



P R E M I E R   M I N I S T R E

Secrétariat général  
de la défense  
et de la sécurité nationale

*Agence nationale de la sécurité  
des systèmes d'information*

Paris, le 20 février 2015

N° DAT-NT-22/ANSSI/SDE/NP

Nombre de pages du document  
(y compris cette page) : 41

## NOTE TECHNIQUE

---

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



### Public visé:

Développeur	<input type="checkbox"/>
Administrateur	<input checked="" type="checkbox"/>
RSSI	<input checked="" type="checkbox"/>
DSI	<input checked="" type="checkbox"/>
Utilisateur	<input type="checkbox"/>

# INFORMATIONS

---

## Avertissement

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. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab ([www.etalab.gouv.fr](http://www.etalab.gouv.fr)). Il est par conséquent diffusable sans restriction.

Ces recommandations 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.

## Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BSS, BAS, BAI, LAM, LRP, MRR	BAS	SDE	20 février 2015

## Évolutions du document :

Version	Date	Nature des modifications
1.0	20 février 2015	Version initiale.

## Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

## Table des matières

1	Préambule	3
2	Rôle de l'administrateur	4
3	Généralités	5
3.1	Objectifs de sécurité	5
3.2	Domaines fonctionnels et techniques	6
3.3	Zones de confiance	7
3.4	La confiance dans les technologies de virtualisation	8
4	Sécurité du poste d'administration et de l'accès aux ressources administrées	8
4.1	Poste et réseau d'administration	8
4.2	Sécurisation du socle	13
4.3	Comptes d'administration	14
5	Outils d'administration	16
6	Ressources administrées	18
7	Annuaire	19
7.1	Annuaire	19
7.2	Authentification	21
8	Passerelle d'administration	22
8.1	Architecture type	23
8.2	Nomadisme et accès distants	25
9	Système d'échange	27
10	Maintien en condition de sécurité	31
10.1	Mises à jour de sécurité des zones d'administration	31
10.2	Supervision de la sécurité	32
	Annexes	35

# 1 Préambule

---

Les tâches d'administration sont une composante indissociable du cycle de vie du système d'information. Elles se traduisent par un ensemble de processus et de mesures techniques et non techniques visant à assurer le maintien en condition opérationnelle et de sécurité du système.

Dans le cadre de ses missions, l'agence nationale de la sécurité des systèmes d'information (ANSSI) souhaite décrire dans ce guide technique les objectifs de sécurité et les principes d'architecture permettant l'élaboration d'une architecture technique d'administration. Ce document n'a pas vocation à être exhaustif ou à couvrir l'ensemble des cas d'usage. Il propose des éléments utiles d'aide à la conception d'architectures sécurisées tout en mettant à la disposition des administrateurs les moyens techniques et organisationnels nécessaires à la réalisation de leurs missions. Ces éléments sont à replacer dans le contexte du système d'information traité autant que de besoin.

Ce guide s'adresse à un large public. Il suppose cependant que le lecteur dispose de connaissances minimales pour appréhender les recommandations de sécurité présentées et les adapter à son contexte.

Des problématiques d'architecture et de cas d'usage (systèmes d'information de type « bureau-tique », centres d'hébergement ou « datacenter ») sont abordés dans la suite du document. Notamment, une attention particulière est portée aux besoins de nomadisme des équipes techniques, dans le cadre des contraintes à distance, et sur la tierce maintenance applicative ou infogérance. En revanche, ce document ne traite pas des besoins *métier* du système d'information tel que l'accès aux services par les utilisateurs (*front office*), ni des interconnexions concourant au fonctionnement de ces services (systèmes décisionnels, systèmes de gestion, etc.).

La responsabilité de la mise en œuvre des recommandations proposées dans ce document incombe au lecteur. Outre la nécessité de s'approprier les principes décrits et de les adapter à son contexte et à ses besoins, il devra s'appuyer sur la politique de sécurité du système d'information existante et sur les résultats d'une analyse de risques<sup>1</sup> pour déterminer les recommandations les plus pertinentes dans son contexte.

Enfin, pour un même domaine technique, plusieurs solutions d'architecture sont proposées dans le document. Ces solutions se distinguent par leur niveau de sécurité. Elles doivent permettre au lecteur, dont le niveau de maturité du SI en termes de sécurité est faible, de définir une cible d'architecture offrant la meilleure protection et de déterminer les différentes étapes nécessaires pour atteindre cette cible. Ainsi, les recommandations seront présentées de la manière suivante :

Rx	La recommandation permet de mettre en place l'architecture cible offrant un niveau de sécurité optimal.
Rx -	Cette mesure propose un premier niveau dérogatoire à la recommandation précédente. Le niveau de confiance est plus faible que Rx.
Rx --	Cette dernière dérogation implique un niveau de sécurité plus faible que Rx -. Le niveau de confiance est donc plus faible.

TABLE 1 – Priorisation des recommandations

Quand plusieurs recommandations portent la même numérotation et le même niveau de sécurité (par exemple, plusieurs R3 --), celles-ci sont cumulatives et doivent toutes être appliquées.

---

1. La méthode EBIOS élaborée par l'ANSSI permet de mener des analyses de risques : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html>.

## 2 Rôle de l'administrateur

---

L'administrateur est un acteur essentiel pour la préservation de la sécurité d'un système d'information. Son action s'inscrit dans un contexte réglementaire dense qui impose à l'entité dont il dépend le respect d'une obligation de sécuriser son système d'information. Les mesures fonctionnelles et techniques nécessaires de sécurisation impliquent d'être réfléchies en amont afin de donner à l'administrateur les moyens de son action. Elles devront être connues de tous les salariés. En effet, les droits et obligations des salariés, dont fait partie l'administrateur, en matière d'utilisation des moyens informatiques doivent être consignés dans une charte informatique annexée au règlement intérieur. L'administrateur prendra directement appui sur ce document pour exercer ses fonctions. L'entreprise peut prévoir, le cas échéant, une charte informatique spécifique applicable aux administrateurs.

Les fonctions d'administrateur, complexes, doivent s'articuler entre des pouvoirs importants et le respect d'obligations précises.

L'administrateur d'un système d'information est tenu à des obligations particulières de loyauté, de transparence et de confidentialité<sup>2</sup> :

- 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>3</sup>, tout comme la faute grave peut être retenue dans le cadre d'une procédure de licenciement<sup>4</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>5</sup> ;
- Confidentialité : l'administrateur est tenu à une obligation particulière de confidentialité, 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).

<b>R1</b>	L'administrateur doit être informé de ses droits et devoirs, notamment en s'appuyant sur la charte informatique annexée au règlement intérieur de l'entité. Le cas échéant, une charte informatique spécifique applicable aux administrateurs pourra être élaborée.
-----------	---

---

2. Le guide pour les employeurs et les salariés élaboré par la CNIL est disponible à l'adresse suivante : [http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/Guide\\_employeurs\\_salaries.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_employeurs_salaries.pdf).

3. TGI rennes, 21 février 2008, n° 0352216, P.

4. 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.

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

L'[annexe II](#) aborde plus en profondeur les aspects juridiques liés aux rôles de l'administrateur d'un système d'information.

## 3 Généralités

---

### 3.1 Objectifs de sécurité

Les ressources informatiques contribuant à l'administration des systèmes d'information sont des cibles privilégiées pour un attaquant. En effet, les droits élevés nécessaires à la réalisation des missions d'administration et les larges accès dont les différents équipements et les administrateurs bénéficient exposent ces ressources à de nombreux risques et menaces. Dans de nombreux cas de compromission ou d'intrusion sur ces équipements, l'attaquant prend aisément le contrôle de l'ensemble du système d'information et accéder aux informations *métier* ou *techniques* traitées par celui-ci.

Cette note n'a pas vocation à établir une analyse exhaustive des risques. Ce travail, 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). Toutefois, les recommandations abordées au travers de ce document visent à couvrir les *objectifs de sécurité* suivants et ainsi réduire la surface d'exposition aux attaques informatiques :

- protéger les ressources et les infrastructures des intrusions et compromissions pour lesquelles les infrastructures d'administration seraient un vecteur d'attaque ;
- protéger les moyens et les ressources d'administration de toute tentative de compromission.

Pour couvrir ces objectifs de sécurité, ce document propose un certain nombre de mesures de sécurité à mettre en œuvre. Ces mesures visent à réduire les risques de compromission des ressources d'administration au vu des scénarios de menaces les plus couramment mis en œuvre par des attaquants. Parmi ces scénarios, le plus usité consiste à exécuter un code malveillant sur le poste d'administration ou sur un poste sur lequel un administrateur s'est connecté avec ses privilèges. Ce code malveillant peut être introduit par exemple par le biais d'une navigation Internet, par l'ouverture d'une pièce jointe dans un courriel piégé ou à partir d'un media amovible.

Le code malveillant profite des privilèges élevés de la session de l'administrateur pour exécuter des actions telles que :

- le vol des empreintes de mots de passe sur le poste, par exemple par une copie mémoire (exemple : *Pass The Hash*). Cette technique permet la réutilisation de cette empreinte administrateur 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 (cheval de troie, enregistreur de frappes clavier - *Keylogger*, etc.) ;
- l'accès à un serveur de commande et de contrôle ;
- la diffusion d'un ver ;
- etc.

### 3.2 Domaines fonctionnels et techniques

Tout en respectant les principes de défense en profondeur et de moindre privilège, il est impératif de définir, au plus tôt, l'ensemble des domaines fonctionnels du système d'information étudié, puis les domaines techniques qui en découlent. Ces travaux contribueront ainsi à définir les zones de confiance à prévoir dans l'architecture et les mécanismes techniques de cloisonnement associés. *In fine*, cette pratique permet de réduire la surface d'exposition aux attaques informatiques et les impacts en cas de compromission.

Parmi les domaines fonctionnels et techniques, on peut citer :

1. les domaines fonctionnels composant le système d'information, tels que :
  - le système bureautique ;
  - le centre d'hébergement (ou datacenter) ;
  - le réseau ;
  - les passerelles nomades ;
  - les passerelles de tierce maintenance applicative (TMA) ;
  - les passerelles d'accès Internet utilisateur ;
  - etc.
2. les domaines techniques d'administration qui en découlent, tels que :
  - les bases de données ;
  - les équipements réseau ;
  - les systèmes d'exploitation ;
  - les hyperviseurs (virtualisation) ;
  - les équipements de sécurité (pare-feux, sondes, etc.) ;
  - les messageries ;
  - les applications Web ;
  - etc.

La figure ci-dessous propose une vue graphique de ces domaines :

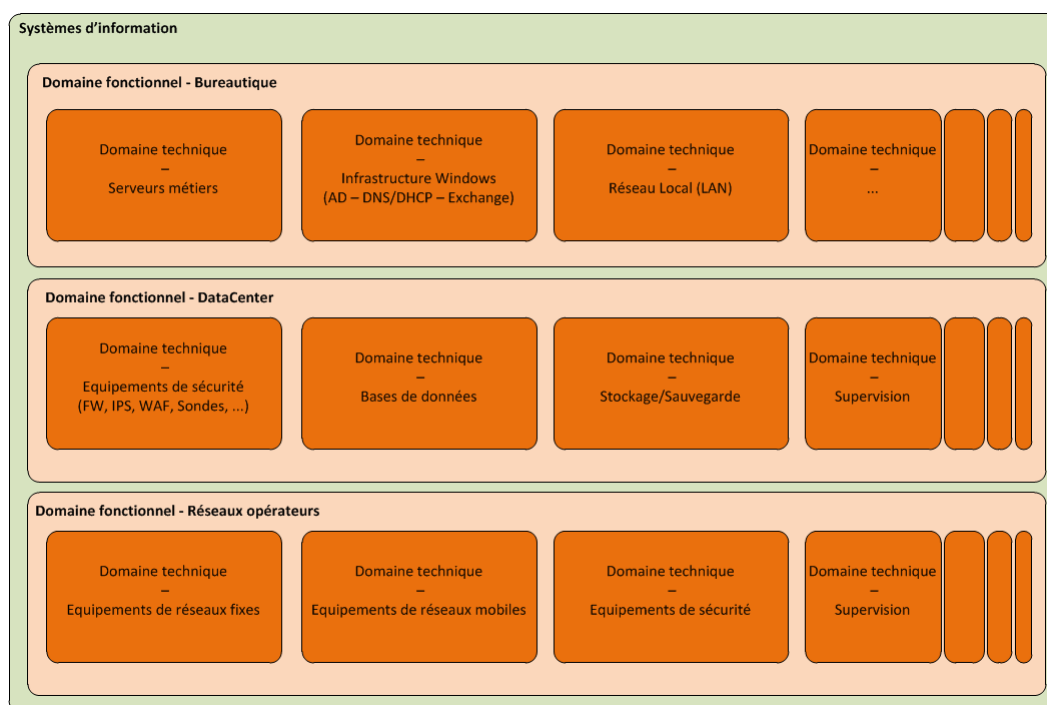


FIGURE 1 – Représentation de domaines fonctionnels et techniques types

**R2** Avant toute étude d'architecture, il est impératif de définir les domaines fonctionnels du système d'information concerné puis les domaines techniques qui en découlent.

Cette étude doit être menée aussi bien en phase de conception qu'avant toute évolution du système d'information. Elle permet d'alimenter les travaux d'architecture afin que soit traité l'ensemble des besoins d'administration. Pour assurer une cohérence d'ensemble, ces domaines doivent être mis au regard de l'organisation des équipes d'administration concernées et des outils d'administration que chacune d'entre elles utilise. Cette réflexion doit être menée par l'organisme, avec l'ensemble des parties prenantes.

### 3.3 Zones de confiance

Comme décrit précédemment, un système d'information se compose usuellement de différents composants techniques. Afin de maîtriser les accès à ces composants et d'assurer leur cloisonnement, ces derniers doivent être regroupés dans des zones de confiance. L'objectif de ces zones est d'isoler ou cloisonner un système, des ressources ou un service par des mesures de protection adaptées et en fonction du juste besoin opérationnel. Elles peuvent se traduire par exemple par des mécanismes de filtrage, de cloisonnement logique de réseau, de chiffrement, d'authentification. La mise en œuvre simultanée de plusieurs de ces mécanismes est nécessaire pour obtenir un niveau de confiance satisfaisant.

Afin de définir ces zones de confiance le plus justement possible, il est nécessaire au préalable de mener une analyse des domaines fonctionnels et techniques à traiter et de définir les besoins de sécurité notamment en termes de confidentialité, d'intégrité, d'authentification et de traçabilité.



### 3.4 La confiance dans les technologies de virtualisation

L'emploi des technologies de virtualisation est de plus en plus 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 une même machine physique. Ces mécanismes ont pour objectif de garantir une étanchéité équivalente à celle d'environnements physiquement distincts. Leur complexité rend difficile l'évaluation de ce niveau de confiance.

Dans l'absolu, l'emploi de solutions *qualifiées* par l'ANSSI peut apporter certaines garanties. Ce processus de qualification permet en effet de s'assurer que les produits répondent aux objectifs définis dans des cibles de sécurité préalablement approuvées. En pratique, ce processus est difficilement applicable aux technologies de virtualisation au vu de la complexité de la maîtrise de la conception et des développements.

En conséquence, en l'absence de telles garanties, le principe de précaution doit prévaloir. Les solutions de virtualisation doivent être utilisées uniquement pour faire cohabiter sur un même support physique des domaines fonctionnels ou techniques, ou des zones de confiance, homogènes d'un point de vue des besoins de sécurité : des composants traitant des données nécessitant le même niveau de protection en termes de confidentialité, d'intégrité ou de disponibilité. Ce principe s'applique notamment pour les équipements de virtualisation réseau (routeurs ou commutateurs virtuels), de filtrage (pare-feux virtuels) et d'hébergement (hyperviseurs).

Le cas présent, les activités d'administration relèvent d'un domaine fonctionnel particulier. Cela se justifie par le caractère spécifique des besoins de sécurité. Le principe de précaution consistera donc à dédier physiquement les équipements de virtualisation pour l'administration de façon à réduire les risques de compromission. Plus concrètement, et à titre d'exemple, les serveurs outils et les annuaires dédiés aux administrateurs peuvent être virtualisés mais devront être hébergés sur des machines physiques dédiées (par exemple : hyperviseurs dédiés), différentes de celles utilisées pour les applications métier. En second exemple et dans un autre domaine technique, le routage et le filtrage des flux des zones de confiance dédiées à l'administration ne devront pas non plus être mutualisés avec les équipements permettant l'accès aux services utilisateur.

<b>R3</b>	Par précaution, il est fortement recommandé de ne pas mutualiser les infrastructures d'administration avec d'autres infrastructures à l'aide d'équipements basés sur des technologies de virtualisation.
-----------	--

## 4 Sécurité du poste d'administration et de l'accès aux ressources administrées

### 4.1 Poste et réseau d'administration

Le poste de travail de l'administrateur est un composant critique par nature car il dispose entre autres d'accès importants et privilégiés. En outre, il traite 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 l'ensemble des informations métier. Il doit donc faire l'objet de toutes les attentions en termes de sécurité afin de restreindre au mieux les risques de compromission.

Plusieurs solutions sont envisageables. Certaines sont décrites plus en détails dans la suite du document en fonction des cas d'usage. La solution qui offre la meilleure garantie en termes de sécurité consiste à utiliser deux postes et réseaux physiquement séparés, respectivement pour les tâches

d'administration et pour les autres usages (par exemple : accès aux services bureautiques de l'entité).

<b>R4</b>	La principale mesure de sécurité consiste à dédié un poste de travail physique aux tâches d'administration. Ce poste doit être distinct du poste permettant d'accéder aux ressources bureautiques conventionnelles accessibles sur le système d'information de l'entité (ressources métier, messagerie interne, gestion documentaire, Internet, etc.).
-----------	--

La séparation physique des environnements de travail, en particulier ceux d'administration et de bureautique, implique de disposer d'au moins deux stations sur le plan de travail. Il est possible que, pour un certain nombre de raisons, l'application de ce principe soit délicate à mettre en œuvre à court terme.

Certaines solutions alternatives peuvent alors être envisagées. Il convient de conserver à l'esprit que ces solutions n'offrent pas le même niveau de sécurité qu'une séparation physique. Ainsi, il est primordial de bien identifier les risques associés à chaque solution, notamment ceux pouvant mener à une compromission, et de mesurer les impacts sur le système d'information avant leur mise en œuvre.

L'emploi des technologies de virtualisation pour obtenir un système « multi-niveaux » peut être considéré. Le principe consiste à disposer de plusieurs environnements logiciels sur un même poste physique. Des mécanismes de durcissement du noyau et de cloisonnement permettent d'isoler ces environnements (cf. figure 2) pour réduire les risques de compromission du niveau de sensibilité haute ou de fuite d'information depuis un niveau de sensibilité haute (ex : système d'administration) vers le niveau de sensibilité basse (ex : système bureautique).

Toutefois, comme indiqué précédemment, la confiance dans ces technologies réside essentiellement dans la robustesse des mécanismes d'isolement de ces environnements. **Il est ainsi préférable que ces mécanismes soient gérés au niveau du système, et non par une application utilisateur.** Néanmoins, s'ils comportent des faiblesses dans leur conception ou présentent des vulnérabilités, l'impact sera très préjudiciable car il concernera l'ensemble des ressources d'administration et plus globalement le système d'information. Par ailleurs, l'emploi de ces produits peut, s'ils ne sont pas de confiance, donner aux administrateurs un faux sentiment de sécurité. Dans l'absolu, l'emploi de technologies de type multi-niveaux, pour les postes d'administration, devrait donc faire l'objet au préalable d'un processus d'évaluation afin de s'assurer au minimum du bon niveau de sécurité des mécanismes d'isolement et de cloisonnement. Seul le suivi de ce type de processus permet de vérifier la confiance de ces solutions.

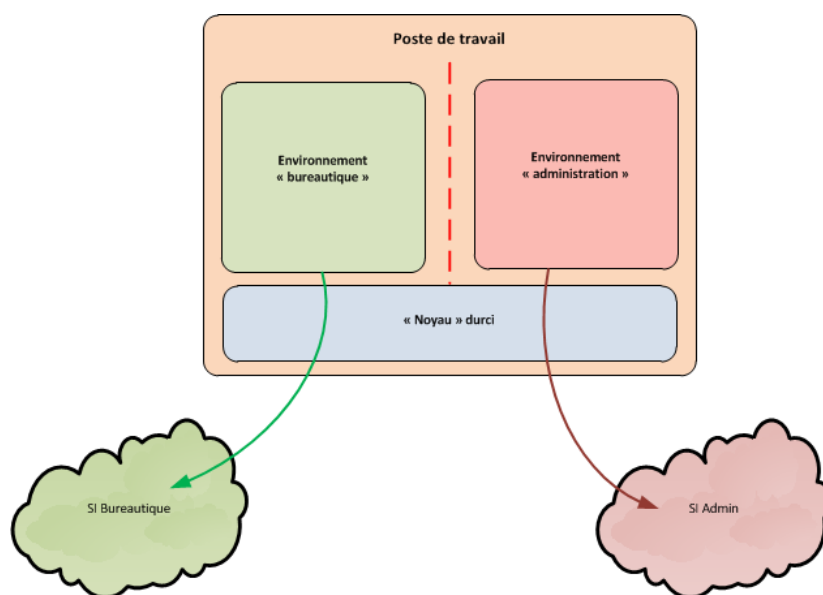


FIGURE 2 – *Système multi-niveaux*

<b>R4 -</b>	À défaut d'un poste d'administration physiquement dédié, l'emploi de technologies de virtualisation 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.
-------------	--

Une dernière solution consiste en l'emploi quotidien d'un poste d'administration physique et permettant un accès distant à un environnement bureautique par connexion à distance. **Il convient de noter que cette solution offre un niveau de sécurité beaucoup plus faible par rapport aux deux précédentes. Elle ne convient pas à l'administration des infrastructures critiques ou pour certains éléments critiques d'un système d'information (par exemple, en fonction des cas d'usage : hyperviseurs, annuaires Active Directory, etc.).** La surface d'attaque du système d'administration est en effet augmentée essentiellement par l'utilisation du logiciel client de connexion à distance directement exécuté sur le poste d'administration. Il existe donc un risque fort de compromission si le logiciel serveur de connexion à distance venait à être contrôlé par un attaquant. Cette pratique nécessite dans tous les cas une maîtrise plus forte de l'interconnexion entre les deux réseaux et des configurations sécurisées des postes.

**Remarque :** Il est à noter que la solution inverse, qui consiste à accéder depuis un poste bureautique vers un poste d'administration par connexion à distance, **est à proscrire**. En effet, les modalités d'interconnexion seraient alors contraires aux bonnes pratiques de sécurité qui imposent d'initier une connexion uniquement depuis une zone de confiance vers une zone de moindre confiance et non l'inverse.

Par ailleurs, 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...), dont les connexions initiées vers le poste d'administration : adresse IP, mots de passe, etc. Un attaquant pourrait alors rejouer ces connexions et, par rebond, accéder aux ressources d'administration puis au cœur du système d'information.

<b>R4 --</b>	<p>À défaut d'un poste d'administration physiquement distinct du poste bureautique ou d'un système de type multi-niveaux de confiance, une solution de contournement peut consister à ce que les administrateurs :</p> <ul style="list-style-type: none"> <li>– utilisent principalement leur poste d'administration physiquement dédié ;</li> <li>– accèdent, par connexion à distance uniquement, à leur environnement bureautique (physique ou virtuel - ex : Virtual Desktop Infrastructure) depuis le poste d'administration.</li> </ul> <p>Il est à noter que cette solution ne convient pas à l'administration d'infrastructures critiques ou à certains éléments critiques du système d'informations.</p>
--------------	---

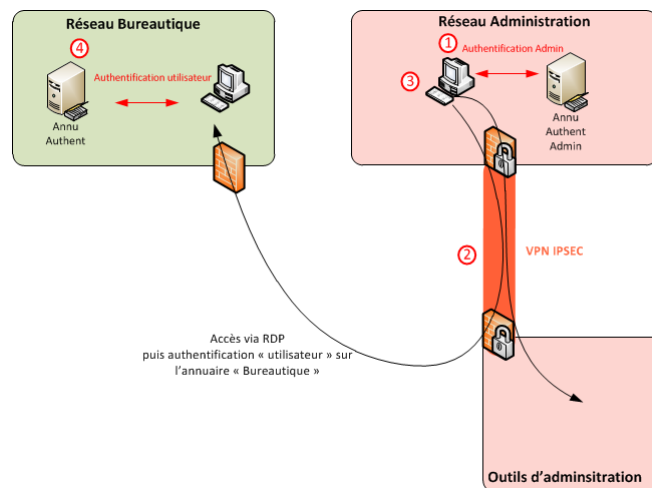


FIGURE 3 – Accès depuis un poste d'administration vers un poste bureautique par connexion à distance

- ① Authentification de l'administrateur sur son poste administrateur avec l'annuaire administrateur
- ② Accès en RDP via le tunnel VPN IPsec
- ③ Configuration du client RDP de façon à interdire les fonctions de :
  - copier/coller
  - prise en charge des périphériques (USB, imprimante, etc.)
  - partage réseaux
  - etc.
- ④ Authentification de l'administrateur sur son poste utilisateur avec l'annuaire bureautique

Dans ce dernier cas dérogatoire d'architecture, que le schéma ci-dessus représente, il est impératif que :

- les flux de connexion à distance transistent systématiquement par le VPN IPsec pour limiter le nombre d'interconnexions avec les zones d'administration ;
- le flux soit déchiffré par le concentrateur VPN de la zone d'administration ;
- un filtrage et un routage des flux de connexion à distance vers le réseau bureautique soient effectués par un pare-feu ;
- l'authentification sur le poste bureautique est réalisée sur l'annuaire « bureautique ».

De plus, l'utilisation d'un logiciel de connexion à distance depuis un poste d'administration vers un poste bureautique nécessite un certain nombre de précautions de configuration. Elles visent à restreindre les fonctions d'échange entre le système local (administrateur) et le système distant (bureautique). En effet, les mécanismes d'échange des logiciels de connexion à distance ne peuvent pas être, *a priori*, considérés comme étant de confiance.

<b>R4 --</b>	<p>Dans le cas de l'utilisation d'un logiciel de connexion à distance, certaines fonctions permettant un échange d'informations entre les deux systèmes doivent être désactivées. De manière non exhaustive, on peut citer :</p> <ul style="list-style-type: none"> <li>– les fonctions avancées de copier/coller ;</li> <li>– le partage d'écran ;</li> <li>– la fonction de prise en charge des périphériques (USB, imprimantes, etc.) ;</li> <li>– les partages réseaux.</li> </ul>
--------------	--

Les flux d'administration doivent être protégés au minimum en confidentialité et en intégrité. En conséquence, ils doivent notamment circuler sur des réseaux d'administration dédiés. A l'instar de la recommandation portant sur les postes d'administration, la mise en œuvre d'un réseau d'administration physiquement dédié contribue à répondre à ces objectifs et offre un niveau de sécurité optimal.

<b>R5</b>	Les postes d'administration doivent être déployés sur un réseau physiquement dédié à cet usage. Les interconnexions avec ce réseau doivent être maîtrisées et identifiées. Une matrice de flux doit être élaborée afin d'assurer la traçabilité et le suivi des règles de filtrage.
<b>R5 -</b>	À défaut d'un réseau physiquement distinct, il convient de protéger les flux d'administration en mettant simultanément en œuvre des mécanismes de cloisonnement logique, de filtrage, de chiffrement et d'authentification de réseau (IPsec), et d'authentification au réseau (par exemple : 802.1x, etc.).
<b>R5 -</b>	Si les flux d'administration doivent circuler à travers un autre système d'information qui servirait de réseau de transport, les flux d'administration doivent y être chiffrés et authentifiés de bout en bout jusqu'à atteindre un autre SI d'administration ou une ressource à administrer.

Les accès à Internet augmentent significativement les risques de compromission, mais aussi la surface d'exposition aux attaques informatiques. Ainsi, il est difficile de garantir l'intégrité des postes ayant accès à Internet d'autant que son utilisation courante permet un grand nombre de vecteurs d'attaque (navigation Web, courriel, ouvertures de fichiers ou exécution de programme téléchargés, etc.). Ces risques sont d'autant plus accrus pour un poste d'administration qui bénéficie de privilèges élevés et d'accès étendus sur le système d'information.

<b>R6</b>	Les postes d'administration ne doivent en aucun cas avoir accès à Internet. Cette recommandation est applicable en particulier aux accès Web et de messageries, même s'ils sont filtrés par des passerelles d'accès Internet.
-----------	---

Les accès à Internet doivent être réalisés uniquement à partir des postes bureautiques mis à disposition, eux mêmes soumis à un filtrage au travers des passerelles de l'entité.

<b>R7</b>	La consultation des boîtes mails fonctionnelles (par exemple, pour le service d'assistance aux utilisateurs) ne sera autorisée qu'à partir des stations de travail « bureautiques ».
-----------	--

Toutefois, pour des raisons opérationnelles telles que les mises à jour des correctifs techniques et de sécurité ou le téléchargement de certaines informations telles que des firmwares, il est possible d'étudier, au cas par cas, la mise en œuvre de « passerelles d'échanges » pour satisfaire chaque besoin. Ces infrastructures ne doivent en aucun cas dégrader le niveau de sécurité du dispositif d'administration. Elles doivent répondre aux mêmes objectifs et enjeux de sécurité que ceux édictés au paragraphe 3.1. Le chapitre 9 traite cette problématique.

## 4.2 Sécurisation du socle

Pour réduire les risques de compromission des postes d'administration, la maîtrise et le durcissement de leur configuration sont impératifs. Il convient de les protéger au mieux et d'assurer leur sécurité dans le temps. Ce paragraphe vise à décrire tous les points de configuration à mettre en œuvre et qui contribueront à atteindre cet objectif.

En premier lieu, il convient que les administrateurs ne puissent pas modifier la configuration de leur poste de travail. Plus simplement, ils ne doivent pas être intégrés au groupe local « administrateurs » du poste.

<b>R8</b>	Tous les administrateurs ne doivent pas disposer des droits d'administration sur leur poste de travail. Il conviendra d'attribuer ces droits uniquement aux administrateurs en charge de l'administration des postes.
-----------	---

En effet, tous les administrateurs n'ont pas ce besoin. La majeure partie des actions d'administration est réalisée à partir des navigateurs Web (portail d'administration Web), d'outils de type clients lourds ou en ligne de commande (ssh, ssh -X, ftps, etc.). L'utilisation de ces outils ne nécessite pas de droits ou de privilèges particuliers sur le poste de travail. Ces droits et privilèges doivent être strictement réservés aux administrateurs en charge des tâches d'administration même de ces postes et, par conséquent, des domaines fonctionnels et techniques (cf. le paragraphe 3.2) associés.

<b>R9</b>	Les droits d'administration des postes doivent être strictement réservés aux personnes en charge de leur configuration et uniquement utilisés pour des tâches qui s'y rapportent.
-----------	---

Des actions de configuration devront être menées pour la sécurité du système d'exploitation. Pour ce faire, il est recommandé de se référer en premier lieu 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.

<b>R10</b>	<p>Les guides de sécurisation des socles des éditeurs doivent être appliqués. Au minimum, les points d'attention sont :</p> <ul style="list-style-type: none"><li>– la désactivation des services inutiles ;</li><li>– l'application de droits restreints ;</li><li>– l'activation et la configuration du pare-feu local pour interdire toute connexion entrante, et limiter les flux sortants au juste besoin ;</li><li>– le durcissement des configurations systèmes (par exemple pour Windows GPO, Applocker, SRP, etc. ou, pour Linux grsec, PaX, etc.) ;</li><li>– l'activation de l'ensemble des mécanismes de mise à jour.</li></ul>
------------	---

De façon à restreindre de manière significative la surface d'exposition du système, il convient d'utiliser uniquement des logiciels ou exécutables préalablement validés et mis à disposition des administrateurs suivant un processus de contrôle défini. Ces vérifications sont cumulables et 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.

<b>R11</b>	Il convient de n'installer sur les postes que les logiciels et les outils utiles aux actions d'administration. Ils sont déployés en fonction du (des) domaine(s) fonctionnel(s) et technique(s) de chaque administrateur. Pour ce faire, il est recommandé : <ul style="list-style-type: none"> <li>– de dresser la liste des outils d'administration utiles ;</li> <li>– de mettre en œuvre un processus de validation et de distribution des outils d'administration suivant les critères techniques et non techniques décrits <i>supra</i>.</li> </ul>
------------	---

Afin de répondre aux contraintes de délais d'intervention nécessaires aux opérations de maintenance, 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 accessible uniquement sur le réseau d'administration, ou via un partage réseau dédié et restreint aux seules personnes ayant le besoin opérationnel.

Les postes d'administration contiennent des données sensibles utiles à l'accès au système d'information. La perte de ces informations est préjudiciable à la sécurité du système d'information. Les ordinateurs portables (cf. paragraphe 8.2) sont en particulier plus exposés aux risques de perte ou de vol. Ces incidents induisent une compromission des informations sensibles contenues sur les disques durs (fichiers, mots de passe, configurations, etc.).

<b>R12</b>	Il est recommandé de procéder au chiffrement complet de l'ensemble des périphériques de stockage (ex : disques durs, périphériques de stockage amovibles, etc.) utilisés pour les tâches d'administration.
------------	--

Les dispositifs de chiffrement utilisés doivent cependant garantir un certain niveau de robustesse et être adaptés à la sensibilité des données à protéger. Le processus de qualification défini par l'ANSSI permet de s'assurer que les produits répondent bien aux objectifs définis dans des cibles de sécurité préalablement approuvées par ses soins.

<b>R13</b>	Il convient d'utiliser des produits de chiffrement ayant été labellisés <sup>6</sup> par l'ANSSI.
------------	---

Enfin, dans le cadre d'un usage nomade, les postes d'administration peuvent faire l'objet d'indiscrétions. Suivant l'environnement dans lequel le poste d'administration est utilisé, les informations affichées à l'écran peuvent être lues à l'insu de l'administrateur. L'utilisation de filtres écran de confidentialité peut pallier ce problème.

<b>R14</b>	Les postes d'administration portables devront être dotés de filtres écran de confidentialité afin de ne pas faire l'objet d'indiscrétions.
------------	--

### 4.3 Comptes d'administration

Les identifiants et les secrets d'administration font partie des premières cibles lors d'une attaque informatique. Le vol de ces informations simplifie grandement la compromission d'un système d'information et la rend plus silencieuse. Ce risque est augmenté par le fait que les administrateurs doivent connaître et utiliser un grand nombre de secrets. L'accumulation de ces mots de passe et le respect des bonnes pratiques en la matière<sup>7</sup> (complexité, longueur, renouvellement, etc.) n'est pas chose aisée et s'avère souvent difficile à respecter dans le temps. Malgré la mise en œuvre d'annuaire d'authentification

6. La liste des produits qualifiés est accessible sur le site de l'ANSSI : <http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/>.

7. La note technique de recommandations relatives aux mots de passe est accessible sur le site de l'ANSSI : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html>.



centralisé, il se peut que le nombre de mots de passe résiduels reste important. Cela concerne essentiellement les équipements ou les logiciels incompatibles avec ces solutions d'authentification. Il convient donc de protéger ces informations de valeur comme il se doit. Pour éviter leur stockage en clair dans un fichier texte ou un tableur, l'utilisation d'un coffre-fort de mots de passe est fortement recommandé. La liste des produits labellisés assurant cette fonction (par exemple, Keepass2) est disponible sur le site de l'ANSSI.

<b>R15</b>	L'utilisation d'un coffre-fort de mots de passe labellisé est recommandé pour éviter de stocker en clair des mots de passe sur les postes d'administration.
------------	---

Le durcissement des mécanismes d'authentification et la protection des ressources associées (annuaire, comptes, mots de passe, etc.) doivent être aussi étudiés et mis en œuvre systématiquement par les administrateurs. Les problématiques relatives à l'identification, l'authentification et au contrôle d'accès sont traitées plus en détails au chapitre 7.

Une série de mesures concernant les comptes d'administration, et relevant des bonnes pratiques<sup>8</sup>, sont à mettre en œuvre par les administrateurs. Elles concernent le bon emploi des authentifiants d'administration (par exemple : mots de passe, certificats, etc.) sur le système d'information et la mise en œuvre de mécanismes de surveillance adaptés. Les recommandations suivantes (non exhaustives) permettent de répondre à ce besoin et d'augmenter le niveau de sécurité du dispositif.

<b>R16</b>	Les comptes et mots de passe d'administration ne doivent pas être utilisés pour ouvrir des sessions de travail sur des postes autres que ceux réservés aux tâches d'administration. Cette recommandation revêt un caractère d'autant plus critique si les postes administrés ont accès à Internet.
------------	--

La recommandation ci-dessus s'applique aussi à l'utilisation de la fonction « exécuter en tant que » (ou « run as ») de Microsoft. Cette fonction implique en effet que l'administrateur se soit authentifié sur le poste de travail. Son empreinte de mot de passe est par conséquent conservée en mémoire sur le poste, ce qui fait peser un risque important sur le compte d'administration en cas de compromission du poste.

<b>R17</b>	Les administrateurs veillent à n'employer les comptes d'administration que pour des tâches qui se rapportent à ces opérations. L'accès aux services d'un autre réseau ou système d'information (bureautique, Internet, messagerie professionnelle, boîtes fonctionnelle, etc.) doit être réalisé non seulement à l'aide de postes de travail bureautiques, mais aussi de comptes utilisateurs à privilèges restreints.
------------	--

Les comptes natifs d'administration, dits *built-in* (ex : root, administrator, etc.), présents sur les systèmes lors de l'installation ne doivent pas être utilisés. L'utilisation de ces comptes doit rester exceptionnelle et restreinte à un nombre d'administrateurs très limité, responsables du domaine technique concerné. En effet, ces comptes ne permettent pas d'imputer de manière précise aux différentes personnes physiques les actions effectuées sur les systèmes. Cela rend aussi impossible la mise en œuvre d'un contrôle d'accès pertinent aux ressources d'administration et la ségrégation des droits. Seule la création de comptes nominatifs d'administration peut répondre à ces besoins.

<b>R18</b>	Les comptes d'administration par défaut ne doivent pas être utilisés pour les tâches courantes d'administration. Ils ne doivent être connus que par un nombre très restreint de personnes. Des comptes nominatifs sont attribués à chaque administrateur.
------------	---

8. Le guide d'hygiène informatique de l'ANSSI est disponible ici : <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/l-anssi-publie-la-version-finalisee-du-guide-d-hygiene-informatique.html>.



Afin de détecter au plus tôt les signes d'une éventuelle compromission et d'appliquer les mesures conservatoires et correctives, il est impératif d'auditer l'usage des comptes d'administration. En outre, il conviendra d'assurer la traçabilité des opérations d'administration effectuées sur le système d'information. L'ensemble des journaux d'événements générés pour cette surveillance ne devra pas être modifiable par un tiers.

<b>R19</b>	<p>Les mécanismes d'audit des événements concernant les comptes d'administration doivent être mis en œuvre. En particulier, les journaux suivants seront activés :</p> <ul style="list-style-type: none"><li>– audit des ouvertures/fermetures de session (opération réussie/échec) ;</li><li>– audit du verrouillage des comptes (opération réussie) ;</li><li>– audit de la gestion des comptes (opération réussie/échec) ;</li><li>– audit de la gestion des groupes de sécurité (opération réussie/échec) ;</li><li>– audit de la validation des informations d'identification (opération réussie) ;</li><li>– audit de la stratégie de compte (opération réussie/échec).</li></ul>
------------	---

L'annexe A de la note technique relative à la mise en œuvre d'un système de journalisation<sup>9</sup> décrit plus en détails les éléments à auditer. Les modalités concernant la journalisation et la supervision de la sécurité sont traitées à la section 10.2.

## 5 Outils d'administration

Les tâches d'administration nécessitent l'usage d'outils qu'il s'agisse de services locaux, de consoles d'administration centralisée, etc. La maîtrise et le contrôle des accès à ces ressources d'administration est une nécessité. **L'accès à ces outils est critique.** Toutes les mesures utiles à leur protection contre des tentatives de compromission ou des usages illicites doivent être mises en œuvre. En fonction des contextes et des solutions techniques, ces mesures peuvent se traduire de différentes manières. Certaines, parmi celles citées ci-dessous de manière non exhaustive, peuvent être cumulatives :

- la mise en œuvre de ressources dédiées aux tâches d'administration (postes, serveurs outils, annuaires, etc.) ;
- le cloisonnement des outils d'administration dans des zones de confiance dédiées ;
- les équipements dotés d'interfaces réseau physiques dédiées à l'administration ;
- l'utilisation de VPN IPsec permettant de cloisonner et protéger les communications d'administration ;
- l'utilisation de protocoles de chiffrement et d'authentification (par exemple, SSH, HTTPS, FTPS, etc.).

Vu la grande surface d'exposition induite par les connectivités réseau, une attention particulière doit être portée sur la protection des accès distants aux ressources d'administration.

Dans la continuité des principes édictés au paragraphe 3.2, la principale mesure vise à cloisonner les outils d'administration en fonction des domaines techniques prédéfinis et des droits d'accès nécessaires à la réalisation des missions de chaque administrateur. Ce cloisonnement se traduit par la mise en œuvre de zones de confiance et de mécanismes de cloisonnement réseau physiques ou logiques (VLAN, etc.), de filtrage et protocoles d'authentification (ex : 802.1x) et de communications chiffrées. Cette pratique contribue à restreindre les risques de compromission, par rebond, d'une zone vers une autre en cas de fragilité d'un des systèmes d'administration. De ce fait, ces zones peuvent être considérées

---

9. Les recommandations relatives à la mise en œuvre d'un système de journalisation sont disponibles ici : <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html>.

comme de *confiance*.

<b>R20</b>	Les outils d'administration doivent être regroupés dans des zones de confiance en fonction des domaines techniques définis et des droits d'accès propres aux administrateurs en ayant le besoin. Le cas échéant, cette mesure peut se traduire par la mise en œuvre de serveurs outils, accessibles à distance, intégrant notamment les logiciels de type clients lourds proposés par les éditeurs et les équipementiers.
------------	---

En complément, il convient d'établir et de mettre en œuvre une matrice des flux en fonction du juste besoin opérationnel. Les règles de filtrage doivent autoriser uniquement les connexions légitimes depuis les postes d'administration vers les services ou équipements. Dans le cadre du maintien en conditions de sécurité, elles doivent faire l'objet d'une procédure régulière de révision. De cette façon, les règles de filtrage obsolètes, inutiles ou trop permissives peuvent être identifiées et supprimées.

<b>R21</b>	Les administrateurs établissent et maintiennent une matrice des flux d'administration depuis les postes d'administration vers les outils d'administration et les ressources administrées.
------------	---

<b>R22</b>	De façon à restreindre les risques de compromission des ressources d'administration, seuls les flux initiés depuis les postes d'administration ou les serveurs outils de la zone d'administration vers les ressources administrées sont autorisés.
------------	--

Quelles que soient les mesures de cloisonnement retenues, il convient de n'utiliser que des protocoles d'administration utilisant des mécanismes de chiffrement et d'authentification (ex : HTTPS, SFTP, etc.). L'objectif consiste à s'assurer de la confidentialité et de l'intégrité des informations. Le choix des outils d'administration doit être judicieux. Une analyse fonctionnelle préalable portant non seulement sur leur conception, sur les mécanismes cryptographiques utilisés mais aussi sur leur fonctionnement doit être menée. Certains outils peuvent en effet 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 des traces éventuelles générées (condensat de mot de passe, etc.) par ces outils et de vérifier le chiffrement de l'ensemble des informations.

<b>R23</b>	Il est recommandé de privilégier systématiquement, dès lors qu'ils existent, des protocoles et des outils d'administration utilisant des mécanismes de chiffrement et d'authentification robustes <sup>10</sup> .
------------	---

Toutefois, certains outils ou protocoles d'administration sont obsolètes et ne mettent pas en œuvre ces mécanismes cryptographiques. Dans ce cas, l'emploi de VPN IPsec, depuis le poste d'administration jusqu'au plus proche de l'équipement, permet de pallier ces carences et est de nature à renforcer le cloisonnement des outils et ressources d'administration. La surface d'attaque de ces ressources en est réduite. Outre les mécanismes d'authentification qu'il offre, il apporte aussi une garantie sur la confidentialité des flux d'administration. Cet avantage est d'autant plus important que certains équipements ne disposent pas de service d'accès distants sécurisés.

<b>R24</b>	À défaut d'un réseau d'administration physiquement dédié ou d'outils d'administration permettant le chiffrement et l'authentification, il conviendra de protéger les flux d'administration par la mise en œuvre d'un VPN IPsec, avec authentification mutuelle par certificats, depuis les outils ou le poste d'administration vers les ressources d'administration.
------------	--

---

10. Le Référentiel Général de Sécurité - RGS - est accessible sur le site de l'ANSSI : <http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/>.

<b>R25</b>	D'une manière générale, il est recommandé que les matériels et les logiciels utilisés pour protéger les ressources d'administration fassent l'objet d'une évaluation de leur niveau de sécurité, idéalement qu'ils soient qualifiés au moins au niveau <i>élémentaire</i> <sup>11</sup> par l'ANSSI.
------------	--

## 6 Ressources administrées

Les ressources du système d'information délivrent avant tout un service aux utilisateurs mais, elles font aussi l'objet de tâches d'administration. L'objectif consiste donc à protéger les éléments nécessaires à leur exécution des tentatives de compromission.

Afin de maîtriser les différentes interconnexions et les communications associées, et ainsi restreindre les risques, il est courant de séparer les interfaces réseau sur chaque équipement administré. Ceci doit être réalisé en fonction des usages. À ce titre, lorsque l'équipement en question est dans un local accessible aux seuls administrateurs, il est recommandé de dissocier les interfaces permettant l'accès aux services de production utilisateurs de celles réservées aux tâches d'administration. Inversement, lorsque celui-ci n'est pas situé dans un tel lieu, comme pour un poste utilisateur ou une station de base sans-fil par exemple, une telle séparation physique n'est pas forcément souhaitable. En effet, un attaquant ayant physiquement accès à l'équipement aurait alors également accès au réseau d'administration.

<b>R26</b>	Lorsque l'équipement est dans un local accessible aux seuls administrateurs, il est recommandé de dédier des interfaces réseaux pour les tâches d'administration.
------------	---

Cette distinction ne doit pas être restreinte aux seules interfaces réseau qu'elles soient physiques ou virtuelles. Les services logiques permettant l'accès aux équipements pour les administrer doivent aussi être configurés de manière à n'être accessibles que sur les interfaces identifiées.

<b>R27</b>	Les services permettant l'exécution des tâches d'administration ne doivent être en écoute que sur les interfaces d'administration prévues à cet effet.
------------	--

L'application de ces mesures implique l'installation d'au moins deux cartes réseau sur les équipements ou, à défaut, d'interfaces virtuelles et de VLAN dédiés. En conséquence, et afin de limiter les risques d'attaque par rebond d'un réseau de production sur un réseau d'administration, il convient de veiller à la bonne configuration des serveurs administrés, notamment en ce qui concerne les tables de routage locale.

<b>R28</b>	Les fonctions internes du système d'exploitation ne doivent pas permettre le routage d'informations depuis les interfaces réseau de production vers l'interface réseau d'administration d'un même équipement. Elles doivent être désactivées (ex : IPForwarding).
------------	---

Dans la continuité des principes de cloisonnement édictés tout au long du document, il est nécessaire de s'assurer qu'il n'est pas possible pour un attaquant, ayant pris le contrôle d'un équipement administré, d'utiliser l'interface réseau d'administration pour rebondir sur les ressources d'administration ou sur tout autre équipement de la production. Pour se prémunir de ce risque, il est impératif de mettre en œuvre des mécanismes de filtrage. Ceux-ci visent à maîtriser les flux entre les équipements administrés et les ressources d'administration. Seuls les flux initiés depuis le réseau d'administration vers les équipements doivent être autorisés.

<b>R29</b>	Un filtrage réseau doit être mis en œuvre entre les équipements administrés et les ressources d'administration. Seuls les flux initiés depuis le réseau d'administration vers les équipements administrés sont autorisés.
------------	---

11. La liste des produits qualifiés est accessible sur le site de l'ANSSI : [www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/](http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/).

Dans le cadre de la défense en profondeur, il conviendra par ailleurs d'interdire toute communication entre les équipements administrés, en particulier via leurs interfaces réseaux d'administration. Ce cloisonnement pourra être réalisé par domaine technique (cf. le paragraphe 3.2).

<b>R30</b>	Un filtrage réseau doit être mis en œuvre entre les équipements administrés, voire par domaine technique, afin d'interdire toute tentative de compromission par rebond via les interfaces réseaux d'administration.
------------	---

## 7 Annuaires

---

### 7.1 Annuaires

L'ensemble des équipements permettant d'identifier et d'authentifier les administrateurs sur les ressources administrées font partie des éléments critiques d'une infrastructure. Leur contrôle permet en effet de disposer de l'ensemble des privilèges sur le système d'information. La principale mesure contribuant à protéger ces ressources et ainsi réduire la surface d'attaque du système d'information consiste à déployer un annuaire propre aux besoins d'administration. Les comptes et privilèges d'administration doivent alors être gérés exclusivement par ce service.

<b>R31</b>	Des annuaires d'identification et d'authentification dédiés aux ressources d'administration doivent être mis en place. Ils assurent la gestion des comptes et des privilèges d'administration ainsi que le contrôle des accès aux ressources administrées.
------------	--

**Remarque** : Les annuaires techniques doivent faire l'objet d'une déclaration à la CNIL dès lors qu'ils contiennent des données à caractère personnel (nom, prénom, etc.). Ils doivent, également, avoir fait l'objet d'une information préalable des salariés quant à leurs droits d'accès, de rectification et d'opposition, y compris lorsque l'annuaire est interne. L'administrateur sera tenu de faire droit aux demandes des salariés concernés.

<b>R32</b>	Les annuaires dédiés à la gestion des comptes d'administration sont déployés dans les zones de confiance, réservées aux ressources d'administration.
------------	--

Pour le cas précis de la technologie Active Directory (AD)<sup>12</sup>, uniquement si ces annuaires ne peuvent pas être totalement dissociés et autonomes pour des raisons techniques, des relations d'approbation pourront être établies entre l'annuaire « utilisateurs » et l'annuaire dédié aux « administrateurs ». Dans ce cas, un certain nombre de précautions est à prendre en compte dans la conception et la configuration des AD.

<b>R32 -</b>	Pour l'administration des annuaires Active Directory de production (ou « utilisateurs »), il est recommandé de mettre en œuvre des forêts et des domaines distincts respectivement pour les administrateurs et les utilisateurs.
--------------	--

Afin de rendre la solution exploitable, cette configuration impose de mettre en œuvre une relation d'approbation. Celle-ci permet à un utilisateur de s'authentifier sur un domaine et d'accéder aux ressources d'un autre domaine sans avoir à se réauthentifier. La direction de cette relation est donc primordiale pour assurer un niveau de sécurité satisfaisant. Dans la continuité du concept de défense en profondeur, il est en effet nécessaire de s'assurer que la compromission de la forêt « Utilisateurs » n'impliquera pas *de facto* la compromission de la forêt « Administrateurs ».

---

12. La note technique concernant les recommandations de sécurité relatives à Active Directory est disponible ici : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-active-directory.html>.

<b>R32 -</b>	Dans le cadre de la mise en œuvre d'une relation d'approbation entre la forêt « Utilisateurs » et la forêt « Administrateurs », il convient que celle-ci soit de type Forêt, de sens unique et qu'elle consiste à ce que seuls les comptes du domaine « Administrateurs » accèdent aux ressources du domaine « Utilisateurs ». Le filtrage des SID <sup>13</sup> doit être activé sur cette relation d'approbation et le paramètre SIDHistory désactivé.
--------------	--

<b>R32 -</b>	Le mode « authentification sélective » est à privilégier pour ce type de relation d'approbation. Cette dernière permet d'adopter une approche simple et sécurisée : toutes les authentifications sont refusées à l'exception de celles explicitement autorisées.
--------------	--

Au-delà de la simple mesure qui consiste à dissocier les annuaires suivant les usages, la configuration et la gestion de ces annuaires doivent faire l'objet d'attentions en matière de sécurité. Cette tâche nécessite une étude préalable afin notamment de définir l'organisation logique de l'annuaire la plus adaptée aux besoins et à l'organisation de l'entité ainsi que les droits d'accès au système d'information. Le résultat de cette analyse permettra aux administrateurs de configurer les équipements.

<b>R33</b>	Une analyse préalable au déploiement des annuaires est indispensable pour définir l'organisation logique de l'annuaire ainsi que les droits d'accès au système d'information cible.
------------	---

Pour définir cette architecture logique d'annuaire, en dehors de tout contexte, les administrateurs peuvent s'appuyer sur les travaux de définition des domaines fonctionnels et techniques évoqués au paragraphe 3.2. Ceci permet d'assurer une cohérence entre la répartition technique des ressources d'administration au sein du système d'information et la politique de contrôle d'accès. Une bonne pratique consiste aussi à regrouper les objets de l'annuaire en fonction de leur nature (serveurs, utilisateurs, etc.).

Après la mise en œuvre de l'annuaire, il faut positionner des droits d'accès de façon à restreindre l'accès aux ressources administrées au juste besoin. L'annuaire doit être protégé de toute modification intempestive mais aussi de tout accès non contrôlé sur les attributs critiques, tels les champs de type *password*.

<b>R34</b>	Des droits, permettant de restreindre l'accès aux éléments de l'annuaire, doivent être mis en œuvre en fonction du juste besoin.
------------	--

De plus, des politiques de sécurité sont à définir et à déployer pour assurer le contrôle d'accès aux ressources d'administration du système d'information pour l'intégrité du dispositif. Cela consiste à maîtriser les accès des différentes catégories d'administrateurs, en fonction des domaines fonctionnels et/ou techniques qui leur sont attribués, au travers de profils 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 tâches d'administration sur les équipements ou les services identifiés. Le principe du moindre privilège doit être appliqué ;
- les autorisations d'accès aux ressources : des règles de contrôle d'accès doivent être définies de façon à préciser les modalités d'accès aux ressources d'administration telles les horaires, le type d'authentification, les actions autorisées et/ou interdites, etc. ;
- le cas échéant, la stratégie de mot de passe : longueur minimale et maximale, délais de modification, nombre de tentatives de connexion avant verrouillage du compte, historique, etc.

---

13. Les SID (Security Identifiant) sont les identifiants uniques d'un objet de l'annuaire.

<b>R35</b>	Des politiques de sécurité sont déployées dans le but de contrôler l'accès aux ressources d'administration du système d'information en fonction du juste besoin opérationnel, de définir les privilèges de chaque compte d'administration et de garantir l'intégrité de l'annuaire.
------------	---

L'exploitation d'un annuaire nécessite d'assurer dans le temps la gestion des comptes et des privilèges. Cette gestion se traduit par un suivi rigoureux des créations, suppressions ou modifications des comptes nécessitant un accès au système. Cela impose aussi d'ajuster les droits et privilèges des utilisateurs autant que de besoin. En application du principe de moindre privilège, il s'agit donc pour les responsables de chaque domaine fonctionnel de formaliser et de mettre en œuvre les processus et les procédures organisationnelles nécessaires.

<b>R36</b>	Un processus organisationnel et technique de gestion des comptes d'administration et des privilèges associés doit être mis en œuvre tout au long du cycle de vie du système d'information.
------------	--

Pour contribuer au maintien en condition de sécurité, il est nécessaire d'inscrire ce processus dans la durée. Une procédure de contrôle et de révision régulière des comptes et des autorisations d'accès doit être définie en associant étroitement des représentants des entités opérationnelles qui devront l'appliquer.

<b>R37</b>	Le processus de gestion des comptes et des privilèges doit intégrer une procédure de contrôle et de révision régulière de ces comptes et des autorisations d'accès aux ressources d'administration.
------------	---

## 7.2 Authentification

Au-delà des mesures propres au contrôle d'accès, il faut définir le type d'authentification qu'il convient de mettre en œuvre. Pour mémoire, l'authentification permet de s'assurer de l'identité d'un administrateur ou d'un service d'administration avant d'autoriser son accès aux ressources administrées. Les mesures de sécurité concernant les mécanismes d'authentification viennent donc en complément des précautions sur les protocoles d'administration évoquées plus haut. Le référentiel général de sécurité (RGS<sup>14</sup>), et notamment les annexes B1, B2 et B3, décrivent plus en détail les mécanismes cryptographiques et d'authentification.

<b>R38</b>	En phase de conception ou de révision des architectures d'administration, il convient de se référer aux annexes B1, B2 et B3 du référentiel général de sécurité (RGS) afin de mettre en conformité les mécanismes d'authentification utilisés.
------------	--

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

Une authentification est dite *forte* dès lors qu'au moins deux facteurs différents sont utilisés<sup>15</sup>. En informatique, il est courant de combiner les facteurs *ce que je sais* et *ce que je possède*.

14. Le Référentiel Général de Sécurité - RGS - est accessible sur le site de l'ANSSI : <http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/>.

15. Il est à noter que l'authentification multi-facteurs n'apporte pas de réelle sécurité si l'authentification par simple mot de passe reste autorisée en parallèle.



<b>R39</b>	Pour les tâches 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 token USB est courant et recommandé. Ces matériels sont porteurs d'une partie des éléments secrets contribuant au processus d'authentification. Conformément à la recommandation précédente, 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 l'acquisition de certificats et, plus généralement, induit la notion de confiance dans la chaîne de certification et dans l'infrastructure de gestion de clé (IGC). En effet, si l'usage de certificats peut paraître 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, révocation, etc.) et, par conséquent, dans le prestataire rendant ces services.

<b>R40</b>	L'usage de certificats électroniques comme élément contribuant à l'authentification est recommandé.
------------	---

<b>R41</b>	Il convient d'acquérir ces certificats auprès d'un prestataire de services de certificats électroniques (PSCE) qualifié <sup>16</sup> par l'ANSSI, ou de déployer une infrastructure de gestion de clés conforme aux exigences du référentiel encadrant ce domaine.
------------	---

Concernant l'authentification des administrateurs, il convient de déterminer si celle-ci doit être locale ou centralisée. Ces deux architectures comportent respectivement des avantages et des inconvénients. Elles ne répondent pas aux mêmes besoins et n'impliquent pas les mêmes contraintes d'exploitation et de sécurité. Une réflexion préalable est donc nécessaire pour déterminer la solution la plus adaptée au contexte de l'entité et du système d'information cible. Toutefois, sauf cas particulier, l'utilisation d'un serveur d'authentification centralisée est préconisée. En effet, cette solution permet notamment d'éviter les problématiques liées à la « sédimentation » des comptes créés dans le temps sur le système d'information. Elle favorise donc un meilleur suivi de ces comptes, de leurs usages et du respect de la politique de sécurité (renouvellement des secrets d'authentification, verrouillage, etc.). Un certain nombre de technologies permettent de répondre à ce type d'architecture : Kerberos, RADIUS, etc. Si ce choix est retenu, l'emploi d'une authentification multi-facteurs revêt un caractère prioritaire car elle apporte une confiance supplémentaire dans le dispositif et résiste mieux aux attaques de type force brute.

<b>R42</b>	Il est recommandé de privilégier une architecture d'authentification centralisée en lieu et place d'une gestion locale directement sur les équipements administrés.
------------	---

## 8 Passerelle d'administration

Les ressources d'administration sont le cœur de tout système d'information. Leur protection est une nécessité pour prévenir toute compromission. Le principe majeur présenté dans ce document consiste à séparer physiquement ou logiquement, à l'aide de mécanismes cryptographiques essentiellement, ces ressources et à maîtriser leurs accès en fonction du besoin d'en connaître. L'augmentation du nombre de systèmes et la complexité croissante des solutions techniques d'administration rend cette tâche, ainsi que la conception d'une architecture adaptée, délicates. Les contraintes budgétaires, la réduction des ressources humaines et la nécessité de maintenir un service continu sont autant de facteurs conjoncturels supplémentaires. Ils incitent généralement les entités à se doter d'accès nomades pour

16. La liste des prestataires de services de certification électronique est disponible : <http://www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies/prestataires-de-services-de-certification-electronique-psce-et-d-horodatage.html>.

leurs administrateurs, voire à externaliser<sup>17</sup> ou sous-traiter certaines actions d'administration.

La mise en œuvre d'une passerelle d'administration peut répondre techniquement, en partie, à ces contraintes. Elle se matérialise par une DMZ déployée entre les ressources d'administration et un système de moindre confiance. Elle permet de protéger les ressources du système d'information au travers d'un point d'accès unique et maîtrisé. Elle propose entre autres des mécanismes relais permettant une rupture des échanges entre l'administrateur et les équipements administrés. Il est primordial de rappeler, conformément au principe de défense en profondeur, la nécessité de sécuriser l'ensemble des éléments constituant le système d'information. En particulier, les équipements finaux devront aussi faire l'objet d'une configuration sécurisée de manière à ralentir un attaquant ou à détecter toute activité malveillante.

Les fonctions minimales nécessaires sur ce type de passerelle<sup>18</sup> doivent être :

- l'authentification ;
- la gestion des identités ;
- le contrôle et la gestion des accès aux ressources administrées ;
- la traçabilité ;
- le chiffrement ;
- les mécanismes d'administration propres aux besoins de la passerelle qui doivent être *hors ligne*.

Toutes ces fonctions sont détaillées en [annexe I](#). En outre, la réelle plus value de ce dispositif est portée par les fonctions d'authentification, de contrôle et de gestion des accès, ainsi que de traçabilité. Elles contribuent de manière significative à la sécurité et ont une granularité suffisamment fine pour permettre de bien identifier les accès sur l'infrastructure du système d'information et les actions effectuées.

<b>R43</b>	En priorité, les passerelles d'administration doivent intégrer les fonctions d'authentification, de contrôle et de gestion des accès, ainsi que de traçabilité.
------------	---

Ces notions sont d'autant plus importantes lorsqu'une externalisation de l'administration est envisagée. Les actions portées par ces passerelles d'administration nécessitant des privilèges élevés, il est impératif de pouvoir attribuer des droits en fonction du juste besoin mais surtout d'assurer la traçabilité et l'imputabilité des actions.

<b>R44</b>	Pour les systèmes d'information les plus sensibles, les composants de la passerelle d'administration portant les fonctions de contrôle et de gestion des accès doivent faire l'objet d'une évaluation de sécurité et utiliser des produits labellisés par l'ANSSI lorsqu'ils existent.
------------	--

## 8.1 Architecture type

Les schémas suivants illustrent la mise en œuvre des fonctions nécessaires à une passerelle d'administration. Deux cas d'usage sont proposés : avec ou sans rupture protocolaire. L'emploi général d'une passerelle d'administration consiste en effet à assurer une rupture des échanges entre le poste d'administration et l'équipement administré. Néanmoins, il peut être nécessaire, dans certains cas, de

---

17. Le guide relatif à l'externalisation et à la maîtrise des risques est disponible : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html>

18. Il n'est pas exclu que ces fonctions puissent être intégrées dans un seul et même équipement. Il conviendra en revanche de s'assurer du niveau de confiance dans cet équipement, notamment au travers du processus de qualification de l'ANSSI : <http://www.ssi.gouv.fr/fr/certification-qualification/qualification-d-un-produit-de-securite/>.



garantir l'établissement de bout en bout d'une authentification puis d'une session. Ce cas d'usage ne doit toutefois pas être utilisé pour des accès à des personnes externes à l'entité (par exemple, TMA, équipementiers, etc.).

Les fonctions de la passerelle sont représentées dans les zones orangées sur les figures suivantes.

### *Passerelle d'administration avec rupture protocolaire*

Cette illustration présente le cas d'usage le plus courant d'une passerelle d'administration. La passerelle met en œuvre des serveurs de rebond 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 lors de session d'administration.

Ce type d'architecture met en œuvre de l'interception protocolaire de façon à appliquer un certain nombre de contrôles sur les flux d'administration. Ces opérations visent notamment à assurer une meilleure journalisation des actions des administrateurs. En premier lieu, il convient de préciser que cette pratique d'interception des flux est à considérer avec précaution et n'est pas souhaitable dans certains cas. L'ANSSI a publié une note technique sur l'analyse des flux HTTPS qui traite notamment des aspects juridiques liés à ces usages<sup>19</sup>.

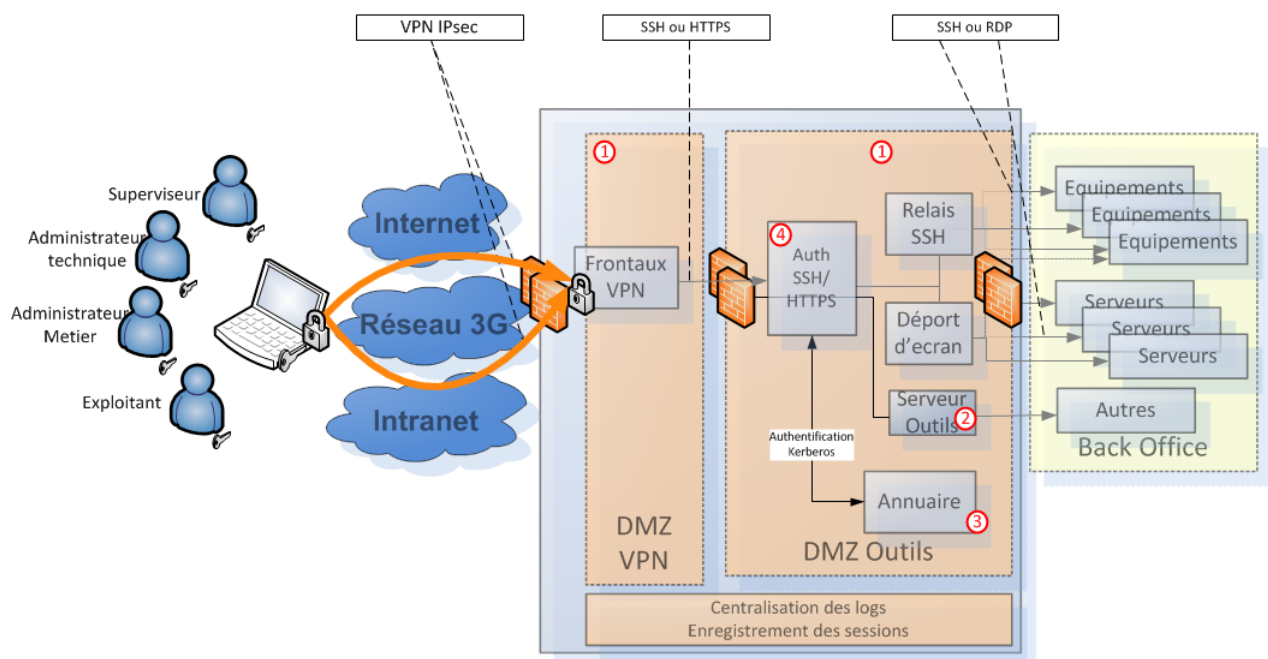


FIGURE 4 – Architecture d'une passerelle d'administration

- ① Instanciation des VPN et des « DMZ Outils » en fonction des domaines fonctionnels et techniques
- ② Clients lourds d'administration (ex : FW, BDD, ...)
- ③ Annuaire dédié aux connexions « Administrateurs », peuplé ou non depuis un référentiel d'identité
- ④ Fonction d'authentification et de contrôle d'accès aux services d'administration (ex : liste des équipements accessibles)

<b>R45</b>	Les passerelles d'administration avec rupture protocolaire doivent être privilégiées pour des accès par des personnes externes (par exemple, TMA, équipementiers, etc.).
------------	--

19. Le document est accessible ici : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/authentification-et-mecanismes-cryptographiques/recommandations-de-securite-concernant-l-analyse-des-flux-https.html>.

## Passerelle d'administration sans rupture protocolaire

Pour ce cas d'usage particulier, l'objectif consiste à ne pas rompre la session sécurisée, basée sur des mécanismes cryptographiques de confiance.

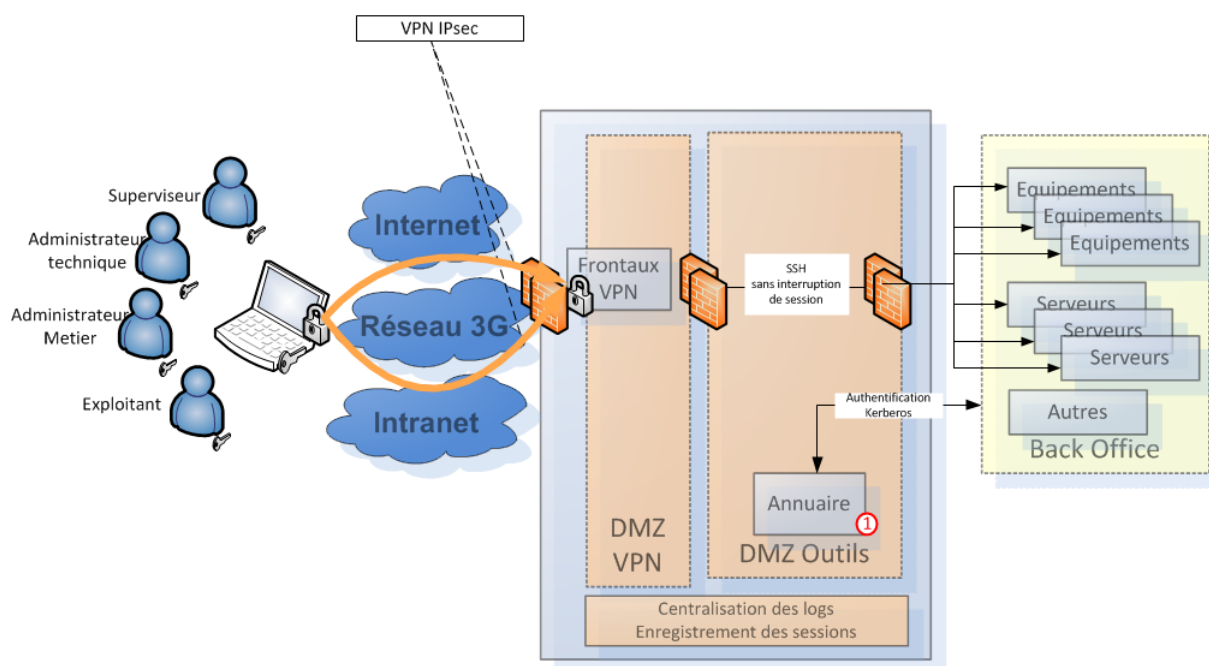


FIGURE 5 – Architecture d'une passerelle d'administration sans rupture protocolaire

① Annuaire dédié aux connexions « Administrateurs », peuplé ou non depuis un référentiel d'identité

<b>R46</b>	Les passerelles d'administration sans rupture protocolaire doivent être réservées à l'usage des administrateurs internes à l'entité.
<b>R47</b>	Dans la mesure où les équipements administrés peuvent assurer les fonctions d'authentification, de contrôle et de gestion des accès et de traçabilité, les passerelles d'administration sans rupture protocolaire sont à privilégier pour les administrateurs internes à l'entité.

## 8.2 Nomadisme et accès distants

Les accès distants ou nomades pour les tâches d'administration tendent à se développer. Les raisons de cette généralisation sont la nécessité, d'une part, d'assurer un service permanent et, d'autre part, de bénéficier des nombreuses compétences techniques pour exploiter les systèmes dont certaines imposent une sous-traitance. L'emploi de ces passerelles doit donc s'envisager pour maîtriser ces interconnexions et les accès différents des administrateurs internes à l'entité ou des sous-traitants (équipementiers, éditeurs pour par exemple de la Tierce Maintenance Applicative - TMA, expertise de niveau 3, etc.).

<b>R48</b>	Dans le cadre de l'emploi de passerelles d'administration pour des accès distants ou nomades à tout ou partie du système d'information, il convient de dissocier physiquement les passerelles dédiées à l'accès distant des administrateurs internes de celles permettant les accès distants aux sous-traitants.
------------	--

<b>R49</b>	Pour les passerelles d'administration dédiées aux sous-traitants, il est recommandé de cloisonner les serveurs outils et de contrôler l'accès aux équipements administrés, en fonction du domaine technique des intervenants.
------------	---

La notion d'accès distant implique aussi de maîtriser la liaison de communication entre le poste ou le site distant et la passerelle d'administration. 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 est recommandé. La technologie VPN IPsec permet de répondre à ce besoin. Contrairement à la technologie SSL/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.

<b>R50</b>	Un VPN IPsec est mis en œuvre entre le poste administrateur nomade, ou le site distant, et sa passerelle d'administration.
------------	--

<b>R51</b>	Pour la mise en œuvre du protocole IPsec, les recommandations de la note technique publiée par l'ANSSI pour la protection des flux <sup>20</sup> doivent être appliquées.
------------	---

<b>R52</b>	Pour un système d'information critique, l'emploi d'un équipement VPN IPsec qualifié au niveau standard est fortement recommandé.
------------	--

La conception d'une architecture permettant de répondre aux besoins de nomadisme, basée sur la technologie IPsec, nécessite d'être étudiée avec attention. Notamment, pour assurer une certaine convivialité d'emploi, il peut être utile de disposer d'un seul poste d'administration permettant une connexion depuis le réseau interne d'administration ou une connexion nomade. Pour répondre à ce besoin, il convient de disposer d'une part de passerelles VPN IPsec au sein du réseau interne, à défaut d'un réseau physiquement dédié et, d'autre part, en périphérie du système d'information. Ces passerelles, ainsi qu'une configuration adaptée du client VPN (2 profils de connexion), permettront aux postes administrateurs d'accéder aux ressources d'administration.

<b>R53</b>	En configuration nomade, des passerelles IPsec supplémentaires sont déployées en frontal du réseau non maîtrisé pour permettre l'établissement d'un tunnel de communication depuis le poste d'administration nomade vers la passerelle d'administration.
------------	--

20. Le guide ANSSI relatif à IPsec pour la protection des flux réseau est disponible ici : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/recommandations-de-securite-relatives-a-ipsec-pour-la-protection-des-flux.html>

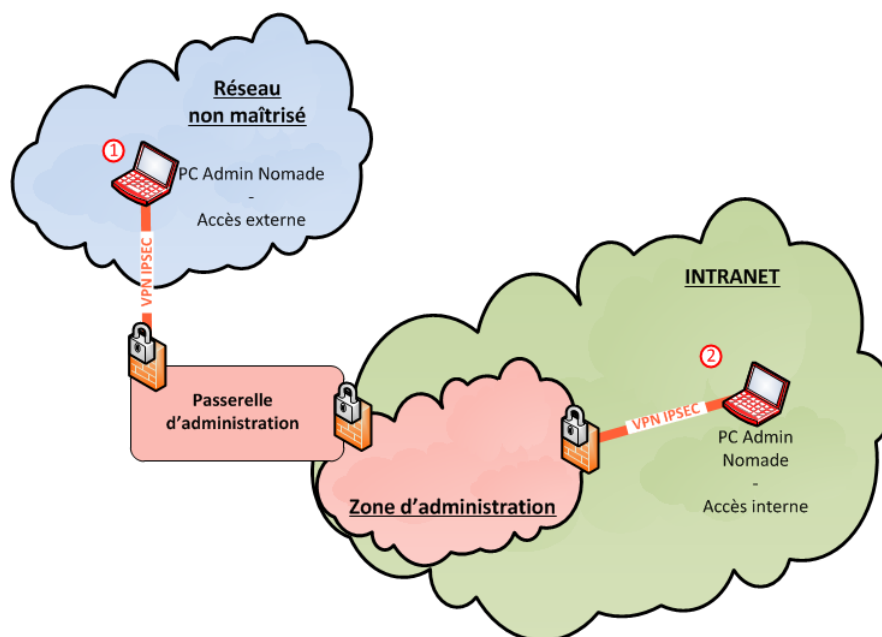


FIGURE 6 – Architecture d'accès nomade aux ressources d'administration

- ① Accès à la zone d'administration via un concentrateur VPN IPsec externe et une passerelle d'administration
- ② Accès à la zone d'administration via un concentrateur VPN IPsec interne

Néanmoins, la mise en œuvre d'accès nomades pour l'administration fait porter un poids plus fort sur la maîtrise du poste de travail et sur sa configuration. En effet, cette pratique augmente sensiblement les risques de compromission du système d'information, en particulier en cas de vol ou de perte du poste.

<b>R54</b>	Les mesures de sécurité décrites au paragraphe 4.2 doivent obligatoirement et intégralement être mises en œuvre sur le poste nomade d'administration.
------------	---

## 9 Système d'échange

Le présent document recommande la séparation physique et/ou logique des ressources d'administration. Ceci interdit l'accès à Internet depuis les postes d'administration. Toutefois, les administrateurs peuvent éprouver le besoin d'échanger des informations avec des correspondants extérieurs (ex : éditeurs, équipementiers, etc.) ou de récupérer certaines informations pour assurer l'exploitation de leurs infrastructures (ex : firmware, etc.). Afin de pallier les risques notamment liés à l'usage des supports de stockage amovibles (ex : clé USB, etc.), un système d'échange d'informations est donc nécessaire. Il est primordial que ce dispositif ne fragilise pas les moyens de protection des ressources d'administration.

<b>R55</b>	Pour la conception de l'architecture d'un dispositif d'échange avec la zone d'administration, il convient de définir au préalable les besoins exacts des équipes d'administration en la matière.
------------	--

<b>R56</b>	Les systèmes d'échange permettant le transfert d'informations entre une zone de confiance d'administration et d'autres zones ne doivent en aucun cas dégrader le niveau de sécurité des ressources d'administration. Ce dispositif doit être intégré au périmètre de l'analyse de risques menée pour le système d'information.
------------	--

Pour cela, il est nécessaire d'établir précisément la liste des besoins en termes d'échange et plus particulièrement :

- le type d'information (documentation, exécutable, etc.) ;
- le format de ces informations ;
- la volumétrie ;
- la fréquence d'échange ;
- le type d'usage (export/import de journaux pour investigation, mises à jour, etc.) ;
- le mode d'accès aux informations.

Sur la base de ce cahier des charges, seules les fonctions strictement utiles à la réalisation des tâches d'administration doivent être retenues. Le système d'échange doit seulement autoriser les protocoles permettant le transfert de données et interdire toute possibilité d'ouvrir des sessions de travail d'une zone de confiance à une autre. À titre d'exemple, le service SSH<sup>21</sup> (*Secure Shell*) doit être configuré uniquement pour permettre des commandes de transfert de fichier de type SCP (*Secure Copy*) ou SFTP (*SSH Transfert File Protocol*).

<b>R57</b>	Les services et les protocoles permettant uniquement le transfert de données doivent composer le système d'échange. En aucun cas, il ne doit être possible d'accéder à une session de travail par le biais d'un système d'échange.
------------	--

L'accès à la zone d'échange depuis une zone de moindre confiance doit être réservé strictement aux postes et aux utilisateurs ayant le besoin de transférer des informations vers la zone d'administration. Cette pratique réduit la probabilité qu'une autre machine compromise sur le réseau de moindre confiance puisse déposer des fichiers malveillants sur la zone d'échange. Cette restriction peut être réalisée par la mise en œuvre d'un filtrage et d'un contrôle d'accès à la zone d'échange.

<b>R58</b>	Il est recommandé de restreindre l'accès à la zone d'échange uniquement aux postes et aux utilisateurs qui en ont besoin.
------------	---



Par ailleurs, ce système d'échange doit être configuré pour ne pas stocker de manière permanente les fichiers transférés d'une zone à une autre. Les informations doivent transiter temporairement et être supprimées dès que leur transfert est effectif. Cette pratique vise à restreindre les risques de fuite ou de compromission des informations pouvant mener, notamment, à la compromission du système d'information d'administration.

<b>R59</b>	Les informations échangées ne doivent pas être stockées de manière permanente sur le système d'échange. Dès que leur transfert d'une zone à une autre est effectif, elles doivent être supprimées.
------------	--

Enfin, les mécanismes de filtrage de contenu et de protection contre les codes malveillants devront être systématiquement déployés. Cette mesure vise à protéger les postes administrateurs 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. Tous les échanges seront soumis à ces moyens de protection.

21. Le guide ANSSI de recommandations pour un usage sécurisé d'(Open)SSH est disponible ici : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/recommandations-pour-un-usage-securise-d-open-ssh.html>

<b>R60</b>	L'ensemble des données échangées doit être soumis systématiquement à une analyse de contenu à la recherche de codes malveillants.
------------	---


Les illustrations présentées au travers des différents cas d'usage ci-dessous comportent deux représentations de systèmes d'échange  ou . Ils correspondent à des niveaux de sécurité et à des principes d'architecture différents.

### *Systeme d'échange simple*

Ce système d'échange, dit simple, est basé sur l'utilisation de matériels et de logiciels courants et assurant des fonctions complémentaires.

Une architecture peut par exemple se composer de pare-feux et de services de type serveur (ex : SCP, FTPS, ...). Elle implique nécessairement une ou plusieurs interconnexions entre des zones de niveaux de confiance différents. La règle générale, qui consiste à ce que seuls sont autorisés les flux après établissement de la connexion depuis la zone qui est la plus de confiance vers celle qui l'est moins, s'applique ici.

<b>R61</b>	Dans le cas d'un système d'échange simple, il convient de s'assurer qu'aucun flux d'une zone de moindre confiance ne puisse accéder directement à une zone de confiance supérieure.
------------	---

Ce système d'échange simple sera représenté dans les schémas par le logo . Ce système ne permet pas de prétendre à un haut niveau de sécurité. Les flux peuvent être organisés de la façon suivante :

- des postes d'administration vers les équipements de transfert de données ;
- des postes de la zone bureautique vers les équipements de transfert de données.

Les deux schémas suivants proposent des illustrations différentes, plus ou moins complexes, pour ce type de système d'échange.

La première représentation est d'un niveau de confiance supérieur à la seconde. En effet, dans la mesure où seuls des services logiques de transfert de fichiers sont autorisés (cf. recommandations précédentes), la « zone de partage » apporte certaines garanties sur la protection du « niveau haut », représentant ici la zone d'administration. Aucun flux direct n'est possible entre les deux niveaux, et ce, quel que soit le sens.

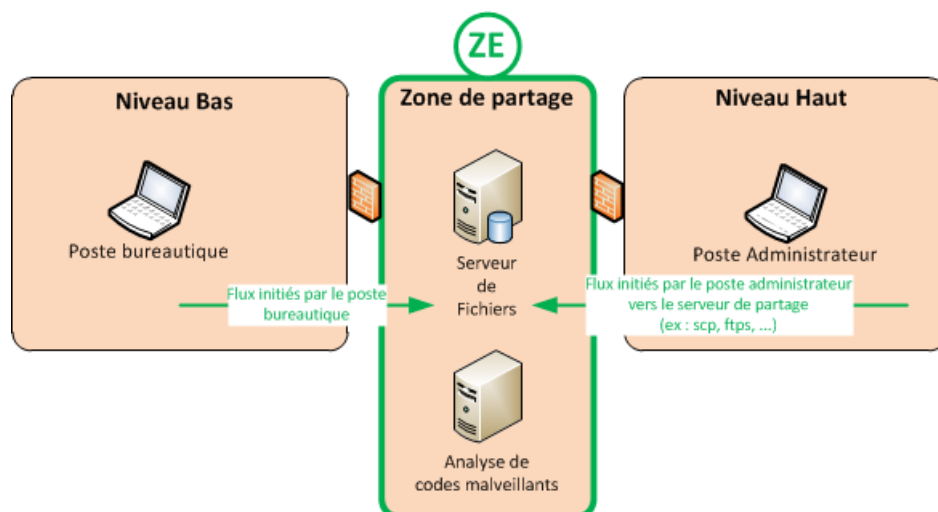


FIGURE 7 – Exemple n°1 de système d'échange de fichiers

La seconde représentation décrit un système d'échange simple de **moindre confiance**. En effet, en l'absence d'une zone de partage, la zone d'administration initie un flux de transfert de fichiers directement dans la zone de moindre confiance : seule une règle de pare-feu interdit un flux à l'initiative de la zone de moindre confiance vers la zone d'administration.

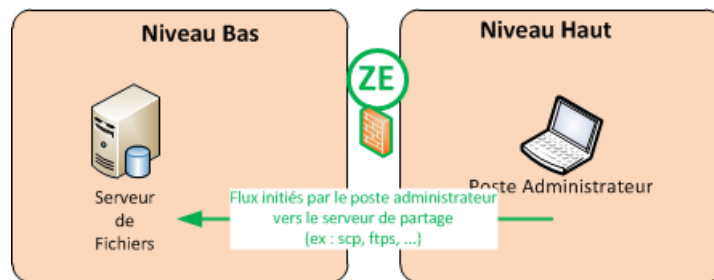



FIGURE 8 – Exemple n°2 de système d'échange de fichiers

Toutefois, ce dernier système d'échange n'assure pas un niveau de sécurité optimal. Il ne permet pas de garantir de manière formelle qu'aucune fuite d'information ou compromission ne sera possible depuis la zone d'administration.

### *Système d'échange sécurisé de type diode*

Pour assurer un niveau de sécurité optimal, l'emploi d'une diode « agréée » par l'ANSSI doit être envisagé. Ce dispositif est représenté dans les schémas d'architecture par le logo . Ce système permet d'atteindre un niveau de sécurité le plus élevé. L'utilisation d'une telle diode implique que seuls les flux initiés depuis la zone bureautique vers la zone administrateur soient autorisés. Cette disposition n'est rendue possible que par l'usage d'un mécanisme physique et optique, de confiance. Cette diode garantit que seuls des flux unidirectionnels (par exemple, UDP) sont possibles. Ceci empêche en particulier les tentatives de connexions malveillantes depuis le réseau d'administration vers un système de moindre confiance et la fuite d'informations. Un système d'émission (guichet bas) et de réception (guichet haut) des fichiers ou des paquets, dans le cas de protocoles en mode « connecté » (par exemple FTP), est nécessaire au fonctionnement du dispositif.

Dans le cas d'une architecture sécurisée, cette diode garantit l'étanchéité de la zone de confiance administrateur qui est physiquement dédiée. On remarque que la règle concernant le système d'échange simple, et indiquant que le flux doit être initié depuis la zone de confiance, n'est pas applicable dans le cas d'un système d'échange sécurisé. En effet, seul un flux unidirectionnel, en mode « non connecté », est techniquement possible ici (par exemple : UDP).

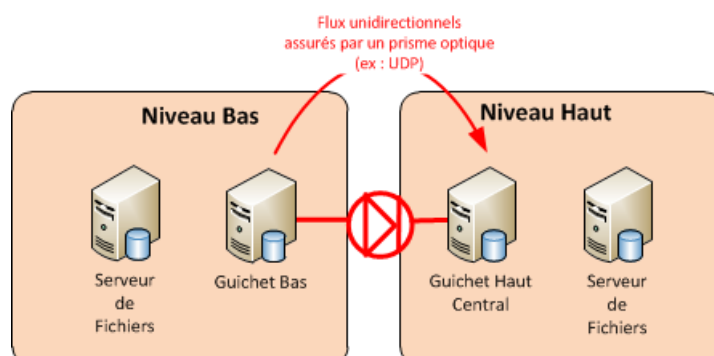


FIGURE 9 – Système d'échange de fichiers sécurisé à l'aide d'une diode agréée



<b>R62</b>	Dans le cadre d'un échange d'informations depuis une zone de moindre confiance vers le système d'administration, pour garantir l'étanchéité du réseau d'administration, il est recommandé de déployer un système d'échange de type diode.
------------	---

## 10 Maintien en condition de sécurité

### 10.1 Mises à jour de sécurité des zones d'administration

De par son caractère critique, l'infrastructure d'administration doit particulièrement respecter le principe de maintien en condition de sécurité. Il consiste en la mise en œuvre de l'ensemble des mesures techniques et non techniques de façon à :

- maintenir au minimum, tout au long du cycle de vie du système d'information, le niveau de sécurité initial du système ;
- anticiper ou, à défaut, pallier l'émergence des nouveaux risques (principe de défense en profondeur). Ce point impose la révision régulière de l'analyse de risques propre au système d'information (au moins annuelle) ;
- éclairer les autorités décisionnelles et les acteurs chargés de la mise en œuvre du système, des risques encourus.

<b>R63</b>	Assurer le maintien en condition de sécurité de l'ensemble des éléments constituant le système d'administration.
------------	--

Les tâches contribuant au maintien en condition de sécurité étant nombreuses et non spécifiques aux tâches d'administration, ce paragraphe n'a donc pas vocation à être exhaustif. Seule la problématique des mises à jours de sécurité, dont celles des systèmes d'exploitation et des logiciels de lutte contre les codes malveillant est traitée ici.

Pour respecter les principes d'architecture de ce document, ces mises à jour ne devront être possibles qu'au travers de dépôts relais internes à l'entité, mettant en œuvre des filtrages par liste blanche. Il convient que ces équipements soient dédiés aux services d'administration et isolés d'Internet par une passerelle de type DMZ.

<b>R64</b>	Pour l'application des mises à jour des correctifs de sécurité, voire des signatures antivirales, il convient de mettre en œuvre des serveurs relais dédiés au sein d'une DMZ. Seuls les flux initiés depuis ces dépôts relais vers Internet doivent permettre le téléchargement des mises à jour.
------------	--

<b>R65</b>	Des mécanismes de filtrage par liste blanche permettent de restreindre l'accès aux seuls sites éditeurs ou constructeurs autorisés.
------------	---



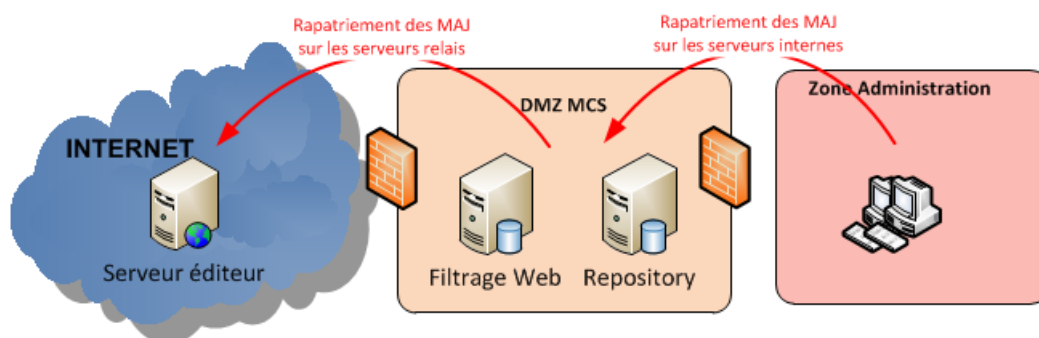


FIGURE 10 – Architecture de mise à jour des correctifs de sécurité

Enfin, pour éviter toute régression de service suite à la mise en œuvre d'un correctif technique ou de sécurité, il convient de qualifier 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.

<b>R66</b>	Les administrateurs procéderont à la qualification des correctifs de sécurité avant leur mise en production et leur généralisation.
------------	---

## 10.2 Supervision de la sécurité

### Généralités

Les bonnes pratiques en matière de sécurité recommandent la mise en œuvre des mécanismes de journalisation et de supervision. En effet, la journalisation, le stockage et l'analyse régulière des événements techniques dont ceux touchant à la sécurité permettent de détecter les traces d'une éventuelle compromission du système. L'archivage de ces informations dans le temps autorisent les analyses post-mortem (ou « *forensic* ») pour comprendre comment et par quels moyens l'intrusion a été possible.

<b>R67</b>	Les administrateurs veillent à s'approprier le guide de l'ANSSI relatif aux problématiques de journalisation <sup>22</sup> , et à en appliquer les principes et les recommandations.
------------	--

### Points d'attention en termes d'architecture

En termes d'architecture, les besoins de journalisation doivent être pris en compte dans l'étude de conception du système. Ce domaine peut être dans une certaine mesure considéré comme un domaine fonctionnel, et les équipements et les services qui le composent, comme un domaine technique (cf. paragraphe 3.2). Suivant le résultat de l'analyse fonctionnelle et l'organisation des équipes d'administration, les orientations d'architecture peuvent conduire à dédier une zone de confiance pour les services de journalisation des moyens d'administration.

<b>R68</b>	La journalisation doit être intégrée à la réflexion dès la phase de conception de l'architecture d'administration. Il est recommandé qu'un domaine fonctionnel et/ou technique lui soit consacré. Ceci se traduit par la mise en œuvre d'une zone de confiance et d'un contrôle d'accès dédié à cette zone.
------------	---

Cette mesure se justifie d'autant plus que, pour assurer une analyse pertinente des journaux d'événements par les personnes en charge de ce domaine, il convient de garantir l'intégrité des journaux

22. Les recommandations relatives à la mise en œuvre d'un système de journalisation sont disponibles ici : <http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html>.

depuis leur génération jusqu'à leur lieu de stockage. En cas d'intrusion, les attaquants pourront vouloir effacer ou modifier les traces générées de façon à ce que leur présence ne soit pas détectée. Afin de couvrir ce risque, au-delà du cloisonnement des services de journalisation, il est nécessaire de s'efforcer de restreindre les accès à ces informations aux seules personnes ayant le besoin d'en connaître.

**R69**

En complément des mesures de contrôle d'accès aux journaux d'événements, l'architecture doit prévoir la transmission des journaux d'événements de manière centralisée, depuis les équipements vers les services de journalisation.

## Annexes

---

## Annexe I : Passerelle d'administration - Cahier des charges

---

Cette annexe décrit, pour chacune des fonctions citées au chapitre 8, les exigences principales de sécurité à prévoir pour une passerelle d'administration.

### *Authentification*

La fonction d'authentification :

- doit être compatible avec une authentification par certificats - IGC externe - avec ou sans support matériel (par exemple, jeton) ;
- doit pouvoir être interopérable avec un relais d'authentification (par exemple : Kerberos, RADIUS, etc.) et/ou les technologies standards de type SAMLv2 ;
- permet de garantir l'authentification distincte de l'utilisateur et de son poste, ainsi que son appartenance à un groupe conférant certains droits ;
- peut imposer une méthode d'authentification des clients distants indépendamment des méthodes d'authentification retenues par les équipements protégés (mode bridge) ;
- dans le cas du mode bridge, elle peut associer deux jeux de certificats x509, un pour l'authentification des utilisateurs distants et l'autre pour les équipements protégés ;
- le cas échéant, elle peut relayer l'identification de l'utilisateur (extrait du certificat utilisateur) jusqu'à l'équipement protégé.

Il est à noter que la protection des secrets d'authentification est un élément fondamental de la solution.

### *Gestion des identités*

La fonction d'identification :

- doit être possible depuis un annuaire LDAP ou un Active Directory distinct ;
- permet une gestion discriminante des droits ;
- est compatible avec les protocoles mettant en œuvre des mécanismes de chiffrement (LDAPS, etc.).

### *Contrôle d'accès*

La passerelle d'administration :

- doit s'intégrer en périphérie du réseau d'administration, en coupure entre les administrateurs et les équipements à protéger ;
- peut permettre la continuité de session entre le client et l'équipement protégé ;
- peut agir comme relais et être positionnée en coupure du trafic, lorsque cela est nécessaire. Les connexions sont clairement coupées entre le client distant et les équipements protégés ;
- permet l'utilisation de protocoles d'administration différents entre le client et la passerelle, puis entre la passerelle et l'équipement protégé (cas d'un équipement obsolète n'intégrant pas les protocoles de sécurité) ;
- permet le rebond d'accès SSH, RDP, HTTPS, SFTP, SCP, etc.
- permet d'imposer des restrictions sur les protocoles d'administration (ex : restriction des commandes/fonctionnalités utilisées par un administrateur, etc.) ;
- gère les accès en fonction des équipements ou groupes d'équipements, des utilisateurs ou groupes d'utilisateurs ;
- autorise la définition d'une durée de validité des comptes ayant accès au système ;

- doit imposer des plages horaires pour l'accès aux équipements en fonction des profils d'administrateur ;
- intègre des mécanismes de haute disponibilité ;
- le cas échéant, permet que l'autorisation d'accès à un équipement soit soumise à l'autorisation, en temps réel, d'un tiers.

### ***Traçabilité***

La fonction de traçabilité de la passerelle d'administration :

- enregistre tout le trafic issu des postes des clients distants et à destination des équipements (raw data et format vidéo) ;
- journalise les événements de connexion (date, heure, volumétrie) de chaque utilisateur ;
- exporte en temps réel les journaux d'événements vers un serveur de journalisation externe ;
- si les journaux sont conservés localement, chiffre les enregistrements de trafic et en assure l'intégrité ;
- peut intégrer une capacité de recherche par mot clé dans les enregistrements (vidéo ou non) et les journaux de logs ;
- est compatible avec les protocoles de journalisation standard (par exemple, SYSLOG, SYSLOG-TLS, SNMPv3, etc.) ;
- permet le contrôle et l'audit du trafic chiffré (par exemple, SSH, SSH -X, RDP, etc.) ;
- intègre une fonction de recherche dans les enregistrements des connexions et les journaux ;
- le cas échéant, fait un horodatage des enregistrements ou peut s'interconnecter avec un système d'horodatage.

### ***Fonctions cryptographiques***

La passerelle d'administration :

- met en œuvre des algorithmes cryptographiques (garantissant CIAD<sup>23</sup>) pour les communications ;
- permet d'interdire les algorithmes obsolètes ou non conformes<sup>24</sup> ;
- autorise l'emploi d'algorithmes de chiffrement entre le client et la passerelle, puis entre la passerelle et l'équipement à administrer ;
- est compatible avec les mécanismes cryptographiques asymétriques (certificats X509 avec gestion des CRL, compatibilité OCSP, etc.).

### ***Fonctions d'administration***

Les mécanismes d'administration de la passerelle d'administration :

- permettent une gestion des utilisateurs ou groupes d'utilisateurs ;
- permettent une gestion des équipements ou groupe d'équipements ;
- permettent de définir des profils d'accès pour chaque utilisateur ou groupe, en fonction des équipements ou groupe d'équipement protégés ;
- intègrent une (des) interface(s) d'administration hors ligne dédiée(s) à l'exploitation de la passerelle ;
- intègrent des fonctions de maintien en condition de sécurité (mises à jour, etc.).

---

23. CIAD : Confidentialité, Intégrité, Authentification, Disponibilité.

24. Cf. les annexes B1, B2 et B3 du RGS.

## Annexe II : Aspects juridiques

---

La sécurité des systèmes d'information passe par des mesures techniques mais également fonctionnelles qui intègrent des obligations pesant sur l'entité, en tant qu'entreprise ou autorité administrative, ou en tant qu'employeur. 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.

L'action de l'administrateur s'intègre dans une obligation plus globale de l'entité de sécuriser le système d'information sur lequel il intervient.

En effet, 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. 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>25</sup>. Le code pénal sanctionne, d'ailleurs, le non-respect de ces dispositions<sup>26</sup>.

D'autres réglementations, sectorielles le cas échéant, peuvent trouver à s'appliquer. À titre d'exemple, l'arrêté du 3 novembre 2014<sup>27</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>28</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>29</sup>.

Enfin, la réglementation européenne est de plus en plus exigeante pour la sécurisation des données

---

25. 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° 2014-299 du 7 août 2014 prononçant un avertissement à l'encontre de la société CA CONSUMER FINANCE (CREDIT AGRICOLE) : « *la formation restreinte retient que les faits précités constituent une atteinte à la confidentialité des données bancaires dont la société ne saurait s'exonérer de sa responsabilité en se retranchant derrière des erreurs humaines.* »

26. Art. 226-17 du code pénal : cinq ans d'emprisonnement et de 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.

27. 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 disponible [ici](#)

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

29. 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.

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>30</sup>.

<b>R70</b>	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 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.

<b>R71</b>	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 agents 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.

<b>R72</b>	L'administrateur doit avoir une action essentielle en matière de sensibilisation des agents. Celle-ci est une des mesures fonctionnelles à prévoir pour la sécurisation du système d'information.
------------	---

<b>R73</b>	Il reviendra à l'administrateur de surveiller l'utilisation des ressources du système d'information pour palier l'éventualité d'un incident.
------------	--

---

30. Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, COM(2013)48 final du 7 février 2013 ; Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM(2012) 11 final du 25 janvier 2012 (et résolution législative du Parlement européen du 12 mars 2014).

## Annexe III : Glossaire

---

À défaut de s'appuyer sur des définitions standardisées et dans un souci de clarté, le glossaire ci-dessous définit les termes qui sont repris dans la présente note technique :

- Zone de confiance : l'objectif d'une zone de confiance est d'isoler ou cloisonner un système, des ressources ou un service par des mesures de protection adaptées au contexte (par exemple le filtrage, le cloisonnement logique de réseau, l'authentification, la mise en œuvre de VPN IPsec) et en fonction du juste besoin opérationnel. De façon à définir ces zones de confiance le plus justement possible, il est nécessaire au préalable de mener une analyse des domaines fonctionnels et techniques à traiter ;
- Domaine fonctionnel : un domaine fonctionnel permet d'identifier un métier ou une activité dans le but de clarifier les périmètres de responsabilité entre plusieurs entités organiques. À titre d'exemple, la *Tierce Maintenance Applicative - TMA* ou l'*administration des réseaux* peuvent être considérées comme deux domaines fonctionnels distincts. Un domaine fonctionnel est composé d'un ou plusieurs domaines techniques ;
- Domaine technique : un domaine technique est un sous-ensemble d'un domaine fonctionnel. Dans contexte de cette note, il représente les matériels ou logiciels nécessaires aux tâches d'administration d'un ensemble de ressources pouvant être confiées à une entité organique bien identifiée ;
- DMZ - Demilitarized Zone : une DMZ est une zone *intermédiaire* qui se situe entre deux réseaux ou systèmes d'information différents. Elle permet de protéger les ressources de la zone de plus haute sensibilité à l'aide d'un certain nombre d'outils de filtrage, voire de serveurs relais ;
- Passerelle : une passerelle consiste en la mise en œuvre d'un ensemble d'équipements matériels et/ou logiciels permettant de rendre un service de relais, associé à des mécanismes de filtrage, en vue d'interconnecter deux systèmes d'information. Ces équipements sont déployés au sein d'un type de DMZ ;
- VLAN : un réseau local virtuel est un réseau logique permettant la commutation de paquets (exclusivement de niveau 2 du modèle OSI<sup>31</sup>), sans fonction de routage ni de filtrage ;
- Ressources d'administration : ce terme désigne la partie du système d'information (SI) dont la fonction est d'effectuer des tâches d'administration sur un autre élément du SI. Elles sont constituées de l'ensemble des dispositifs contribuant aux tâches d'administration : poste d'administration, services et serveurs d'administration, réseaux et interfaces réseau, serveurs relais, passerelles, outils, scripts, etc. ;
- Administrateur : un administrateur est une personne physique chargée des tâches d'administration sur un SI dont les opérations de configuration et de gestion : installation, gestion des configurations, maintenance, évolution du SI administré, supervision ou gestion de la sécurité. Les administrateurs sont en charge d'un ou plusieurs domaines fonctionnels et/ou techniques définis ;
- Administrateur métier, exploitant ou intégrateur : Les administrateurs métier, les exploitants ou encore les intégrateurs sont considérés dans cette note comme des sous-ensembles du groupe des

---

31. Couche « *Liaison de données* » du modèle OSI



administrateurs. Ils désignent des personnes physiques en charge de l'exploitation ou de l'emploi d'un service ou d'une ressource en particulier. Ils disposent de privilèges adaptés à ces fonctions ;

- Superviseur : Un superviseur est une personne physique en charge de la supervision d'un ensemble d'équipements ou d'un système d'information et de la gestion des incidents techniques ou de sécurité. Il exploite le système de supervision mis à sa disposition. Les équipes de supervision ne disposent pas des privilèges d'administration ;
- Connexion à distance : la connexion à distance consiste à se connecter depuis un équipement sur un autre afin d'y ouvrir une session graphique (ex : RDP<sup>32</sup>, ICA<sup>33</sup>, etc.).

---

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

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