-tique et SI d'administration ;
- section 13.6 : nouvelle section pour l'administration de ressources dans un *cloud* public, en cohérence avec le référentiel d'exigences PAMS ;
- annexe A : refonte.

## A.3 Matrice de rétrocompatibilité depuis la version 1.0 vers les versions ultérieures

Afin de permettre aux lecteurs ayant déjà travaillé sur la base de la première version du guide [24], dénommée v1.0 dans la suite du texte, il est proposé une matrice de rétrocompatibilité permettant de trouver les ajouts, suppressions ou équivalences de recommandations.



### Attention

Cette matrice est un outil pour faciliter la lecture mais n'a pas vocation à établir une équivalence stricte entre les différentes versions du guide. La lecture détaillée des recommandations actualisées est fortement conseillée.

Référence v1.0	Référence actuelle	Référence v1.0	Référence actuelle
R1	R1	R33	suppression
R2	R5	R34	R39
R3	R7	R35	R41
R4	R9	R36, R37	R32
R4 -	R9-	R38	R33
R4 --	R9--	R39	R36
R5	R15 et R16	R40, R41	R37
R5 -	R15-	R42	R38
R5 - (bis)	R21	R43, R44	suppression
R6, R7	R10	R45	R25
R8, R9	R12	R46, R47	R26
R10	R11	R48, R49	suppression
R11	R13	R50, R51	R49
R12	R14	R52	R6
R13	R6	R53	R51
R14	R48	R54	R10, R11, R12, R13, R14
R15	R35	R55, R56	R52
R16, R17	R29	R57	R54
R18	R30	R58	R55
R19	R31	R59	R57
R20	R22	R60	R58
R21, R22	R23	R61	suppression
R23	R24	R62	suppression
R24	R24-	R63	R42
R25	R6	R64, R65	R43
R26, R27, R28	R18 ou R18-	R66	R44
R29	R19	R67	suppression
R30	R20	R68	R46
R31, R32	R28	R69	R47
R32 -	suppression	R70-R73	suppression

# Annexe B

## Aspects juridiques

La sécurité des systèmes d'information passe par des mesures techniques mais également fonctionnelles qui intègrent des obligations pesant sur l'entité. L'administrateur est devenu un acteur clé de la sécurité des systèmes d'information sur lequel pèsent des responsabilités accrues. Ces recommandations n'ont pas vocation à être exhaustives et nécessitent de consulter un conseil juridique spécialisé pour plus de détails.

Tout d'abord, l'administrateur est tenu à des obligations de :

- **loyauté** : l'administrateur étant investi de larges pouvoirs de surveillance sur les données qui circulent sur les systèmes d'information de l'entreprise, le respect de règles d'éthique est attendu de sa part. Compte tenu de la « dépendance » de l'entreprise à l'égard de ce type de fonctions, la jurisprudence a tendance à se montrer plus sévère en cas de non-respect par l'administrateur de ses obligations. Des sanctions pénales peuvent être prononcées à son encontre<sup>12</sup>, tout comme la faute grave peut être retenue dans le cadre d'une procédure de licenciement<sup>13</sup> ;
- **transparence** : l'administrateur doit exercer ses missions dans le cadre du règlement intérieur et de la charte informatique édictés par l'entreprise. La charte informatique est un véritable outil de sensibilisation des salariés qui leur est opposable dès lors qu'elle est annexée au règlement intérieur. Son non-respect s'analysera en une violation du contrat de travail pouvant donner lieu à des sanctions disciplinaires, y compris un licenciement. A contrario, tolérer des agissements pourtant contraires à ce qui est prévu par la charte informatique conduira à l'absence de sanction<sup>14</sup> ;
- **confidentialité** : l'administrateur est tenu à une obligation particulière de confidentialité<sup>15</sup>, tenant notamment au secret professionnel. Il ne doit pas divulguer les informations auxquelles il aurait pu avoir accès lors de l'exercice de ses fonctions, a fortiori lorsqu'elles sont couvertes par le droit à la vie privée ou le secret des correspondances, à moins qu'une disposition législative ne l'impose (ex. en cas de découverte de contenus illicites).

Par ailleurs, l'entité doit prendre les mesures nécessaires afin de protéger certaines données contenues dans son système d'information, se traduisant, en cas de défaillance, par la mise en jeu de sa responsabilité civile et/ou pénale.

L'obligation de sécurité des données s'applique, notamment, au travers de l'article 34 de la loi Informatique et Libertés et de l'article 32 du règlement général sur la protection des données<sup>16</sup> (RGPD).

12. Condamnation pour accès et maintien frauduleux à un système de traitement automatisé de données, atteinte au secret des correspondances émises par voie électronique : TGI Annecy, 4 décembre 2015, Tefal et autres.

13. CA Paris, 4 octobre 2007, n° 06/02095, Association ARFP pour le téléchargement de fichiers contrefaits ; CA Paris, 29 octobre 2008, n° 06/14072, JurisData n° 2008-373540 ou CA Paris 10 avril 2014, n° 11/04388, JurisData n° 201-007648, consultation d'informations personnelles relatives aux dirigeants et collègues et téléchargement de musique, consultation de sites pornographiques.

14. Cass. Soc. 10 mai 2012, n° 11-11060 ; CA Metz, 24 février 2014, n° 14/00120.

15. Cass. Soc., 17 juin 2009, n° 08.40274.

16. Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), applicable à partir du 25 mai 2018.

À ce titre, la CNIL se montre de plus en plus sévère en cas de défaut de sécurisation donnant lieu à une violation de données à caractère personnel<sup>17</sup>. Le code pénal sanctionne, d'ailleurs, le non-respect de ces dispositions<sup>18</sup>.

D'autres réglementations, sectorielles le cas échéant, peuvent trouver à s'appliquer. À titre d'exemple, l'arrêté du 3 novembre 2014<sup>19</sup> en matière bancaire, plus particulièrement ses articles 88 et suivants, oblige les banques à veiller « *au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés* » en prévoyant des audits réguliers, des procédures de secours ainsi que des mesures permettant de préserver en toutes circonstances l'intégrité et la confidentialité des informations ou encore le Code de la santé publique qui prescrit l'agrément des hébergeurs de données de santé ainsi que le respect de mesures de sécurité des systèmes d'information de nature à préserver le secret médical<sup>20</sup>. Le rôle de l'administrateur dépendra directement de l'environnement réglementaire dans lequel il exerce ses fonctions.

La jurisprudence a, en outre, tendance à attendre de l'entité qu'elle prenne la mesure de la nécessité de protéger son système d'information, sous peine de considérer qu'elle a contribué à son propre dommage<sup>21</sup>.

La réglementation européenne est de plus en plus exigeante pour la sécurisation des données des entreprises et administrations en imposant, selon les cas, une obligation de notification des failles de sécurité et/ou de mise en place de mesures techniques et organisationnelles de gestion des risques menaçant la sécurité des réseaux et de l'information sous leur responsabilité<sup>22</sup>. Par ailleurs, le règlement général sur la protection des données, entrant en application en mai 2018, renforce les conséquences du défaut de sécurisation en augmentant le montant des sanctions pécuniaires pouvant être prononcées par la CNIL<sup>23</sup>.



### Attention

Par son action, l'administrateur contribue à assurer la sécurité du système d'information, obligation prescrite par de nombreux textes législatifs et réglementaires. Le non-respect de cette obligation peut engager la responsabilité civile et/ou pénale de l'entité.

À noter que l'administration sécurisée d'un système d'information passera également par la sécurisation des contrats dont l'entité est titulaire (contrats de travail, achat de matériel *software* ou

17. Délibération de la formation restreinte n° 2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société Orange : « *Si la société a remédié dans des délais satisfaisants aux faiblesses techniques relevées et a démontré pour l'avenir une meilleure prise en compte des problématiques de confidentialité des données, il n'en demeure pas moins qu'elle a manqué à son obligation d'assurer la sécurité et la confidentialité des données à caractère personnel de ses clients.* » ; Délibération de la formation restreinte n° 2015-379 du 5 novembre 2015 prononçant une sanction pécuniaire de 50 000 € à l'encontre de la société Optical Center pour défaut de sécurisation de sa base de données clients : « *la formation restreinte relève que le manquement relatif à la sécurisation du site était caractérisé au jour de l'expiration du délai de mise en conformité imparti et persistait au jour du second contrôle. Le fait que le protocole HTTPS est dorénavant en place sur l'ensemble du site est sans incidence sur la caractérisation de ce manquement.* »

18. Art. 226-17 du code pénal : cinq ans d'emprisonnement et 300 000 euros d'amende et art. 131-38 du code pénal : 1 500 000 euros pour les personnes morales ainsi que des peines complémentaires.

19. Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.

20. Art. L. 1111-8 du Code de la santé publique.

21. CA Paris 4 mai 2007, Normaction c/ KBC Lease France, DMS, JurisData n° 2007-334142 ; TGI Paris, 21 février 2013, Sarenza c/ Jonathan et autres.

22. Directive (UE) n° 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS).

23. Les sanctions prononcées par les autorités de contrôle pourront s'élever désormais jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires, le montant le plus élevé des deux étant retenu, règlement général sur la protection des données, art. 83. Précédemment, le montant maximal des sanctions pouvant être prononcées par la CNIL était de 150 000 euros.

*hardware*, prestations d'hébergement ou de sauvegarde, etc.). Des clauses essentielles à la bonne exécution des contrats sont à prévoir, telles que, notamment, les clauses de confidentialité, de sécurité, d'audit, de responsabilité incluant le cas échéant des pénalités, de continuité d'activité ou encore de réversibilité. Le risque est d'autant plus grand que le prestataire choisi peut être soumis, parfois, au respect de législations pouvant être considérées comme intrusives du point de vue de la sensibilité des données de l'entité. L'assistance d'un conseil juridique spécialisé en la matière sera un atout lors de la négociation de celles-ci.



### Attention

La sécurisation du système d'information doit être prévue aussi dans le cadre de clauses adaptées dans les contrats conclus par l'entité pour le fonctionnement de son système d'information. Ces clauses, selon le type de contrat concerné, peuvent pour partie avoir un impact sur l'étendue des pouvoirs de l'administrateur.

Enfin, la formation et la sensibilisation des collaborateurs à la nécessité de protéger le système d'information de l'entité ne doivent pas être négligées. En effet, certains comportements, pouvant pourtant donner lieu à sanctions (disciplinaires voire pénales), ne révèlent pas nécessairement d'intention de nuire mais uniquement une méconnaissance des conséquences potentiellement dommageables pour l'entité.

L'administrateur, en concertation avec le délégué à la protection des données<sup>24</sup> le cas échéant, doit avoir une action essentielle en matière de sensibilisation. Celle-ci est une des mesures fonctionnelles à prévoir pour la sécurisation du système d'information.

Il reviendra à l'administrateur de surveiller l'utilisation des ressources du système d'information pour palier l'éventualité d'un incident.

---

24. Prévu aux articles 37 et suivants du règlement général sur la protection des données.



# Annexe C

## Glossaire

À défaut de s'appuyer sur des définitions standardisées et dans un souci de clarté, le glossaire ci-dessous définit les termes spécifiques à ce guide :

**Actions d'administration** : ensemble des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système participant au SI et susceptibles de modifier son fonctionnement ou d'altérer la sécurité du SI ;

**Administrateur** : personne physique disposant de droits privilégiés sur un système d'information, chargée des actions d'administration sur celui-ci, responsable d'un ou plusieurs domaines techniques ;

**Administrateur métier, exploitant** : personne physique ayant le rôle d'administrateur, en charge de l'exploitation ou de l'emploi d'un service ou d'une ressource d'administration en particulier ; il ou elle dispose de privilèges adaptés à ses fonctions ;

**Administration à distance** : désigne l'administration d'un système d'information en dehors d'un périmètre de protection physique sous maîtrise directe ou indirecte de l'entité ; ceci inclut l'administration en situation de nomadisme ;

**Authentifiants d'administration** : combinaison d'un identifiant et d'un ou plusieurs facteurs d'authentification (information connue, possédée, qui peut être montrée ou réalisée par l'administrateur) associés à un compte d'administration ;

**Compte d'administration** : compte disposant de privilèges nécessaires aux actions d'administration ; il peut être générique, individuel ou de service ;

**Connexion à distance** : depuis un poste de travail, la connexion à distance consiste à se connecter sur un autre environnement (physique ou virtuel) afin d'y ouvrir une session graphique (ex. : RDP<sup>25</sup>, ICA<sup>26</sup>) ou console (ex. : SSH ou PowerShell<sup>27</sup>) ;

**DMZ (*Demilitarized zone*)** : zone intermédiaire séparant deux zones de confiance hétérogène notamment grâce à des pare-feux réalisant un filtrage périmétrique de part et d'autre ;

**Flux d'administration** : flux de communication, direct ou indirect, vers une ressource administrée pour la réalisation d'une action d'administration ;

**Interface d'administration** : point d'entrée réseau, logique ou physique, sur une ressource administrée ;

**Outils d'administration** : outils techniques (consoles, utilitaires, etc.) utilisés pour accéder aux ressources administrées au travers des interfaces d'administration afin d'effectuer les actions d'administration ;

---

25. RDP (*Remote Desktop Protocol*) : protocole d'accès à distance proposé par les solutions Microsoft.

26. ICA (*Independent Computing Architecture*) : protocole d'accès à distance proposé par les solutions Citrix.

27. *Windows PowerShell* : suite logicielle incluant un interpréteur de commandes associé au langage du même nom pour l'administration automatisée des systèmes Windows.



**Poste d'administration** : terminal matériel, fixe ou portable, utilisé pour les actions d'administration ;

**Réseau d'administration** : réseau de communication faisant transiter les flux internes au SI d'administration et les flux d'administration ;

**Ressources administrées** : ensemble des dispositifs physiques ou virtuels du SI administré qui nécessitent des actions d'administration ;

**Ressources d'administration** : ensemble des dispositifs physiques ou virtuels du SI d'administration : poste d'administration, serveurs d'infrastructures d'administration, serveurs outils d'administration, équipements de réseau d'administration, etc. ;

**SI d'administration** : système d'information utilisé pour administrer des ressources qui sont présentes dans un autre SI dit SI administré, distinct du SI d'administration ;

**Zone d'administration** : sous-ensemble du SI d'administration dont l'objectif est d'isoler ou cloisonner des ressources d'administration par des mesures de protection adaptées au contexte et en fonction du juste besoin opérationnel ;

**Zone de confiance** : ensemble de ressources informatiques regroupées en fonction de l'homogénéité de facteurs divers, liés ou non à la sécurité (ex. : exposition aux menaces, vulnérabilités résiduelles technologiques intrinsèques, localisation géographique, etc.).

# Bibliographie

- [1] *Guide pour les employeurs et les salariés.*  
Guide, CNIL, 2010.  
<https://www.cnil.fr>.
- [2] *Supply chain attacks. Menaces sur les prestataires de service et les bureaux d'études.*  
Rapport CERTFR-2019-CTI-004, ANSSI, octobre 2019.  
<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-004.pdf>.
- [3] *Instruction générale interministérielle n°1300.*  
Référentiel, SGDSN, novembre 2020.  
<https://www.ssi.gouv.fr/igi1300>.
- [4] *Points de contrôle Active Directory.*  
Page Web CERTFR-2020-DUR-001, ANSSI, juin 2020.  
<https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001>.
- [5] *Recommandations de sécurité relatives à un système GNU/Linux.*  
Note technique DAT-NT-002/ANSSI/SDE/NP v1.1, ANSSI, juillet 2012.  
<https://www.ssi.gouv.fr/reco-securite-systeme-linux>.
- [6] *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>.
- [7] *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>.
- [8] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation.*  
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.  
<https://www.ssi.gouv.fr/windows10-vsm>.
- [9] *Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10.*  
Guide ANSSI-BP-036 v1.2, ANSSI, juillet 2017.  
<https://www.ssi.gouv.fr/windows10-collecte-donnees>.
- [10] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows.*  
Note technique DAT-NT-013/ANSSI/SDE/NP v2.0, ANSSI, janvier 2017.  
<https://www.ssi.gouv.fr/windows-restrictions-logicielles>.
- [11] *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>.
- [12] *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information.*  
Guide Version 1.0, ANSSI, décembre 2010.  
<https://www.ssi.gouv.fr/infogerance>.

- [13] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures.*  
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.  
<https://www.ssi.gouv.fr/hygiene-informatique>.
- [14] *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>.
- [15] *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>.
- [16] *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>.
- [17] *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu.*  
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.  
<https://www.ssi.gouv.fr/nettoyage-politique-fw>.
- [18] *La méthode EBIOS Risk Manager - Le Guide.*  
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.  
<https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide>.
- [19] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet.*  
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.  
<https://www.ssi.gouv.fr/guide-pare-feux-internet>.
- [20] *Recommandations de sécurité relatives à TLS.*  
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.  
<https://www.ssi.gouv.fr/nt-tls>.
- [21] *Recommandations relatives à l'interconnexion d'un système d'information à Internet.*  
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.  
<https://www.ssi.gouv.fr/passerelle-interconnexion>.
- [22] *Référentiel général de sécurité (RGS).*  
Référentiel Version 2.0, ANSSI, juin 2012.  
<https://www.ssi.gouv.fr/rgs>.
- [23] *Instruction interministérielle n°901.*  
Référentiel Version 1.0, ANSSI, janvier 2015.  
<https://www.ssi.gouv.fr/ii901>.
- [24] *Recommandations relatives à l'administration sécurisée des systèmes d'information.*  
Note technique DAT-NT-022/ANSSI/SDE/NP v1.0, ANSSI, février 2015.  
<https://www.ssi.gouv.fr/securisation-admin-si>.
- [25] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences.*  
Référentiel Version 2.0, ANSSI, décembre 2017.  
[https://www.ssi.gouv.fr/uploads/2014/12/pdis\\_referentiel\\_v2.0.pdf](https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf).

- [26] *Prestataires d'administration et de maintenance sécurisées. Référentiel d'exigences.*  
Référentiel Version 1.0, ANSSI, avril 2020.  
<https://www.ssi.gouv.fr/uploads/2020/09/anssi-pams-referentiel-v1.0.pdf>.
- [27] *Qualification.*  
Page Web Version 1.0, ANSSI, mars 2016.  
<https://www.ssi.gouv.fr/visa-de-securite/qualification>.
- [28] *Licence ouverte / Open Licence v2.0.*  
Page web, Mission Etalab, 2017.  
<https://www.etalab.gouv.fr/licence-ouverte-open-licence>.



ANSSI-PA-022

Version 3.0 - 11/05/2021

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

## AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

[www.ssi.gouv.fr](http://www.ssi.gouv.fr) / [conseil.technique@ssi.gouv.fr](mailto:conseil.technique@ssi.gouv.fr)

