PROJET ECP

AP3

CAHIER DES CHARGES

Création d'un système d'information hautement disponible et interconnecté

Propriétés	Description
Intitulé	Fourniture d'un système d'information hautement disponible et d'une connexion inter-sites pour un centre de formation.
Présentation Rapide	Le projet consiste à mettre en place la solution technique sur le réseau de l'entreprise, en intégrant les différents serveurs sur le LAN et en activant les différentes techniques de sécurisation : authentification forte, redondance des services, chiffrement des données, filtrage des services par le firewall
Positionnement	Semestre 1 Semestre 2 Semestre 3 Semestre 4 >>>>
Durée estimée en SEMAINE	10 semaines
Documents joints	Cahier des charges, ANNEXES 1 A 8
Modalités de réception	Présentation d'un système opérationnel – recettage solution stephane.beteta@ecp-apprentissage.fr gabriel.beteta@ecp-apprentissage.fr

Lancement : 01/09/2025 – Fin : 31/12/2025

1) CONTEXTE

1.1) Présentation de l'ECP

L'ECP Apprentissage fait partie du Groupe GEFE (Groupe Europe Formation Education) ; depuis 2020, nous avons pour mission de former les professionnels de demain dans les domaines de l'Immobilier, de l'Assurance et de la Gestion Patrimoniale. Pour cette raison, nous vous apportons les savoir-faire et compétences qui vont vous permettre de rapidement intégrer le monde de l'entreprise dans les meilleures conditions et dans des métiers porteurs.

Nous avons un catalogue de formations, uniquement dispensées en apprentissage. Parce que l'expérience pratique et la théorie se marient à merveille, cette méthode d'alternance vous ouvre les portes des métiers de l'Informatique, l'Immobilier, de l'Assurance et de la Gestion de Patrimoine. Du Bac+2 au Bac+5, nos cursus en BTS, Bachelors (Bac+3) et Mastères (Bac+5) sont des Diplômes d'Etat et des Titres RNCP.

ECP est implantée sur 2 sites à Strasbourg (site Vauban et site Somme).

L'ouverture de 2 nouvelles classes (BTS SIO à Strasbourg), nécessite d'aménager de nouvelles salles informatiques et de répondre à plusieurs critères :

- Cahier des charges technique liés aux référentiels des formations
- Souhait des professeurs, intervenants et des apprenants
- Décisions de la direction générale et informatique
- Règlements et lois

2) Objectifs du projet

2.1) Axes stratégiques à atteindre

La DSI en accord avec la Direction Générale a décidé de lancer un appel d'offres pour la création d'un réseau informatique indépendant, la création et l'équipement de nouvelles salles informatiques.

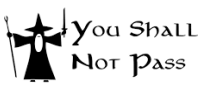
Ce projet doit permettre de mesurer des améliorations sur 4 axes principaux :

1. Amélioration du service aux utilisateurs et faciliter d'administration par la DSI
    a. Création d'un Système d'Information indépendant
    b. Uniformisation du SI
    c. Liaison inter-sites entre les établissements de Strasbourg et Mulhouse
    d. Redondance des services

2. Retour sur investissement par la réduction des coûts de possession et d'exploitation
    d. Facilité d'administration
    e. Documentation complète (installation, configuration, exploitation)

3. Faciliter le travail collaboratif au niveau régional
    g. Partage et accessibilité des données inter-sites (sécurisé et redondé)

4. Sécurité des systèmes et des données
    i. Faciliter la mise en place d'un plan de continuité d'activité (PCA)
    j. Redondance des serveurs, services et des données
    k. Sauvegarde régulière des serveurs



2.2) Objectifs attendues

Chaque groupe devra mettre en œuvre une solution technique répondant aux objectifs suivants :

- Respecter la date de début (01/09/25) et de fin de projet (31/12/25)
- La solution doit être à moindre coût et respecter un budget maximum de 100 000 € HT
- Rendre les livrables et effectuer les soutenances aux dates prévues

1. Etude du projet et réponse au cahier des charges (planning, coûts…)

   - Mise en œuvre des solutions informatiques
   - Equipements (Serveurs)
   - Coût des licences ANNEXES 3 et 4
   - Coût de la main d'œuvre

2. La mise en œuvre d'une liaison WAN inter-sites chiffrée
   - Entre les nouvelles salles informatiques de Strasbourg Vauban et Strasbourg Somme *(IPsec)*

3. Harmoniser le plan d'adressage et de nommage sur l'ensemble des sites
   - Segments réseaux, login, noms d'hôtes, serveurs etc.

   ANNEXES 1 et 2

4. Création de serveurs et rôles/services suivants en <u>haute disponibilité</u> :
   - Annuaire d'authentification (AD)-> SSO
   - Résolution de noms (DNS)
   - Distribution d'IP dynamique (DHCP)
   - Systèmes de fichiers distribués (DFS) et réplica (DFSR) / données utilisateurs
   - Données accessibles via un partage SMB (droits et permissions adaptés)
   - Clichés instantanés (Shadow Copy) du disque contenant les DATAS stockés sur le SAN
   - Sauvegarde complète (Sur un espace disque SAN via un point de montage iSCSI)

5. Accès aux données stockant les dossiers personnels des enseignants et des élèves à partir des 2 sites :
   - Redondances des données
   - Droits et permissions adaptés (*j'accède à mes données, pas à celles des autres)*

6. Création à minima d'1 poste client Windows 11 Pro à Strasbourg Vauban et Somme dans le domaine AD

7. Vous prendrez connaissances des recommandations de l'ANSSI

   ANNEXES 5 à 8

La haute disponibilité (ou High Availability ou HA) permet d'assurer et de garantir le bon fonctionnement des applications ou services procurés, et ce, 24h/24 et 7j/7 ".

L'Active Directory sera l'unique moyen d'authentification et de contrôle des habilitations (droits/permissions) et permettra le déploiement du SSO (Single Sign-On).

2.3) Solution recommandée par la DSI

Informations techniques complémentaires en ANNEXES 1 et 2

Suite à l'Audit réalisée par la DSI ; elle estime qu'il faut au moins 8 serveurs pour la réalisation du projet :

- 2 routeurs
- 4 serveurs de production
- 2 serveurs de sauvegarde

Tableau : Répartition des serveurs et services par sites

SITES	RÔLES / SERVICES
A – Strasbourg Vauban	Active Directory : 1 seule forêt et 4 contrôleurs de domaine (sites A et B) Les clients seront sous Windows 11 Pro 1 routeur/pare-feu avec VPN Inter-sites (IPsec) Serveurs avec les rôles/services suivants : 1er serveur : Principal (WS 2022 Standard GUI) ▪ AD DS, DNS, DHCP, DFS, cible DFSR (Réplica) 2nd serveur : Secondaire (WS 2022 Standard CORE) ▪ AD DS secondaire, DNS secondaire, DHCP de basculement, DFS, cible DFSR (Réplica) 3ème serveur : Serveur NAS/SAN contenant ▪ Espace disque SAN accessible via un point de montage iSCSI, contenant la sauvegarde complète (OS + DATAS) du serveur STG1-SRVW-01 ▪ Clichés instantanés de la partition DATAS sur le même disque ou stockés sur un point de montage iSCSI
B – Strasbourg Somme	1 routeur/pare-feu avec VPN Inter-sites (IPsec) Serveurs avec les rôles/services suivants : 1er serveur : Principal (WS 2022 Standard GUI) ▪ AD DS (connecté à l'AD Strasbourg), DNS, DHCP, DFS, cible DFSR (Réplica) 2nd serveur : Secondaire (WS 2022 Standard CORE) ▪ AD DS secondaire, DNS secondaire, DHCP de basculement, DFS, cible DFSR (Réplica) 3ème serveur : Serveur NAS/SAN contenant ▪ Espace disque SAN accessible via un point de montage iSCSI, contenant la sauvegarde complète (OS + DATAS) du serveur STG2-SRVW01 ▪ Clichés instantanés de la partition DATAS sur le même disque ou stockés sur un point de montage iSCSI

Tableau : Nombre d'utilisateurs estimé

Sites	Utilisateurs	PC Fixes	PC Portables*
Strasbourg	60	40	60
Mulhouse	30	20	30
Total	90	60	90

**avec la multiplication du AVEC / BYOD, il y a potentiellement autant de PC Portables que d'utilisateurs à prendre en compte. On peut également supposer l'utilisation de smartphones/tablettes…*

2.4) Responsabilités

- Le commanditaire fournira à la demande toute information sur le contexte nécessaire à la mise en place de l'infrastructure.
- Le prestataire est à l'initiative de toute proposition technique.
- Le prestataire fournira un système opérationnel sous forme de machines virtuelles
- Le prestataire présentera une maquette

2.5) Transfert de compétences et accompagnement au changement

La prestation dans sa globalité devra être entièrement documentée et un mémoire technique fonctionnel, rédigé impérativement en Français, devra être remis pour chaque élément technique de la solution mis en place. Il pourra être demandé la fourniture de mode opératoire concis pour les utilisateurs.

2.6) Démarche ITIL / Normes ISO 2700x

La DSI de la CCI Grand-Est a initiée une démarche de mise en place des bonnes pratiques de l'informatique basée sur le référentiel ITIL V3. La DSI vise à terme une certification du service sur les normes ISO 20000 et ISO 27000.

Dans ce contexte, la solution mise en place devra faciliter la mise en place de la démarche et permettre d'identifier des indicateurs précis quant au bon fonctionnement des équipements.

3) Groupes et évaluations

3.1) Constitution des groupes

- Chaque groupe sera composé de 2 apprenants
- Le cas échéant, le dernier groupe (à trois ou seul) sera composé sur avis des formateurs
- Chaque apprenant du groupe aura un site affecté dont il sera responsable (A ou B)

SITE A : Apprenant 1, SITE B : Apprenant 2

L'apprenant qui met en œuvre est responsable de la production de la documentation

A l'examen, l'épreuve technique est individuelle, chaque partie de cet AP peut constituer un sujet d'examen

Le jour de l'épreuve, vous pouvez réutiliser vos machines virtuelles et snapshots !
Il est impératif que chacun puisse être autonome et sache réaliser l'ensemble de AP.

3.2) Notations

La notation est individuelle.

- Coeff. 1 pour chaque soutenance, démonstrations techniques, QCM, Badges CISCO et éventuels bonus ou défis individuels
- Coeff. 2 pour chaque production écrite
- Coeff. 3 pour la démonstration technique finale (maquette de l'ORAL-2)

3.3) Planning prévisionnel – 8 Séances

1. Lundi 01/09/2025 matin : **LANCEMENT DU PROJET +** *Présentation des épreuves informatiques à l'examen de BTS SIO / Présentation du sujet / Validation des solutions en séance*
2. Vendredi 05/09/25 matin : Etudes CdC + Maquettage LOT1
3. Vendredi 03/10/25 matin : Livraison du 1er LOT – **MAQUETTAGE LOT1 + QCM1**
4. Vendredi 17/10/25 matin : Séance de travail en groupe
   Lundi 20 octobre 25 : **Livraison du LIVRABLE 1 (avant 23h59)**
5. Vendredi 31/10/25 matin : ORAL 1
6. Jeudi 13/11/25 matin : Réalisation maquette/expérimentation
7. Vendredi 28/11/25 matin : Livraison 2nd LOT- **MAQUETTAGE LOT2 + QCM2**
8. **Mardi 09/12/25 matin :** ORAL 2- MAQUETTE COMPLETE (LOTS 1 à 4)

31/12/25 : **Livraison du LIVRABLE 2 et 3 (avant 23h59)**

Mardi 06/01/26 matin : BTS Blanc – Epreuve technique (sujets AP3)

3.4) Aide à l'ordonnancement des tâches

Aide méthodologique :

1. Lire le sujet
2. Relevé des objectifs pour chaque site (A, et B,)
3. Relevé les dates importantes du projet (Début, Fin, livrables, oraux…)
4. Etudes / Analyse par le groupe (Discussions, échanges, recherches…)
5. Réaliser un agenda partagé et fixer vous des dates de « réunions teams/discord » pour avancer progressivement
6. Découper le projet en objectifs intermédiaires et créer une liste de tâches (Méthode SMART)
7. Evaluer la durée de chaque tâche en heures (Cible 2h par tâches)
8. Définir l'ordre chronologique des tâches (tâches en parallèles ou après qu'une soit terminée)
9. Calculer la planification du projet (combien d'heures, jours ?) et prévoir les marges nécessaires.
10. Créer le planning prévisionnel puis transposer le sur un logiciel de type Gantt Project
11. Editer le diagramme de Gantt du projet
12. Affecter les tâches aux personnes

NB : Vous avez le droit d'organiser des sessions de travail en ligne sous forme de « soutien » / réaliser un travail collaboratif entre les groupes

3.5) Description des lots

- LOT 1 :
  - 2 Routeurs/Pare-Feu avec 1 VPN site à site (IPsec) entre les sites A et B
  - Documentation d'installation et de configuration en V1 du LOT 1

- LOT 2 :
  - 4 serveurs Windows Serveur 2022 Standard avec les rôles suivants fonctionnels et configurés : ADDS, DNS, DHCP et DHCP de basculement
    (2 serveurs sur le Site A et 2 serveurs sur le site B)
  - Documentation d'installation et de configuration en V1 du LOT 2

- LOT 3 :
  - DFS + DFSR (Réplica) fonctionnel sur les quatre serveurs des sites A et B
  - Sauvegarde et Shadow Copy sur un espace de stockage séparé (serveur SAN avec montage iSCSI)
  - Documentation d'installation et de configuration en V1 du LOT 3

- LOT 4 :
  - Appliquer les consignes et GPO de l'Annexe 2
  - Règles de pare-feu configurées (WAN, LAN, VPN et SAN)

3.6) Livrables et Oraux

- Chaque groupe déposera sur le dossier partagé avec les formateurs les différents livrables, dans les délais.
- A chaque séance, il faudra compléter le tableau de suivi partagé avec les formateurs sur Teams.
- Rendre compte de problèmes par courriel aux formateurs ou conversation Teams (avec les deux formateurs invités dans la conversation).

LIVRABLE 1 : PROPOSTION TECHNIQUE ET COMMERCIALE
A RENDRE AVANT LE LUNDI 20 OCTOBRE 2025, 23h59

- Rédaction d'un document de réponse argumentée au Cahier des Charges, selon le modèle proposé : « LIVRABLE_1_Reponse_CDC_GROUPE_X_YYYYMMJJ_HHMM.docx ».

Ce document contiendra à minima :

- La composition et présentation de votre groupe
- Le rappel des besoins et objectifs du projet
- Votre solution argumentée :
  - *Présentation de chaque solution + arguments du choix par rapport au cahier des charges*
  - *Tableau comparatif ou un tableau de synthèse sur des points clés avec des smileys ou coches vertes/rouges afin d'orienter immédiatement vers les points clés et la solution que vous retenez.*
    (Les serveurs Windows étant imposés, il n'est pas demandé une alternative)

- Schéma réseau complet

(Contenant : les pares-feux, serveurs, rôles/fonctionnalités, versions OS et logiciels, noms, adresses IP, équipements réseaux et connexions / liens et toutes informations utiles).

  - *Utiliser plutôt Microsoft VISIO ou un logiciel similaire pour réaliser vos schémas (Draw.io).*

- Budget / Coût du projet
  (Devis et/ou un tableau complet reprenant les différentes ressources (humaines, financières, matérielles) nécessaires à la réalisation de votre projet et le coût global s'approchant du réel).
  - *N'oubliez-pas les licences CAL (Annexe 4)*
  - *Comment est justifié la main d'œuvre ?*

- La liste des tâches prévisionnelle de votre projet

(Lister les tâches dans l'ordre chronologique ; pour vous aider, identifier les tâches que vous pouvez réaliser sans attendre qu'une autre soit terminée)

- Diagramme de Gantt prévisionnel de votre projet
  Spécifiant les tâches, durées et ressources nécessaires
  - *Le diagramme de Gantt doit permettre de déterminer le temps nécessaire à la réalisation du projet et son ordonnancement.*
  - *Combien de jours/heures sont nécessaires ? -> coût de la main d'œuvre*

ORAL 1 : LE VENDREDI 31 OCTOBRE 2025, 8h30

- PHASE 1 - PRESENTATION ORALE : 15 minutes
  10 minutes de présentation puis 5 minutes de questions / réponses
  Le diaporama sera déposé dans le dossier partagé avec les formateurs

Chaque groupe présentera aux formateurs sa réponse au cahier des charges à l'aide d'un support projeté selon le modèle proposé « ORAL_1_Reponse_CDC_GROUPE_X_YYYYMMJJ_HHMM.pptx »

Le contenu reprendra les éléments du livrable 1, bien que complet, cela doit être concis pour respecter le temps.

ORAL 2 : LE MARDI 09 DECEMBRE 2025, 8h30

- PHASE 1 - PRESENTATION ORALE : 15 minutes
  10 minutes de présentation puis 5 minutes de questions / réponses
  Chaque groupe présentera à l'oral son rapport de clôture de projet, à l'aide d'un support projeté, selon le modèle proposé « ORAL_2_Rapport_de_cloture_du_projet_GROUPE_X_YYYYMMJJ_HHMM .pptx »

  Ce sera une synthèse qui permettra d'évoquer les écarts entre les éléments prévisionnels de votre livrable 1 et la réalité.

- PHASE 2 - DEMONSTRATION TECHNIQUE : 30 minutes
  Chaque groupe présentera techniquement la solution validée dans le Livrable 1.

  Les maquettes devront permettre aux formateurs de vérifier le bon fonctionnement de l'ensemble de la solution ainsi que la cohérence des éléments entre eux dans la solution.

LIVRABLES 2 et 3 : FICHE DE SITUATION PROFESSIONNELLE N°1 ET DOCUMENTATION TECHNIQUE A RENDRE AVANT LE MARDI 31 DECEMBRE 2025, 23H59

Ces livrables au format éditable devront être partagés dans le groupe pour être réutilisés ultérieurement

- « LIVRABLE_2_GROUPE_X_Fiche_situation_professionnelle_1_BTS-SIO 2025 ».
  - Reprise du livrable 1 et tenir compte des remarques et demandes de modifications
  - Analyse prévisionnel vs réel / Conclusion et améliorations possibles du projet

- « LIVRABLE_3_ GROUPE_X _Documentation_technique_situation_professionnelle_1_BTS-SIO 2025 »
  - Documentation technique complète du projet à la façon d'un mode d'emploi, rédigée et mise en forme à rendre sous format électronique .DOCX et .PDF, obligatoire.

La documentation est autorisée à l'examen technique et peut-être demandée à l'examen « oral pro »

3.7) Pénalités et Bonus

- Les productions à livrer (déposer) sur le dossier partagé avec les formateurs ont des dates de remise à respecter.

- Chaque jour de retard entraîne le retrait d'1 point sur 20 par jour.

- La remise en retard des livrables 2 et 3 seront sanctionnés d'un 0/20 (Date de fin du projet).

- La remise aux formateurs des attestations de réussite des MOOC suivants seront comptabilisés (note sur 20 coeff. 1, pondéré selon le volume horaire théorique).

CISCO : S'inscrire/être authentifié avec son adresse électronique personnelle ou réutiliser un compte existant avant de cliquer sur les liens.

P1 : Introduction à la Cybersécurité /rapide 6h
https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=fr-FR&instance_id=8a0c0dbf-6bfd-4246-bede-8b4a4aef7ea7

P2 : CCNA1 : Présentation des réseaux
https://www.netacad.com/courses/ccna-introduction-networks?courseLang=fr-FR&instance_id=c7b77b94-ba98-4b06-86dd-da50987b3798

P3 : Principes de cybersécurité
https://www.netacad.com/courses/cybersecurity-essentials?courseLang=fr-FR&instance_id=1fd2a67c-d8de-4f78-811f-2ec6689dc817

P4 : CCNA2 : Switching, Routing, and Wireless Essentials (SRWE)
https://www.netacad.com/courses/ccna-switching-routing-wireless-essentials?courseLang=fr-FR&instance_id=4071adba-3b66-495f-bc55-662ffc6934c5

Rapide / ½ journée :

https://secnumacademie.gouv.fr/

https://atelier-rgpd.cnil.fr/

ANNEXES

ANNEXE 1 : SPECIFICATIONS TECHNIQUES

ANNEXE 2 : CONSIGNES AD ET GPO

ANNEXE 3 : LICENCES CLIENTS WINDOWS

ANNEXE 4 : LICENCES SERVEURS 2016 ET CAL + DOCS-MICROSOFT.zip

ANNEXE 5 : RECOMMANDATIONS DE SECURITE RELATIVES A IPSEC, ANSSI

ANNEXE 6 : RECOMMANDATIONS DE SÉCURISATION D'UN PARE-FEU STORMSHIELD NETWORK SECURITY, ANSSI

ANNEXE 7 : RECOMMANDATIONS DE SECURITE RELATIVES AUX MOTS DE PASSE, ANSSI

ANNEXE 8 : RECOMMANDATIONS À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION, ANSSI

SITOGRAPHIE

https://www.ecp-apprentissage.fr/

https://gefe-strasbourg.fr/

https://www.ssi.gouv.fr/administration/bonnes-pratiques/

OUTILS

https://trello.com

https://www.notion.so/fr-fr/product/projects

ANNEXE 1
Indications techniques des machines virtuelles
(À adapter…)

SITE A (VMNET1)

PLAN D'ADRESSAGE :

SITE A : 192.168.100.0 /24 (LAN)

RTE-STG01 : 512 Mo RAM – FreeBSD Unix – Pfsense / OPNsense

- 1 disque de 20 Go
- 3 interfaces Ethernet :
  - WAN = VBR01
  - LAN = AP3-TRIGRAMME-ELEVE
  - SAN = SAN-ELEVE / réservé réseau local pour liaison/montage iSCSI
- VPN SITE A vers SITE B

STG-SRVW01 : 2 Go RAM - Microsoft Windows 2022 Standard (GUI)

- 2 disques durs :
  - 1 disque de 60 Go (OS)
  - 1 disque de 60 Go (DATAS01)
- SMBV3 à activer (chiffrement à démontrer avec une analyse de trames Wireshark)
- Serveur Active Directory (contrôleur principal du domaine)
- Serveur de fichiers racine (Espace de Noms DFS) et Réplica (DFSR)
  - Clichés instantanés DATAS01
  - Fonctionnalité déduplication de fichiers DATAS01
- Partage réseau DATAS01
- Montage du disque iSCSI Backup01 (STG-SAN01) / sauvegarde complète de STG-SRVW-01
  (Possibilité de déplacer les clichés instantanés sur la cible iSCSI également)
  (Option) sécurisation d'accès/montage de la cible iSCSI avec un mot de passe ou IPSEC

STG-SRVW02 : 1 Go RAM - Microsoft Windows 2022 Standard (CORE)

- 2 disques durs :
  - 1 disque de 60 Go (OS)
  - 1 disque de 60 Go (DATAS02)
- Serveur Active Directory (contrôleur supplémentaire)
- Serveur de fichiers (Espace de Noms DFS) et Réplica (DFSR)
- Partage réseau DATAS02

STG-SAN01 : 512 Mo RAM
(Attention aux versions récentes de TrueNas gourmandes en mémoire vive. D'autres solutions sont envisageables, 1 serveur Windows Core supplémentaire avec diffusion de cible iSCSI. Ou bien encore… Xpenology / RR / /Veeam Backup….

- 1 disque de 20Go
- ISCSI services : Backup01

Attention, pour les sites A et B.

- La version de Windows Serveur doit être identique sur l'ensemble des serveurs
- Active Directory : 1 seule foret, 1 contrôleur de domaine principal, 3 contrôleurs de domaine supplémentaires.
- DFS : 1 espace de nom « INTRANET » accessible à :
  - \\IEF.LOCAL\INTRANET ou \\IEF.LOCAL\DFS\INTRANET
- 4 cibles DFSR (les données seront répliquées en maille pleine et accessibles à partir des 4 cibles) :
  - \\STG-SRVW-01\DATAS01
  - \\STG-SRVW-02\DATAS02
  - \\STG2-SRVW-01\DATAS03
  - \\STG2-SRVW-02\DATAS04

SITE B (VMNET2)

PLAN D'ADRESSAGE :

SITE B : 192.168.200.0 /24 (LAN)

RTE2-STG01 : 512 Mo RAM – FreeBSD Unix – Pfsense / OPNsense

- 1 disque de 20 Go
- 3 interfaces Ethernet :
  - WAN = VBR01
  - LAN = AP3-TRIGRAMME-ELEVE
  - SAN = SAN-ELEVE / réservé réseau local pour liaison/montage iSCSI
- VPN SITE B vers SITE A

STG2-SRVW01 : 2 Go RAM - Microsoft Windows 2022 Standard (GUI)

- 2 disques durs :
  - 1 disque de 60 Go (OS)
  - 1 disque de 60 Go (DATAS03)
- SMBV3 à activer (à démontrer avec une analyse de trames Wireshark)
- Serveur Active Directory (contrôleur supplémentaire)
- Serveur de fichiers (Espace de Noms DFS) et Réplica (DFSR)
  - Clichés instantanés DATAS03
  - Fonctionnalité déduplication de fichiers DATAS03
- Partage réseau DATAS03
- Montage du disque iSCSI Backup02 (STG2-SAN01) / sauvegarde complète de STG2-SRVW01
  (Possibilité de déplacer les clichés instantanés sur la cible iSCSI également)
  (Option) sécurisation d'accès/montage de la cible iSCSI avec un mot de passe ou IPSEC

STG2-SRVW02 : 1 Go RAM - Microsoft Windows 2022 Standard (CORE)

- 2 disques durs :
  - 1 disque de 60 Go (OS)
  - 1 disque de 60 Go (DATAS04)
- Serveur Active Directory (contrôleur supplémentaire)
- Serveur de fichiers (Espace de Noms DFS) et Réplica (DFSR)
- Partage réseau DATAS04

STG2-SAN01 : 512 Mo RAM

(Attention aux versions récentes de TrueNas gourmandes en mémoire vive. D'autres solutions sont envisageables, 1 serveur Windows Core supplémentaire avec diffusion de cible iSCSI. Ou bien encore Xpenology / RR / /Veeam Backup….

- 1 disque de 20Go / iSCSI services : Backup02

ANNEXE 2 : CONSIGNES AD ET GPO

- Vous installerez Microsoft Windows 2022 Serveur Standard en mode GRAPHIQUE / GUI en tenant compte des informations suivantes :

Nom d'hôte : Voir annexe 1 ;
Nom de la société : IEF ;
Organisation : IEF ;
Disques durs / partitions : Voir annexe 1
Nombre de connexions simultanées : 100 ;
Adresses IP : Voir annexe 1
Password Administrateur recommandé dans le cadre de l'AP : P@ssword10

Nom de domaine : IEF.

Nom de domaine FQDN : IEF.LOCAL

Le mot de passe de restauration d'AD doit être identique à celui de l'administrateur *(recommandé dans le cadre de l'AP)*

Nom de zone DNS : IEF.LOCAL
Le serveur DNS devra être capable de résoudre les noms DNS de tous les hôtes du réseau. La/les station(s) seront membres de ce domaine.

- Créez les objets suivants :

  - Unités Organisationnelles nommée VAUBAN et SOMME
  - Les comptes utilisateurs : Paul, Pierre placés dans l'UO VAUBAN
  - Les comptes utilisateurs : Isabelle, Nathalie placés dans l'UO SOMME
  - Un compte utilisateur ADMIN (Administrateur de secours)
  - Un groupe nommé GRP1, auquel appartiennent Paul et Pierre seront membres ;
  - Un groupe nommé GRP2, dans lequel Isabelle et Nathalie seront membres ;

Seuls les comptes ADMIN et ADMINISTRATEUR ont tous les privilèges.

- La politique de mots de passe sera la suivante :
(Plus pratique pour les AP sinon se référer aux recommandations de l'ANSSI)

- Longueur de 12 caractères minimum, avec au minimum 1 chiffre, 1 caractère spécial, 1 majuscule.
- Verrouillage du compte utilisateur pendant 30 minutes après 3 tentatives de mot de passe erroné

- Créez une infrastructure réseau avec un seul et unique partage de type (utilisé pour DFS/DFSR) \\IEF.LOCAL\intranet

  - Créer les dossiers GRP1, GRP2, TRANSFERT situés dans le répertoire INTRANET avec les dossiers personnels des utilisateurs en respectant le cahier des charges au niveau des droits et permissions.
  - Tous les utilisateurs auront les droits lecture/écriture sur le partage TRANSFERT.
  - Seuls les membres du groupe « Administrateurs du Domaine » auront le droit contrôle total sur tous les partages.

- Une stratégie de groupe affectera par défaut à tous les comptes de l'AD, les paramètres suivants :

- Création du lecteur réseau U: sur le répertoire personnel de chaque utilisateur (%username%)
- Création du lecteur réseau T: sur le répertoire TRANSFERT
- Déploiement d'un fond d'écran unique et bloquer sa personnalisation
- Redirection des dossiers Mes documents et Bureau vers le dossier personnel de l'utilisateur

Exemple : Dossier documents redirigé vers \\ief.local\intranet\users\%USERNAME%\

- Une stratégie de groupe affectera uniquement les utilisateurs :
  - Interdiction d'accès au panneau de configuration
  - Bloquer les ports USB
  - Masquer **et** bloquer les accès aux disques locaux des postes
  - Bloquer l'accès aux consoles Powershell et Invité de commande

Informations sur les Licences :

"Le nouveau modèle de licence inclut obligatoirement des licences par cœurs + des Licences d'Accès Client (CALs). Chaque utilisateur et/ou appareil accédant une licence de Windows Server 2016 édition Standard ou Datacenter a besoin d'une CAL Windows Server."

Il est bien nécessaire d'acheter des licences CAL (par utilisateur ou par device) en plus des licences Serveur et Windows 10. Confirmation de Microsoft par téléphone, 09 70 01 90 90 (support/infos gratuit)

Licence CAL par utilisateur : environ 50€/users et 40€/Device

Il n'y a pas d'installations à faire, c'est une simple "règle morale", il faut prouver l'achat en cas de contrôles (sauf licences CAL RDS).

Nota bene :

- Il existe également des CAL pour SQL Serveur, Exchange, Link, SharePoint... et bien sur RDS. (En supplément à chaque fois...)

ANNEXE 3 : LICENCES CLIENTS WINDOWS

1) LICENCE RETAIL

La **licence Retail** de Windows est la licence la plus chère mais aussi la moins restrictive.

Licence Retail ou FPP de Windows 10 vendue à 129,99€ sur Amazon (le 02/03/2016)

Avec la **clé de produit fournie**, vous pouvez installer Windows sur n'importe quel PC.

Vous pouvez **changer tous les composants de votre ordinateur actuel** (carte mère, disque dur…) sans aucun souci, même si une réactivation de Windows sera parfois nécessaire (surtout si vous changez un composant essentiel comme la carte mère).

La **licence Retail** n'est pas liée au matériel comme la licence OEM (voir ci-après) mais à l'utilisateur. Vous devez par contre respecter la licence d'utilisation à savoir **une licence par poste**. Vous ne pouvez pas utiliser votre clé de produit pour installer et activer Windows sur plusieurs PC en même temps : **votre licence doit être installée sur un seul PC à la fois**. Si vous tentez d'installer et d'activer Windows avec votre clé de produit sur un second PC, Windows ne sera plus activé sur le premier PC.

La **licence Retail** peut s'acquérir de deux façons différentes. Première façon : en **achetant la version boîte (Full Packaged Product ou FPP) de Windows** chez un revendeur agréé. La boîte contient le support d'installation de Windows (une clé USB ou un DVD d'installation), le guide produit

(ou le manuel d'utilisation), la clé de produit ainsi que la licence d'utilisation. Deuxième façon : **en achetant et en téléchargeant la version digitale (téléchargement) de Windows** chez un revendeur agréé (le Store de Microsoft, Amazon, Materiel.net…). Vous recevrez alors un e-mail de confirmation contenant les détails de votre commande ainsi que votre clé de produit.

Contenu de la version Retail ou FPP de Windows 10 Pro – Source : https://youtu.be/05vl06yMdRQ

L'**activation de votre licence Retail** se fait directement dans Windows, par internet ou avec un ID de confirmation que vous obtenez par téléphone. Une **nouvelle activation** sera nécessaire si vous changez de carte mère et/ou de disque dur sur votre machine.

En cas d'incident technique de Windows, le **support** de Windows est effectué par Microsoft.

LICENCE « MISE A JOUR »

La **licence « Mise à jour »** est identique à la licence Retail à la différence près qu'elle est uniquement utilisable **en mettant à jour une version précédente de Windows, dite « qualifiante »**. Si vous achetez une licence « Mise à jour », vous devrez donc lancer le programme d'installation de Windows depuis une **version précédente de Windows déjà installée et activée.**

Par exemple, pour installer et activer Windows 8 en version « mise à jour », vous devez lancer l'installation directement depuis Windows XP, Windows Vista ou Windows 7. Peu importe que cette version qualifiante soit une version OEM, une version boîte ou elle-même une version « mise à jour ». Si vous lancez l'**installation de cette version « mise à jour » sur une partition vierge** (en démarrant directement sur le DVD ou la clé USB d'installation au démarrage du PC par exemple), l'activation de Windows ne fonctionnera pas.

Licence « Mise à jour » de Windows 8 vendue à 130,00€ sur Amazon (le 02/03/2016)

Licence Retail ou FPP de Windows 8 Pro vendue à 279,99€ sur Amazon (le 02/03/2016)

Les **termes d'utilisation** sont les mêmes que la licence Retail : vous pouvez transférer votre licence sur n'importe quel autre PC, tant que cette licence est installée sur 1 PC à la fois. Niveau prix, elle se situe entre la licence Retail et la licence OEM. Elle a été lancée pour permettre aux possesseurs d'une licence d'une ancienne version de Windows de monter en version à moindre coût. La licence « Mise à jour » est en tout point **identique à la licence Retail**, seul le mode opératoire de l'installation diffère.

Point important, vous ne **pouvez pas réutiliser l'ancienne licence** (celle de la version qualifiante de Windows) sur un autre PC. Exemple : vous installez Windows 7 en version Retail sur votre PC, puis vous le mettez à jour en installant Windows 8.1 en version « Mise à jour » : vous ne pourrez pas utiliser votre clé de produit Windows 7 sur un autre PC.

2) LICENCE OEM

La **licence OEM** (Original Equipment Manufacturer) de Windows est la licence la moins chère mais aussi la plus restrictive. D'une manière générale, la **licence OEM est destinée aux assembleurs** (entreprises qui fabriquent des PC sur-mesure comme HP, Asus, Lenovo… ou le magasin d'informatique en bas de chez vous) et aux intégrateurs système : elle permet de fournir un Windows préinstallé à moindre coût lors de la vente d'une configuration complète.

Lorsque vous **achetez un PC préinstallé avec Windows**, vous avez donc dans 99% des cas une **licence OEM de Windows**.

Néanmoins, en tant que **particulier**, vous avez aussi la possibilité de vous procurer une **licence OEM**.

Licence OEM de Windows 10 Famille vendue à 119,99€ sur Amazon (le 02/03/2016)

Le **gros point noir de la licence OEM** (qui explique son prix réduit) est qu'elle est **liée à vie** à votre machine, il est donc **impossible de déplacer la licence sur un autre PC**. Si vous avez acheté une licence OEM de Windows dans le commerce, c'est après avoir activé Windows par Internet ou par téléphone avec la clé de produit fournie que le lien est définitivement fait entre votre PC et votre licence OEM.

Vous pouvez **changer tous les composants de votre PC** sans devoir acheter une nouvelle licence, sauf si vous changez de disque dur (uniquement pour les licences OEM:SLP) ou si vous changez de carte mère : dans ces cas précis, Windows ne sera plus activé. Mais alors que se passe-t-il si votre carte mère ou votre disque dur tombe en panne ? Si vous avez acheté un PC où Windows était préinstallé, vous devez contacter le support technique du fabricant de votre PC (HP, Lenovo, Dell…) afin de procéder à un remplacement du composant (disque dur – uniquement pour les licences OEM:SLP – ou carte mère) pour **préserver votre licence OEM de Windows**.

Il existe 4 types de licences OEM, chacune proposant une méthode d'activation différente :

1. La **licence OEM:DM** : c'est la licence que vous avez si vous avez acheté un **PC de marque** préinstallé avec **Windows 8, 8.1 ou 10**. Vous avez une étiquette Microsoft authentique (*Genuine Microsoft Label* ou GML) apposée sur votre appareil. Vous n'avez **pas de clé de produit**. A la place, une clé SLP (*System Locked Pre-installation*) est enregistrée dans la table ACPI **MSDM** (Microsoft Digital Marker) du firmware UEFI de votre carte mère, qui est

automatiquement lue par le programme d'installation de Windows. Vous n'avez donc pas besoin d'entrer de clé de produit lors d'une éventuelle réinstallation de Windows.

2. La **licence OEM:SLP** : c'est la licence que vous avez si vous avez acheté un **PC de marque** préinstallé avec **Windows XP, Vista ou 7**. Vous avez une étiquette de certificat d'authenticité Microsoft (*Certificate of Authenticity* ou COA) apposée sur votre appareil. Une **clé de produit est imprimée** sur l'étiquette COA mais ce n'est pas cette clé de produit qui est utilisée en premier lieu pour activer Windows ! Voici comment votre licence Windows s'active : une clé SLP (*System Locked Pre-installation*) et un certificat OEM sont enregistrés dans la table ACPI **SLIC** du BIOS de votre carte mère. Cette clé SLP et ce certificat OEM sont comparés à la clé de produit et au fichier certificat OEM installés dans Windows ; si c'est les deux « match », l'activation de Windows est validée. La clé de produit sur l'étiquette COA est uniquement fournie si une réinstallation de Windows est nécessaire et que pour une raison ou une autre, l'activation hors-ligne de Windows via le SLP ne fonctionne pas. Dans ce cas, les utilisateurs devront activer Windows manuellement par téléphone en utilisant la clé de produit sur l'étiquette COA. Vous activez alors votre **licence OEM:COA** de Windows.

3. La **licence OEM:COA** : c'est la licence que vous avez si vous avez acheté un **PC de marque** préinstallé avec **Windows XP, Vista ou 7**, **et** lorsque vous avez utilisé la clé de produit imprimée sur l'étiquette COA (voir le point précédent pour plus d'informations).

Étiquette de certificat d'authenticité (COA) de Windows 10

4. La **licence OEM:NONSLP** (Non System Locked Pre-installation) : une clé de produit vous est fournie, comme pour la licence Retail. L'activation de Windows doit être faite par l'utilisateur soit par Internet ou par téléphone.

D'un point de vue fonctionnalités, la **version OEM est strictement identique à la version Retail**. Les **clés de produit OEM:DM et OEM:SLP** sont les seules clés capables d'activer Windows hors-ligne, sans avoir besoin de contacter les serveurs de Microsoft. Elles sont seulement utilisées par les fabricants de PC de grande marque comme Asus, Dell, HP…

En cas d'incident technique de Windows, le **support** est assuré par le constructeur du PC ou le revendeur de la licence et non par Microsoft.

Informations concernant les copies OEM (Extrait de l'Annexe 4)

Réimager consiste à copier des logiciels sur différents appareils à partir d'une même image standard. Si une entreprise souhaite récupérer son système à l'aide d'un support OEM ou d'images personnalisées fournies par l'OEM, les restrictions suivantes s'appliquent :

- Le support de récupération fourni par l'OEM peut être utilisé pour copier une image sur un appareil particulier.
- Le support de récupération OEM (1) doit correspondre à la version du produit initialement préinstallé sur le système (2) ne peut être utilisé que pour imager les appareils avec lesquels il a été fourni et (3) ne peut être modifié avant la copie d'une image de récupération sur l'appareil.

Copie d'image depuis le support OEM. Le support OEM (y compris les images OEM personnalisées) peut être utilisé pour réimager les appareils, mais uniquement si la première installation a été faite avec ce support.

3) LICENCE EN VOLUME (VL)

Microsoft vend des **clés de licence en volume** (VLK ou Volume Licensing Key) pour les organisations et les entreprises qui ont besoin d'installer et d'activer Windows sur plusieurs machines en même temps.

Quel est l'intérêt d'une licence en volume ?

Pour bien comprendre, mettons-nous à la place d'un administrateur : nous devons installer une copie identique de Windows sur l'ensemble des machines de notre parc informatique et en plus activer Windows sur chacune de ces machines. Pour gagner du temps, il serait bon d'avoir un **outil de déploiement automatique** pour installer et activer cette copie identique de Windows – configurée selon la stratégie de l'entreprise – depuis notre serveur sur l'ensemble des postes clients. Les services de déploiement Windows (WDS ou Windows Deployment Services) répondent justement à ce besoin. Grâce aux WDS, l'administrateur va pouvoir **déployer une image (ou copie) identique de Windows** sur l'ensemble des postes clients !

Comment obtenir cette licence en volume ?

D'abord, il faut que l'administrateur achète pour son serveur une **licence OEM ou Retail de Windows**. C'est une étape obligatoire. Malheureusement, avec une licence OEM ou Retail, l'administrateur n'a pas le droit des créer une image (ou copie) de Windows, c'est écrit dans la licence d'utilisation. Impossible donc d'utiliser les **services de déploiement Windows**(WDS) pour déployer notre image de Windows sur l'ensemble des postes clients. Une **licence en volume** permet en revanche d'utiliser les WDS !

Toutefois, les licences OEM Windows 10 Pro existent, effectuer un sysprep est également possible. Une fois l'installation effectuée sur chaque machine, les licences OEM sont reconnus et activés via Internet.

Comment se passe l'activation de Windows sur les postes clients ?

Avec **une licence en volume**, les postes clients n'ont pas besoin d'activer Windows par internet ou par téléphone. A la place, l'administrateur peut utiliser un **service d'activation local** au sein de son réseau appelé le service de gestion des clés ou KMS (Key Management Service). Le KMS est **obligatoire** pour activer plus de 25 machines sur son réseau. En choisissant l'**activation KMS**, l'administrateur installe donc un **service KMS** sur le serveur. Dès lors, c'est lui qui va servir de serveur d'activation pour les postes clients : il remplace le serveur d'activation de Microsoft que nous – les particuliers – utilisons pour activer Windows. Toutes les machines activées via le service KMS doivent être réactivées de façon périodique 2 fois par an, tous les 180 jours.

Si l'administrateur veut activer moins de 25 machines, il peut choisir **clé d'activation multiple (clé MAK)** au lieu du service KMS : chaque ordinateur se connecte alors séparément et en une seule fois au serveur d'activation de Microsoft pour activer Windows.

Comment ça marche ?

En achetant une **licence en volume**, l'administrateur aura accès à une image ISO spéciale de Windows. Cette ISO spéciale contient une version de Windows qui n'a pas besoin de clé de produit. C'est cette image ISO qui sera déployée sur les postes clients.

L'administrateur aura aussi accès à une clé de produit spéciale : une **clé de produit KMS**, lui permettant d'**activer le serveur KMS**. Une seule activation est nécessaire auprès de Microsoft : une fois le serveur KMS activé, il n'y aura plus **aucune communication** entre les postes clients et le serveur KMS d'un côté et Microsoft de l'autre. L'administrateur déploie alors son image ISO de Windows sur l'ensemble des postes clients. Une fois qu'un client est installé, il scanne le réseau à la **recherche du serveur KMS** et s'active grâce à lui. Une fois activé, les clients possèdent une licence de Windows valide, du moment que l'activation est renouvelée 2 fois par an (180 jours) avec le **service KMS**.

4) LA METHODE D'ACTIVATION PAR LICENCE NUMERIQUE

A la sortie de Windows 10, une nouvelle méthode d'activation a vu le jour : la **licence numérique** (appelée « droit numérique » dans Windows 10 version 1511). Contrairement à la méthode d'activation traditionnelle où l'on saisit une clé de produit pour activer Windows, ici l'activation de Windows se fait uniquement par internet et évite d'avoir à saisir une clé de produit.

Une **licence numérique** de Windows 10 sera attribuée à votre PC dans les cas suivants :

- En faisant la mise à niveau gratuite vers Windows 10 depuis une copie authentique de Windows 7 ou Windows 8.1 **(cette offre n'est plus disponible)**
- En faisant la mise à niveau vers Windows 10 (version 1511 ou supérieure) et après avoir activé votre copie de Windows 10 à l'aide d'une clé de produit Windows 7, Windows 8 ou Windows 8.1
- En achetant une copie authentique de Windows 10 dans le Windows Store et après avoir activé votre copie de Windows 10
- En achetant une mise à niveau vers Windows 10 Pro dans le Windows Store et après avoir activé votre copie de Windows 10
- En étant Windows Insider et en faisant la mise à niveau gratuite vers Windows 10 Insider Preview depuis une copie authentique de Windows 7 ou Windows 8.1, ou depuis Windows 10 Preview **(cette offre n'est plus disponible)**

Comment fonctionne la procédure d'activation par licence numérique ?

C'est simple : après la première installation de Windows 10 et lors de la première activation de Windows, un **code d'identification unique** est généré pour identifier votre machine (PC de bureau, PC portable, tablette, etc.). Pour créer ce code unique, Microsoft se base sur l'ensemble de votre configuration matérielle (carte mère, disque dur, processeur…). Grâce à lui, **Microsoft attribue à votre machine une licence numérique de Windows 10** dans sa base de données. Si vous refaites une installation « propre » de Windows 10 sur votre PC, lors de l'activation de Windows, Microsoft recherchera le code d'identification unique de votre machine et vérifiera s'il est lié à une licence

numérique de Windows 10 ou non. Si c'est le cas, Windows 10 sera activé. Ce code d'identification unique étant stocké sur les serveurs de Microsoft, l'**activation se fait exclusivement par internet**.

Que se passe-t-il si je change ma configuration matérielle ?

Deux cas de figure se présentent :

1. Si vous avez une **licence Retail de Windows 10** (en ayant acheté directement Windows 10 en boite ou via le Windows Store, en ayant fait la mise à jour gratuite vers Windows 10 depuis une licence Retail de Windows 7/8.1 ou en activant Windows 10 avec une clé de produit de Windows 7/8.1 en version Retail), votre Windows ne sera certainement plus activé mais il suffit de **relancer le processus d'activation** pour qu'il le soit de nouveau.
2. Si vous avez une **licence OEM de Windows 10** (en ayant acheté un PC préinstallé avec Windows 10 ou en ayant fait la mise à jour gratuite vers Windows 10 depuis une licence OEM de Windows 7/8.1) : comme votre licence Windows 10 est liée à votre code d'identification unique qui est basé sur l'ensemble de votre configuration matérielle actuelle, si vous changez un composant essentiel de votre configuration (carte mère ou disque dur), **Windows 10 ne sera plus activé**. En modifiant un composant de votre système, vous obtiendrez un **nouveau code d'identification** qui lui, n'est pas lié à votre licence Windows 10. Pour réactiver Windows 10, vous devrez obligatoirement contacter le support client de Microsoft.

5) FAQ SUR LES LICENCES WINDOWS

Je n'ai pas ou plus de support d'installation de Windows (clé USB ou DVD d'installation), le fabricant de mon PC ne m'en a pas fourni : comment faire si je veux réinstaller Windows ?

Plusieurs solutions :

- Utilisez la partition de restauration installée par le fabricant sur le disque dur pour faire une restauration d'usine du PC

- Créez un DVD ou une clé USB de restauration grâce au logiciel installé par le fabricant dans Windows. Cela vous permettra aussi de faire une restauration d'usine du PC
- Créez votre propre DVD ou clé USB d'installation de Windows (cliquez ici pour savoir comment créer un support d'installation de Windows 10, 8.1 ou 7)

Rapidement, quelles sont les différences entre une licence Retail et une licence OEM ?

Les licences OEM de Windows sont identiques aux licences Retail à l'exception des points suivants :

- Les licences OEM n'offrent pas le support de Microsoft, avec l'assistance des techniciens de Microsoft. En cas de problème technique avec Windows, il faut vous tourner vers le support du fabricant de votre ordinateur
- Les licences OEM sont attachées définitivement au tout premier PC sur lequel Windows est installé et activé
- Les licences OEM permettent la mise à jour de tout composant matériel, à l'exception d'un modèle différent de carte mère et de disque dur
- Les licences OEM ne peuvent pas être utilisées directement pour mettre à jour une ancienne version de Windows

J'ai la version 32 bits de Windows qui est installée sur mon PC. Est-ce que je peux réinstaller Windows en version 64 bits ?

Une licence OEM peut être utilisée pour installer une version 32 bits ou 64 bits de Windows. Si vous avez acheté un PC préinstallé avec une version 32 bits de Windows Famille, vous pouvez réinstaller Windows 10 Famille dans sa version 64 bits. Le contrat de licence accorde le droit d'installer votre version Windows quel que soit sa version, 32 bits ou 64 bits.

Puis-je revendre la clé de produit d'une licence OEM ?

Non ! Vous devrez revendre le PC au complet et pas seulement la licence, étant donné que la licence est liée à vie au PC.

Est-ce que je peux activer ma licence OEM en utilisant un DVD ou une clé USB d'installation de Windows depuis un ISO que j'ai téléchargé sur internet ?

Oui !

Comment savoir si j'ai une licence OEM ou une licence Retail ?

Appuyez simultanément sur les touches Windows + Pause pour ouvrir le panneau *Système*du Panneau de configuration. Descendez-en bas de l'écran et repérez la ligne **ID de produit**.

L'ID du produit devrait être sous la forme xxxxx-xxx-xxxxxxx-xxxxx. Repérez les 3 caractères du second groupe : si ces 3 caractères sont « OEM », c'est que vous avez une **licence OEM de Windows**.

Puis-je rétrograder ma version de Windows vers une version antérieure ?

Oui, les licences OEM de certaines versions de Windows sont éligibles à la **rétrogradation** :

- **Windows 10 Professionnel** permet de rétrograder vers Windows 8.1 Professionnel ou Windows 7 Professionnel

- **Windows 8.1 Professionnel** permet de rétrograder vers Windows 7 Professionnel ou Windows Vista Professionnel
- **Windows 7 Professionnel** et **Windows 7 Édition Intégrale** permettent de rétrograder vers Windows Vista Professionnel, Windows Vista Édition Intégrale, Windows XP Professionnel, Windows XP Édition Tablet PC ou Windows XP Édition x64

Dois-je vraiment activer Windows ?

L'activation de Windows est **obligatoire** sauf pour les PC achetés chez un fabricant de grande marque (Asus, Lenovo, Packard Bell…) qui ont des licences OEM pré-activées, et les licences en volume (VL). Vous avez 30 jours pour activer Windows par internet ou par téléphone après l'installation de Windows. Vous pouvez activer Windows autant de fois que vous le voulez : le nombre d'activation par internet est limitée, au contraire de l'activation par téléphone qui est illimitée.

Puis-je utiliser ma clé de produit sur plusieurs PC en même temps ?

Non, les termes de la licence stipulent que la clé de produit ne peut être utilisée que sur un PC à la fois.

Je compte changer la configuration matérielle de mon PC, est-ce que je vais devoir réactiver Windows ? Ma licence sera-t-elle toujours valide ?

Si vous avez une **licence Retail**, après la mise à niveau de votre configuration matérielle, vous aurez simplement à **relancer le processus d'activation** pour activer Windows. Si vous avez une **licence OEM** en revanche, c'est plus compliqué : si vous modifiez un composant matériel essentiel (comme la carte mère ou le disque dur), Windows ne sera plus activé. Si vous relancez le processus d'activation, vous obtiendrez un message d'erreur. Pour réactiver Windows, vous devrez obligatoirement contacter le support technique du fabricant de votre ordinateur ou le support de Microsoft.

Sources :

- https://lecrabeinfo.net/
- https://www.microsoft.com/fr-fr/Licensing/existing-customer/FAQ-product-activation.aspx
- https://obinshah.wordpress.com/2010/08/30/installing-windows-7-%E2%80%93-part-3/
- http://louwrentius.com/understanding-windows-kms-and-mak-volume-license-activation.html
- http://forum.hardware.fr/hfr/WindowsSoftware/Tutoriels/licences-microsoft-windows-sujet_262410_1.htm
- http://www.mydigitallife.info/differences-between-oem-channel-slp-nonslp-and-coa-license-product-keys/
- https://blog.hqcodeshop.fi/archives/207-Transferring-Windows-7-OEM-license-to-a-new-hard-drive.html

BTSSIO

ANNEXE 4 : LICENCES 2016 SERVEUR ET CAL

Comprendre la structure des Licences Microsoft Windows Server 2016

Microsoft® Windows Server® 2016 apporte de nombreux changements et améliorations qui le distinguent des versions précédentes. Rien d'étonnant à ce que Windows Server 2016 introduise aussi un nouveau modèle de licences. Quelles sont les nouveautés ? Pour l'édition Standard et Datacenter de Windows Server 2016, les licences ne sont plus basées sur le nombre de processeurs, mais sur le nombre de cœurs (la version Essentials[1] de Windows Server 2016 est quant à elle toujours basée sur le nombre de processeurs).
A quoi sont dus ces changements ? Et non, ils ne sont pas intervenus juste pour compliquer les choses ! Baser les licences sur les cœurs c'est établir une unité commune pour les ressources informatiques sur site et dans le cloud. Ce modèle de licences permet non seulement la mise en place d'un environnement multi-cloud, mais il améliore aussi la portabilité des environnements Windows Server et aide à éliminer les frictions entrer les différents modèles de licences.

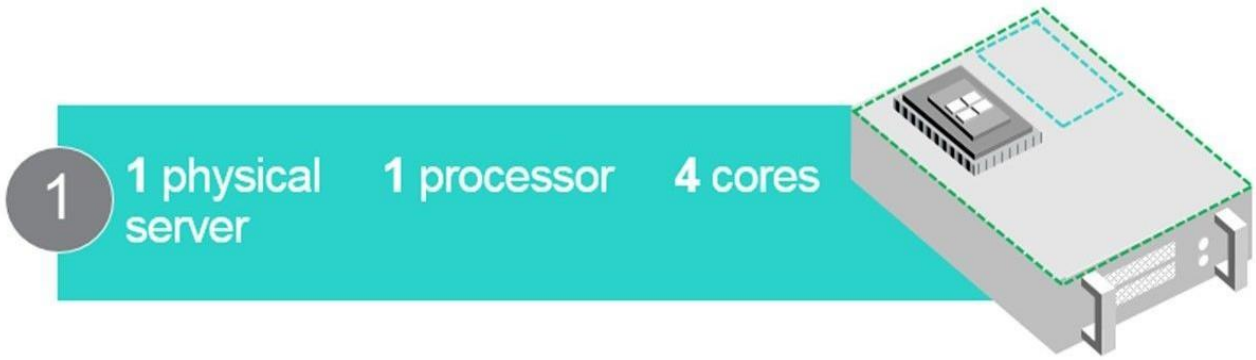
Voici les 3 règles principales qui doivent être suivies avec le modèle de licences basées sur les cœurs:

- Une licence pour chaque cœur physique dans le serveur
- Vérifiez que chaque processeur possède une licence couvrant un minimum de 8 cœurs
- Vérifiez que chaque serveur possède une licence couvrant un minimum de 16 cœurs

La licence de base pour les éditions Standard et Datacenter de HPE OEM Microsoft Windows Server 2016 (Kit d'Option Revendeur/ROK et préinstallé en usine) couvrira jusqu'à 16 cœurs par système. Les clients ayant besoin de licences pour plus de 16 cœurs peuvent facilement acquérir des Licences Additionnelles. Les licences additionnelles couvrent 2, 4 ou 16 cœurs.

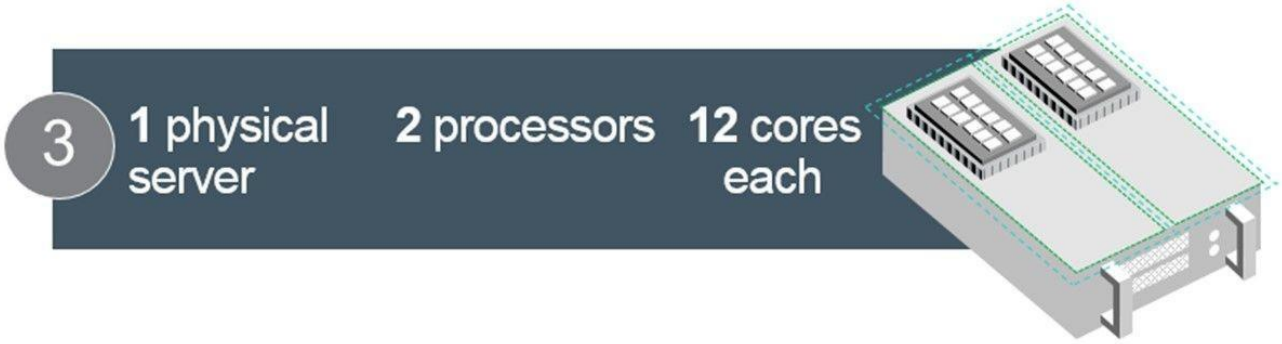
Pour les clients ayant besoin de licences pour Machines Virtuelles (VM), l'édition Standard de Windows Server 2016 donne droit à un maximum de deux environnements système (OSEs) ou conteneurs Hyper-V lorsque tous les cœurs physiques dans le serveur ont une licence. Pour chaque unité ou paire de VMs additionnelles, le client doit acquérir de nouvelles licences pour tous les cœurs physiques dans le serveur.
***La licence Datacenter de Windows Server 2016 donne droit à un nombre illimité de VMs et de conteneurs Hyper-V.*

Voyons quelques scenarios possibles et les licences Windows Server 2016 basées sur les cœurs qu'il convient d'acheter dans de telles configurations.



Scenario 1: Pour 1 serveur physique avec 1 processeur et 4 cœurs une Licence de Base (qui couvre 16 cœurs et 2 processeurs par serveur) est requise, bien que le serveur n'ait qu'un processeur et quatre cœurs. La règle c'est une licence couvrant un minimum de 8 cœurs par processeur et 2 processeurs par serveur. Chaque serveur doit donc posséder une licence couvrant un minimum de 16 cœurs.

Scenario 2: Pour 1 serveur physique avec 2 processeurs et 8 cœurs pour chaque processeur, là encore, comme dans le scenario 1, une seule Licence de Base est requise
Et si le client a besoin de licences pour un serveur avec plus de 16 cœurs ?



Scenario 3: Pour 1 serveur avec 2 processeurs et 12 cœurs pour chaque processeur une Licence de Base est requise (qui couvre 2 processeurs et 16 cœurs), plus des Licences Additionnelles pour couvrir les 8 cœurs restant de manière à ce que les 24 cœurs aient une licence (une licence pour chaque cœur physique).
Si votre scenario est différent et que vous souhaitez savoir de combien de licences il vous faut disposer, HPE a créé l'outil Windows Server 2016 Core Licensing Calculator pour vous aider à déterminer les licences exigées pour votre système. Il suffit de choisir l'édition (Standard ou Datacenter), indiquer le nombre de processeurs et de cœurs qui ont besoin d'être sous licence, et l'outil se charge de calculer le nombre et le type de licences requises.

N'oubliez pas les CALs !

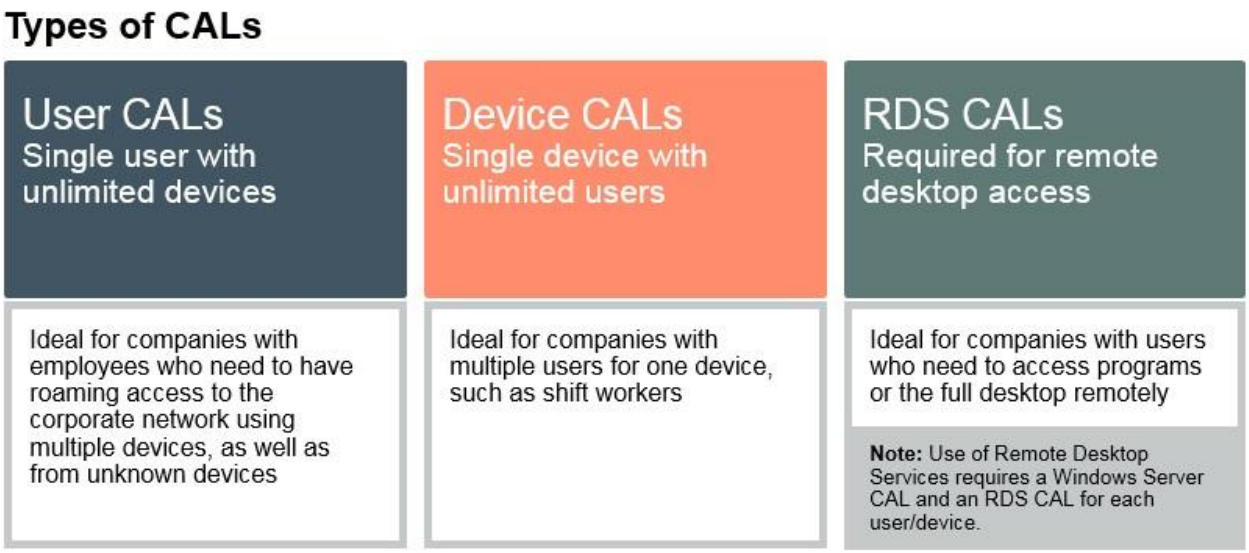
Le nouveau modèle de licence inclut obligatoirement des licences par cœurs + des Licences d'Accès Client (CALs). Chaque utilisateur et/ou appareil accédant une licence de Windows Server 2016 édition Standard ou Datacenter a besoin d'une CAL Windows Server.

Les besoins en Licences d'Accès Client (CALs) Windows Server 2016 de vos clients sont-ils comblés ?

Une CAL n'est pas un produit software. Il s'agit d'une licence qui donne à un utilisateur ou à un appareil le droit de profiter des services du serveur. (Active Directory ou partage de fichiers par exemple).

Il y a de nombreux types de CALs :

- CAL User (utilisateur),
- Device CAL (appareil)
- CAL Remote Destktop Service (RDS)



User CALs (utilisateur):

Avec les CALs utilisateur, une CAL est achetée pour chaque utilisateur qui accède le serveur et utilise des services comme le stockage de fichiers ou l'imprimante, indépendamment du nombre d'appareils qu'il utilise pour y accéder.

Solution la plus économique et la plus simple à administrer pour une entreprise comptant beaucoup d'employés itinérants qui accèdent au réseau à partir de postes inconnus, et/ou le nombre d'utilisateurs est inférieur au nombre de postes (un utilisateur pouvant utiliser plusieurs ordinateurs

différents.

Avec la prolifération d'appareils et les pratiques BYOD (Bring Your Own Device), les employés utilisent de plus en plus d'appareils. De ce fait, il est souvent plus facile de prendre en compte le nombre d'utilisateurs accédant le serveur, plutôt que le nombre d'appareils accédant le serveur.

Device CALs (appareil):

Avec les CALs appareil, une CAL est achetée pour chaque appareil qui accède le serveur indépendamment du nombre d'utilisateurs qui utilisent ces appareils pour accéder le serveur. Les CALs appareil peuvent être plus avantageuses pour les entreprises dont les employés partagent les appareils.

RDS CALs:

Une CAL Remote Desktop Service (RDS) est requise pour les utilisateurs qui ont besoin d'accéder à distance à des programmes ou à leur bureau complet. Pour accéder à distance au bureau, une CAL Windows Server (CAL utilisateur ou CAL appareil) et une CAL RDS sont requises.

Les CALs peuvent être achetées directement chez HPE ou chez un revendeur HPE agréé et sont disponibles à l'unité ou en pack de 5, 10 ou 50.

FAQ: CALs pour Windows Server 2016 :

Q: Les CALs sont-elles toujours requises pour Windows Server 2016?

R: Les éditions Standard et Datacenter de Windows Server requièrent des CALs Windows Server pour chaque utilisateur ou appareil accédant un serveur (l'édition Essentials ne requiert pas de CALs). Certaines fonctionnalités avancées ou additionnelles requièrent l'achat de RDS CALs. Les RDS CALs sont indispensables en addition aux Windows Server CALs pour accéder des fonctionnalités comme Remote Desktop Services.

Q: Est-il possible d'acheter des CALs additionnelles après avoir acheté la licence OS?

R: Oui, les clients peuvent acheter des CALs additionnelles chez HPE ou chez les revendeurs HPE agrées sans que l'achat d'un nouveau serveur HPE soit nécessaire. HPE propose actuellement des CALs à l'unité ou en pack de 5, 10 ou 50 (utilisateur ou appareil) et des packs de 5 CALs pour les CALs RDS (utilisateur ou appareil).

Q: Puis-je utiliser mes CALs Windows Server 2012 pour accéder Windows Server 2016?

R: Non. Les CALs doivent être de la même version ou d'une version plus récente que le software serveur que vous accédez . Les utilisateurs ou appareils accédant un serveur exécutant Windows Server 2016 doivent posséder des CALs Windows Server 2016.

Q: Puis-je utiliser des CALs Windows Server 2016 pour accéder Windows Server 2012 R2?

R: Oui. Une CAL Windows Server permet d'accéder à toutes les versions antérieures de Windows Server.

NOTA BENE :

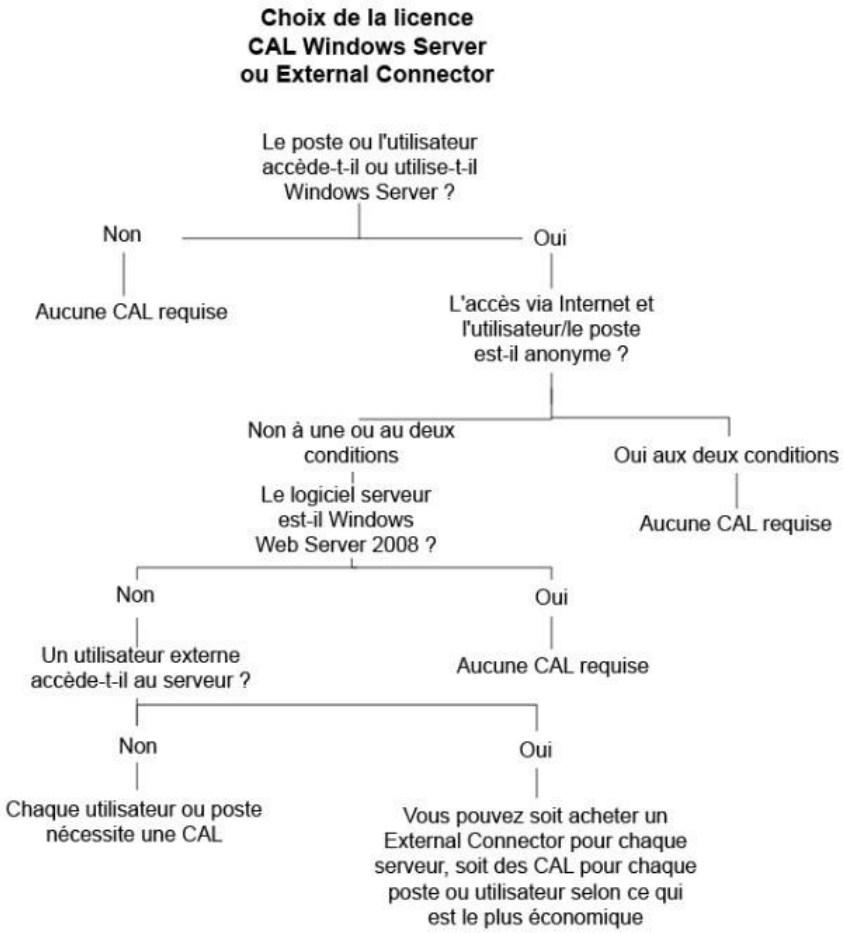
1) MAIS, si une version future de Windows Serveur est installée (2018 / 2020 etc..)

Il faudra acheter à nouveau des licences CAL pour chaque utilisateur ou device.

2) Windows 2008 R2 Standard est livré avec 5 licences CAL, ce n'est plus le cas pour 2012.

3) Il existe également des CAL pour SQL Serveur, Exchange, Link, SharePoint...

Licence d'accès client Windows Server 2008 : arbres de décision, types et modes



Sources : Documents Microsoft
-> VOIR DOCS-MICROSOFT.ZIP

- Windows_Server_2008_Guide_des_Licences
- WS2016LicensingDatasheet
- Microsoft Product Terms (WW) (French) (January2018) Blog HP : https://community.hpe.com/t5/L-Avenir-de-l-IT

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

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

Paris, le 3 août 2015

N° DAT-NT-003/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 18

Note technique

Recommandations de sécurité relatives à IPsec [1] pour la protection des flux réseau

Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

1. Internet Protocol Security

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les **« Recommandations de sécurité relatives à IPsec [a] pour la protection des flux réseau »**. Il est téléchargeable sur le site www.ssi.gouv.fr/ipsec. 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). 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.

a. Internet Protocol Security

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
LAM, LRP, COSSI	DAT	SDE	31 août 2012
DAT	DAT	SDE	3 août 2015

Évolutions du document :

Version	Date	Nature des modifications
1.0	31 août 2012	Version initiale
1.1	3 août 2015	Corrections mineures Exemples de groupes de DH

Pour toute remarque :

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

Table des matières

1 Préambule

Les systèmes d'information adoptent généralement aujourd'hui une architecture distribuée. Les différentes briques logicielles et matérielles qui les composent sont de plus en plus communicantes, non seulement entre elles mais également avec des systèmes d'information distants et à travers l'internet. La montée en puissance de l'informatique en nuage et de l'externalisation ne font qu'accélérer cette tendance.

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

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

2 Présentation d'IPsec

IPsec permet, par encapsulation, de protéger en confidentialité, intégrité et anti-rejeu un flux au niveau de la couche réseau (couche « Internet » de la pile TCP/IP ou couche 3 « réseau » du modèle OSI). IPsec est normalisé par l'IETF, au travers notamment des RFC 4301 à 4309. Plusieurs versions se sont succédées et divers éléments additionnels ont été définis. Un inventaire en est donné dans la RFC 6071.

Un très grand nombre d'équipements réseaux, en particulier les routeurs et les pare-feux, permettent l'utilisation d'IPsec. De même, les principaux systèmes d'exploitation pour micro-ordinateurs ou ordiphones prennent en charge IPsec nativement. Le dialogue IPsec est généralement possible entre ces différents systèmes et équipements.

Dans de nombreux cas, l'utilisation d'IPsec présente un rapport "bénéfice en sécurité" sur "coût" appréciable dans la mesure où cette technologie est prise en charge nativement par la plupart des systèmes clients et des équipements réseau et ne nécessite donc généralement pas d'investissements lourds. Il s'agit par ailleurs d'un protocole arrivé à maturité et bien connu. Sa mise en œuvre peut donc se faire sans charge excessive pour les équipes d'administration.

3 Glossaire

AH *Authentication Header* : protocole faisant partie de la suite IPsec, cf 6.1.1.

ESP *Encapsulation Security Payload* : protocole faisant partie de la suite IPsec, cf 6.1.2.

IKE *Internet Key Exchange* : protocole d'échange de clés, cf 6.4.3.

VPN *Virtual Private Network* : réseau privé virtuel.

IETF *Internet Engineering Task Force* : organisme à l'origine des standards Internet.

RFC *Request for comments* : documents émanant de l'IETF, tels que les standardisations de protocoles.

NAT *Network Address Translation* : mécanisme de traduction d'adresses réseau.

TLS *Transport Layer Security* : protocole de sécurisation en couche applicative.

SSL *Secure Socket Layer* : version obsolète de TLS.

LS *Liaison spécialisée.*

MPLS *Multiprotocol Label Switching* : protocole fonctionnant par commutation de labels, utilisé notamment dans les offres de type « IP-VPN ».

RGS *Référentiel général de sécurité* : document disponible sur `www.ssi.gouv.fr/rgs`.

MTU *Maximum Transmission Unit* : taille maximale d'un paquet pouvant être émis ou reçu sur une interface réseau.

4 Différents cas d'usage d'IPsec

La technologie IPsec est la plupart du temps associée aux connexions de réseau privé virtuel (Virtual Private Network) qui, bien souvent, transitent sur un réseau public tel que l'internet. Il est toutefois important de noter que cet usage d'IPsec est loin d'être le seul possible.

4.1 Accès distants en nomadisme

Les flux réseau échangés entre un poste en situation de nomadisme et le système d'information doivent être protégés. IPsec est très souvent employé pour la connexion à distance d'un poste à un réseau privé et se prête effectivement bien à ce cas d'usage. Le VPN est habituellement monté entre un poste client (ordinateur portable ou ordiphone par exemple, via un client VPN logiciel) et un équipement réseau de sécurité (pare-feu ou boitier VPN).

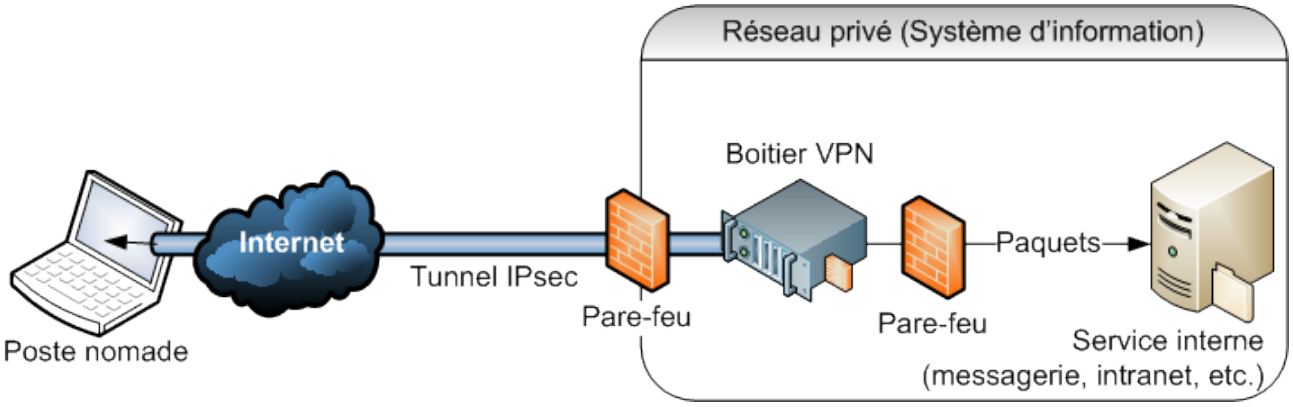


FIGURE 1 – Exemple d'emploi d'IPsec dans le cas d'un VPN.

La protection apportée est certes plus évidente pour des applications qui ne reposent pas sur des protocoles sécurisés (tels que TLS), mais il est recommandé de recourir systématiquement à IPsec y compris pour des applications bénéficiant d'une sécurisation en couche applicative. Cela s'inscrit dans une démarche de défense en profondeur et permet en outre d'adopter une politique plus simple à définir et à maintenir. IPsec apporte alors généralement la protection en intégrité et en confidentialité après une authentification préalable. L'usage d'IPsec comme technologie de protection des flux VPN est donc à privilégier et complète utilement les protocoles tels que PPTP ou L2TP.

R1 - Équipements de confiance

> Un certain nombre de logiciels ou d'équipements réseau destinés à la mise en oeuvre de VPN IPsec ont été évalués par l'ANSSI et ont obtenu une certification de sécurité ou une qualification. Il est recommandé de recourir à ces produits, en priorité à ceux qui sont qualifiés, (listés sur www.ssi.gouv.fr/fr/certification-qualification/) dès lors qu'il existe un besoin de produits de confiance.

4.2 Liaison de deux sites distants

Il est également possible d'utiliser IPsec pour relier de manière sécurisée les réseaux locaux de deux sites distants. Cela permet de se prémunir de malveillances qui consisteraient à accéder au lien entre ces deux réseaux, et à ainsi intercepter des informations sensibles ou procéder à des attaques par le milieu.

L'intérêt d'utiliser IPsec est avéré lorsque le lien considéré s'appuie sur un réseau public (tel que l'internet), mais l'est également lorsqu'un lien loué (de type LS ou VPN MPLS par exemple) est utilisé.

Dans ce contexte, le lien IPsec est généralement monté entre deux équipements dédiés ou entre deux pare-feux périmétriques au système d'information. La recommandation R1 est aussi applicable à ce cas d'usage.

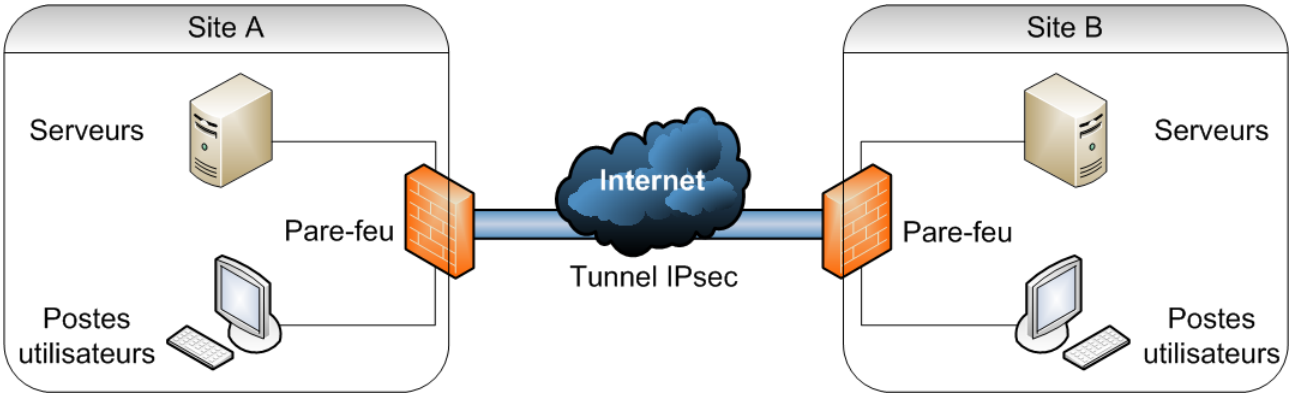


FIGURE 2 – Exemple d'emploi d'IPsec entre sites distants.

Note : Dans cet exemple, un tunnel IPsec est monté entre deux pare-feu.

4.3 Protection vis à vis d'une faiblesse protocolaire ou d'une vulnérabilité logicielle

Il arrive qu'il soit nécessaire de gérer la subsistance dans un système d'information d'équipements ou de briques logicielles dont les mécanismes de confidentialité ou d'authentification ne sont pas à l'état de l'art (voire inexistant), et dont les communications réseau ne sont donc pas protégées efficacement. Des individus malveillants qui auraient accès à ces flux (parce qu'ils transitent par des liens réseau publics ou insuffisamment sécurisés), pourraient alors les intercepter ou procéder à des attaques par le milieu. Ceci est par exemple souvent le cas :

- sur les systèmes SCADA en milieu industriel, utilisant des protocoles de communication de faible robustesse ;
- entre serveurs applicatifs et systèmes de gestion de bases de données ;
- entre briques applicatives distribuées utilisant des protocoles propriétaires, ou des bus logiciels pas ou mal sécurisés ;
- entre clients et serveurs utilisant des protocoles non sécurisés (FTP, POP3, SMTP, HTTP, RDP, VNC, etc.) ;
- etc.

Nombreux sont les cas ou les flux réseau doivent être protégés par des solutions tierces. IPsec se présente alors comme la technologie idéale pour pallier certaines faiblesses des protocoles de plus haut niveau. Son emploi est donc recommandé pour encapsuler des flux réseau véhiculant des informations jugées sensibles, et ainsi leur assurer la protection nécessaire. Lorsque les nœuds terminaux ne prennent pas en charge IPsec, il peut être nécessaire d'interposer des équipements réseau intermédiaires. La recommandation R1 s'applique alors à nouveau. On ne négligera pas, dans ce cas, le risque résiduel constitué par les tronçons d'extrémité en clair.

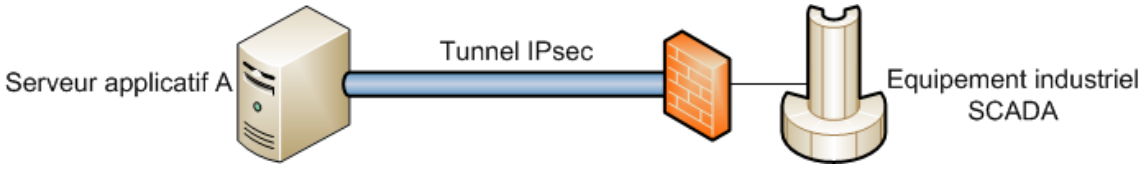


FIGURE 3 – Exemple d'emploi d'IPsec avec un équipement intermédiaire.

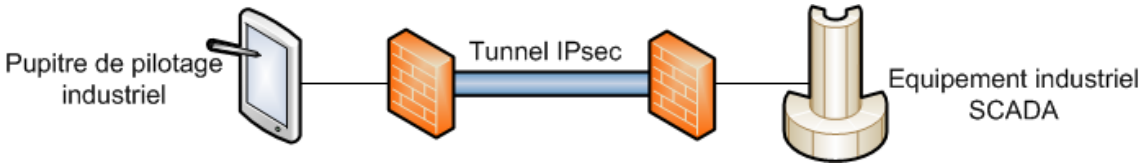


FIGURE 4 – Exemple d'emploi d'IPsec avec deux équipements intermédiaires.

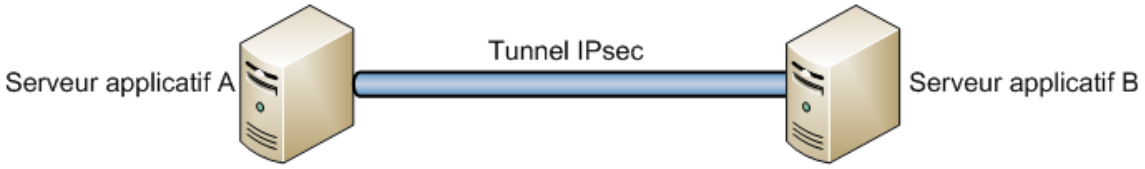


FIGURE 5 – Exemple d'emploi d'IPsec de point à point.

4.4 Défense en profondeur

Dans le cadre d'une défense en profondeur, IPsec peut être utilisé comme mesure de sécurité additionnelle pour encapsuler des protocoles qui sont déjà sécurisés par d'autres mécanismes voire un tunnel IPsec existant. Comme déjà indiqué, IPsec étant dans la plupart des cas peu couteux à mettre en place, il peut permettre de renforcer le niveau de sécurité de manière efficiente.

5 Comparaison avec TLS

Il est fréquent de voir IPsec comparé au protocole TLS [2]. Il est vrai que les deux technologies permettent de bénéficier de mécanismes de confidentialité, d'intégrité ou d'authentification. Il existe toutefois plusieurs différences importantes, qui tendent à faire préférer IPsec.

TLS agit beaucoup plus haut dans la pile réseau qu'IPsec, en se plaçant au dessus de la couche transport réalisée par TCP. TLS est souvent employé pour sécuriser d'autres protocoles : c'est ainsi que fonctionne par exemple le protocole HTTPS. C'est toutefois sur un autre usage que ce protocole entre en concurrence avec IPsec, à savoir la mise en oeuvre de « VPN-SSL ». Cette méthode consiste à encapsuler un flux réseau dans une session TLS. Certaines solutions de ce type proposent de s'appuyer sur un navigateur pour se dispenser de la nécessité de déployer un client spécifique sur les postes utilisateurs.

Le premier inconvénient de TLS est que les opérations liées à la sécurité sont effectuées en espace utilisateur, au sein du processus utilisateur. Ces opérations (et les secrets qu'elles manipulent) sont alors nettement plus exposées aux attaques que dans le cas d'IPsec où les opérations critiques se déroulent au sein du noyau ou dans des processus dédiés. Cela est d'autant plus vrai dans le cas où le client VPN s'appuie sur un navigateur, logiciel présentant une surface d'attaque considérable, y compris à distance.

En outre, sur le plan cryptographique, plusieurs éléments plaident en faveur d'IPsec. D'une part, IPsec permet plus largement l'utilisation d'algorithmes modernes recommandés par les bonnes pratiques, que ce soit en termes de prise en compte dans les standards ou d'implantations concrètes dans les logiciels disponibles sur le marché. D'autre part, dans IPsec, l'utilisation des primitives cryptographiques est légèrement meilleure au regard des bonnes pratiques. IPsec recourt, par exemple, à un fonctionnement « Encrypt-then-MAC », méthode considérée plus sûre que le « MAC-then-Encrypt » employé par TLS.

Enfin, on peut observer que le détournement de TLS de l'usage initialement prévu [3] en recourant à des « VPN SSL » n'est pas une solution idéale. L'encapsulation de paquets de la couche réseau en couche applicative conduit notamment à avoir une en-tête TCP « externe » sans aucune corrélation avec l'éventuelle en-tête TCP « interne », ce qui débouche sur un fonctionnement non optimal des mécanismes de contrôle de congestion.

R2

Pour les cas d'usage évoqués précédemment, il est recommandé d'utiliser IPsec plutôt que TLS.

Note : TLS reste bien entendu tout à fait adapté pour la sécurisation d'un protocole applicatif particulier (comme c'est la cas pour HTTPS, IMAPS, LDAPS, ...) et cet emploi est complémentaire et pleinement compatible avec la mise en oeuvre d'IPsec.

2. Le mot SSL se rapporte en toute rigueur à une version ancienne et ayant pratiquement disparu du protocole TLS, protocole quant à lui très couramment employé à l'heure actuelle. Il est toutefois très fréquent de rencontrer des documents utilisant le mot SSL pour désigner TLS, au point d'éclipser cette dernière dénomination.

3. TLS n'est en principe pas destiné à sécuriser des liens entre sites distants mais plutôt à sécuriser la communication entre un utilisateur et un service. Même si la nuance est parfois ténue, il s'agit réellement d'une approche différente.

6 Fonctionnement d'IPsec

IPsec, de par ses subtilités, est souvent partiellement compris et peu maîtrisé. Les choix de configuration, y compris ceux par défaut, ne sont pas toujours judicieux et l'emploi d'IPsec peut alors offrir un niveau de sécurité plus faible que celui attendu.

6.1 Services fournis par IPsec

Les services de sécurité fournis par IPsec reposent sur deux protocoles différents qui constituent le coeur de la technologie IPsec :

- AH : « Authentication Header » (protocole n°51) dont la version la plus récente est normalisée par la RFC 4302 ;
- ESP : « Encapsulation Security Payload » (protocole n°50) dont la version la plus récente est normalisée par la RFC 4303.

Ces deux protocoles peuvent être utilisés indépendamment ou, plus rarement, de manière combinée.

6.1.1 AH : intégrité et authentification des paquets

Le protocole AH, qui est utilisé de manière moins fréquente qu'ESP, permet d'assurer l'intégrité et, employé avec IKE (voir infra), l'authentification des paquets IP. C'est à dire qu'AH permet d'une part de s'assurer que les paquets échangés n'ont pas été altérés et d'autre part de garantir l'identité de l'expéditeur d'un paquet. Il garantit aussi une protection contre le rejeu.

On notera qu'AH ne protège pas la confidentialité des données échangées. Les données ne sont pas chiffrées et transitent en clair, ou plus exactement sous le même format que si l'on utilisait un lien IP sans IPsec (un chiffrement peut être mis en œuvre plus haut dans la couche protocolaire, par exemple en utilisant TLS).

Le contrôle d'intégrité s'effectue sur l'ensemble des paquets IP y compris les en-têtes, à l'exception des en-têtes variables par nature telles que les champs DSCP, ECN, TTL, « Flags », l'offset de fragmentation et la somme de contrôle. Cela signifie en particulier que les adresses sources et destinations font partie des données protégées. Un paquet où ces données ont été modifiées est considéré comme corrompu. Cela crée une incompatibilité avec les mécanismes de traduction d'adresses, voir 6.5.

Les RFC relatives à IPsec rendent la prise en charge d'AH par les équipements mettant en oeuvre IPsec optionnelle tandis que celle d'ESP est obligatoire. De manière générale, face à ESP, AH peut être considéré comme obsolète et d'un faible apport du point de vue de la sécurité, il n'y a généralement pas lieu de le mettre en œuvre.

R3

L'emploi d'IPsec doit se faire avec le protocole ESP. Bien qu'il ne présente pas de risque de sécurité en soi, l'emploi d'AH est déconseillé.

6.1.2 ESP : confidentialité, intégrité et authentification des paquets

Le protocole ESP permet quant à lui d'assurer la confidentialité, l'intégrité et, employé avec IKE (voir infra), l'authentification des données échangées. Il garantit aussi une protection contre le rejeu. Il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH et justifie donc l'abandon d'AH).

Certaines implémentations permettent à l'inverse la protection en confidentialité sans mécanisme de contrôle d'intégrité : cet usage, lui-aussi obsolescent, doit être évité. La suppression du service d'intégrité ne présente aucun avantage (le coût en performance des opérations de contrôle d'intégrité

est en général négligeable devant celui du chiffrement) et expose l'utilisateur a un certain nombre d'attaques connues et réalistes.

R4

Le service de confidentialité d'ESP ne doit jamais être employé sans activer le mécanisme de contrôle d'intégrité.

Contrairement à l'approche retenue dans le cadre d'AH, les données protégées sont ici uniquement le « payload », c'est à dire le contenu du paquet IP et non ses en-têtes. Il n'y a donc pas d'incompatibilité fondamentale avec les mécanismes de traduction d'adresses. Il est toutefois nécessaire de prendre un certain nombre de mesures pour assurer l'interopérabilité entre ESP et la traduction d'adresse, voir 6.5.

6.2 Modes transport et tunnel

Indépendamment du choix entre AH et ESP, il est possible d'utiliser IPsec dans deux modes distincts : le mode tunnel et le mode transport. Le mode tunnel rend le service attendu dans la majorité des cas.

Dans le mode transport, les données associées à AH ou à ESP viennent se greffer sur le paquet IP initial (c'est à dire celui qu'on aurait envoyé en l'absence d'IPsec). Le paquet IP résultant contient un paquet AH ou ESP qui contient lui-même le contenu du paquet initial (un segment TCP par exemple). On peut remarquer que l'en tête IP initiale doit être modifiée : son champ protocole doit indiquer 50 ou 51 pour ESP ou AH en lieux et place par exemple de 6 (TCP) ou 17 (UDP). C'est l'en tête (AH ou ESP) qui indiquera le protocole encapsulé qui était auparavant indiqué dans l'en-tête IP.

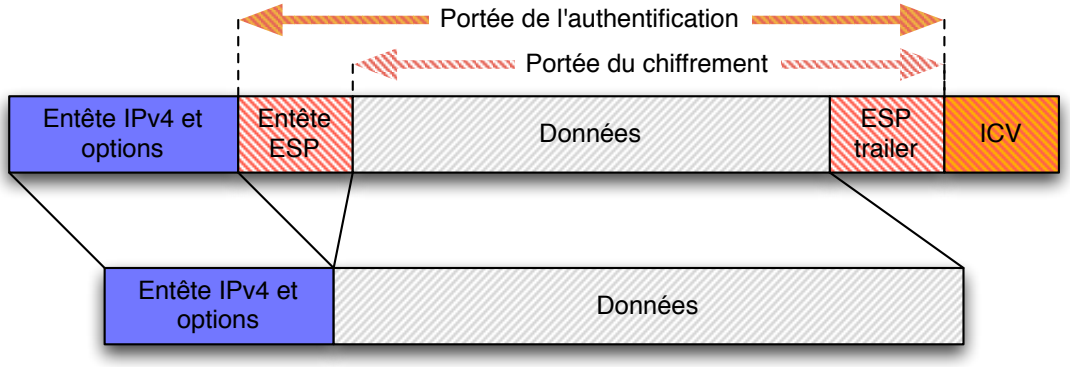


FIGURE 6 – Utilisation d'ESP en mode transport. ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité

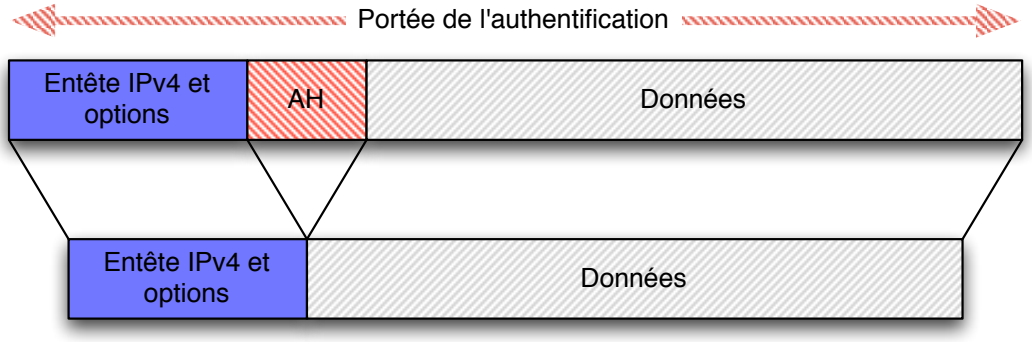


FIGURE 7 – Utilisation d'AH en mode transport

Dans le mode tunnel en revanche, un nouveau paquet IP est généré pour contenir un paquet AH ou ESP qui contient lui-même le paquet IP initial sans modification. Dans ce mode, il y a donc en définitive deux en-têtes IP. L'en-tête externe sera effectivement utilisé pour le routage dès l'émission du paquet. L'en-tête interne, qui peut être chiffrée dans le cas où l'on utilise ESP avec le service de confidentialité, ne sera traitée que par le destinataire (du paquet externe). Elle sera ignorée par les équipements réseau situés entre l'émetteur et le destinataire. On réalise ainsi un « tunnel » à travers ce réseau, de la même façon qu'on peut le faire avec des protocoles tels que IPIP (RFC 2003) ou GRE (RFC 2784).

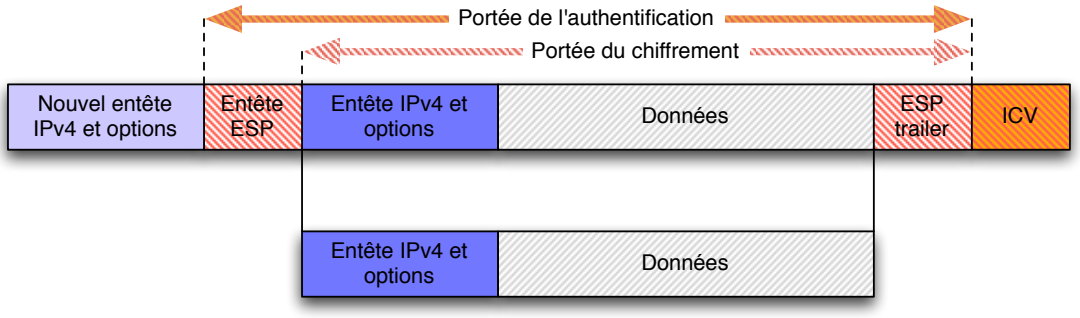


FIGURE 8 – Utilisation d'ESP en mode tunnel. ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité

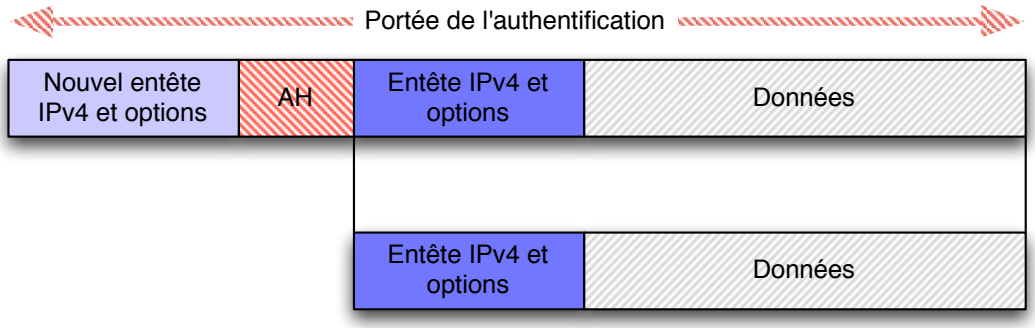


FIGURE 9 – Utilisation d'AH en mode tunnel

Le mode tunnel se prête bien à un scénario d'accès distant à un réseau privé au travers d'un réseau public. Il permet de masquer sur les tronçons publics l'adressage interne du réseau privé, fréquemment non routable sur le réseau public. IPsec est utilisé sur le réseau public entre le client et une passerelle qui extrait le paquet IP interne et l'injecte dans le réseau privé (et réciproquement pour le sens de communication inverse).

Naturellement, du fait de la duplication de l'en tête IP, l'utilisation du mode tunnel résulte en des paquets plus gros qu'en mode transport pour une même quantité de données utiles. La consommation en ressources réseau est donc plus importante. En particulier, il faudra prendre garde au fait que le MTU effectif du tunnel est le MTU du lien diminué de la taille des méta-informations ajoutées par IPsec (nouvelle en-tête IP, en-tête et trailer ESP, somme de contrôle). La taille de ces méta-données varie notamment en fonction des paramètres cryptographiques, mais il est courant que le « surcoût » en taille dû au tunnel soit de 50 à 100 octets. Dans certains cas, les mécanismes de configuration automatique du MTU gèrent mal cette situation. Il est par conséquent relativement fréquent, lors de l'utilisation d'IPsec, de devoir limiter manuellement la taille maximale des paquets IP clairs pour s'assurer qu'une fois ceux-ci encapsulés ils n'atteignent pas une taille qui nécessite de les fragmenter.

Un élément qui peut s'avérer important est le fait qu'en mode tunnel, le contrôle d'intégrité offert par le mode AH porte non seulement sur le paquet interne mais aussi sur l'en-tête IP externe, de la même façon qu'en mode transport. Cela peut avoir des effets indésirables en cas de NAT, voir 6.5. Le contrôle d'intégrité d'ESP ne porte quant à lui que sur le paquet interne et permet donc à l'en-tête externe d'évoluer.

6.3 Security Policy

Le terme « Security Policy » désigne, dans le contexte IPsec, le choix pour un lien unidirectionnel [4] donné :

- de l'utilisation obligatoire ou facultative ou de la non-utilisation d'IPsec ;
- de l'utilisation du mode tunnel ou transport ;
- de l'utilisation d'AH ou d'ESP.

L'ensemble des SP est regroupé dans une SPD : « Security Policy Database ».

À l'image des règles de flux d'un pare-feu, les SP ont pour but de spécifier les flux que l'on veut autoriser et ceux que l'on veut interdire.

R5

Les SP permettant un usage « facultatif » ou « optionnel » d'IPsec doivent être évitées car elles ne garantissent pas la sécurité (possibilité de « downgrade attack »). Pour un lien donné, on s'en tiendra donc à n'autoriser que les flux sécurisés dès lors qu'il existe un besoin de sécurité.

R6

Malgré la possibilité technique de fonctionnement asymétrique, on préfèrera lorsque c'est possible avoir une politique uniforme entre le lien aller et le lien retour.

6.4 Etablissement d'un lien IPsec

Les mécanismes cryptographiques utilisés pour la protection en intégrité ou en confidentialité sont paramétrés par une ou plusieurs clés. Ces éléments doivent être partagés par les différents hôtes

4. On distingue en effet le lien $A \to B$ et le lien $B \to A$ qui peuvent avoir deux politiques différentes.

employant IPsec. Deux approches sont possibles : mettre en place manuellement des clés sur chaque hôte ou utiliser le mécanisme d'échange de clés IKE pour que les hôtes puissent négocier ces clés.

6.4.1 Security Association

Pour chaque lien unidirectionnel (comme ci-dessus), on désigne par « Security Association » (SA) les données de contexte telles que :

- les hôtes source et destination ;
- le mode (transport/tunnel) et les protocoles (AH/ESP) employés ;
- les algorithmes cryptographiques employés ;
- les clés associées à ces algorithmes.

Chaque SA est associée à une période de validité et à un nombre entier la désignant de manière univoque et appelé SPI (Security Parameter Index). Les en-têtes AH et ESP indiquent systématiquement le SPI associé à la SA utilisée.

Les premiers éléments (hôtes aux extrémités, mode, protocole) sont conditionnés par les SP en vigueur : un système ne doit pas avoir de SA qui violent ses SP.

Les paramètres cryptographiques (algorithmes, taille de clés) peuvent être fixés manuellement ou négociés par le protocole IKE (voir plus bas). Les options possibles sont configurées par l'administrateur.

On définit, comme pour la SPD, la SAD comme étant la « Security Association Database » (base des SA).

R7

Il est préférable de fixer a priori les algorithmes et tailles de clés employés (voir infra pour le choix) et de n'utiliser IKE que pour l'échange de clés. À défaut de pouvoir les fixer, on ne permettra la négociation que sur un nombre réduit d'algorithmes.

Note : Dans ce dernier cas, la sécurité du lien est conditionnée par l'algorithme le plus faible parmi ceux acceptés ; il est donc nécessaire que toutes les options soient conformes à la politique de sécurité de l'organisme.

6.4.2 Mise à la clé manuelle

Les algorithmes et les clés peuvent être paramétrés manuellement sur chaque équipement. On parle généralement du « Manual Keying » ; il est important de ne pas confondre cette méthode avec l'authentification « Pre-Shared Key » d'IKE abordée au chapitre suivant.

La mise à la clé manuelle est fortement déconseillée. Elle exige en effet une configuration fastidieuse, la clé étant idéalement différente pour chaque couple d'hôtes. Par ailleurs, il est difficile en pratique de renouveler les clés à une fréquence suffisante pour être conforme tant aux bonnes pratiques cryptographiques (usure de la clé) que de SSI (cryptopériode) [5]. En outre, elle ne permet pas de bénéficier de la propriété de « Perfect Forward Secrecy » présentée en 6.6. Enfin, elle ne permet pas de mettre en oeuvre des mécanismes d'authentification cryptographiques.

En définitive, la mise à la clé manuelle doit être réservée à des procédures de tests ou de diagnostics ou à des système très particuliers ayant fait l'objet d'une étude de sécurité approfondie, notamment pour s'assurer que le cycle de vie des clés est bien géré et qu'il y a bien une clé différente pour chaque usage.

5. On distingue en effet l'usure de la clé, qui décrit une propriété mathématique selon laquelle le système cryptographique est fragilisé au delà d'une certaine quantité d'information chiffrée, de la cryptopériode, durée maximale d'usage de la clé basée sur des considérations organisationnelles ayant pour but de borner l'impact d'une compromission.

6.4.3 Utilisation d'IKE

La négociation dynamique des algorithmes et clés d'une SA peuvent se faire grâce au protocole IKE, actuellement en version 2 (RFC 5996).

R8

Il est recommandé d'utiliser la version 2 d'IKE.

6.4.3.1 Un protocole en deux phases

Le protocole IKE se décompose en deux phases distinctes. Dans une première phase, un canal sécurisé (chiffré et authentifié) est créé entre les deux participants. Dans une deuxième phase, ce canal est utilisé pour négocier les divers paramètres de la SA.

La première phase utilise bien entendu elle aussi des algorithmes cryptographiques, qui ne sont pas nécessairement les mêmes que ceux définis finalement dans la SA. Les paramètres du canal sécurisé négocié lors de la première phase et utilisé pour protéger la seconde phase sont parfois désignés sous le terme ISAKMP [6] SA ou encore IKE SA, par opposition aux IPSEC SA qui sont les SA négociées lors de la seconde phase et utilisées pour protéger le trafic « utile ».

La première version d'IKE permettait deux modes différents pour la phase 1, le mode principal (« main mode ») et le mode agressif (« aggressive mode »). Le deuxième a la caractéristique de nécessiter moins de messages que le premier mais de ne pas cacher l'identité des participants à un éventuel attaquant en écoute passive sur le réseau. La phase 2 utilisait quant à elle le mode rapide (« quick mode »). IKE version 2 a une première phase similaire au mode principal mais n'emploie plus cette terminologie. On trouve toutefois encore des produits désignant par « mode principal » la première phase et « mode rapide » la deuxième.

6.4.3.2 Authentification des correspondants

L'authentification des participants à la première phase peut se faire soit au moyen d'un secret partagé (PSK : « Pre-Shared Key ») soit par utilisation d'un mécanisme de cryptographie asymétrique tel que RSA. Dans ce cas, il est possible d'utiliser une Infrastructure de Gestion de Clés (IGC ou PKI) pour certifier les clés publiques des participants et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes.

On privilégie généralement l'utilisation d'une IGC, ce qui permet de simplifier l'exploitation du système : l'ajout d'un nouvel hôte ou la révocation d'une clé compromise est aisée (il n'est pas nécessaire d'intervenir sur tous les équipements déjà en place). Il peut être délicat dans les autres modes de réagir avec la diligence nécessaire à une compromission de clé, par exemple le vol d'un équipement.

Le mode PSK doit en principe être évité pour des systèmes en production et être cantonné à des systèmes de tests ou à des opérations de diagnostic. S'il était nécessaire d'y recourir exceptionnellement, une bonne pratique générale pour les secrets partagés est de prendre garde à ce que l'entropie soit suffisante pour rendre difficile une attaque par recherche exhaustive. On se reportera à se sujet au référentiel général de sécurité publié par l'ANSSI. Une entropie inférieure à 100 bits est considérée à la date de rédaction de ce document comme un choix risqué.

6. ISAKMP est un « protocole cadre » (framework) au sein duquel le protocole IKE a été défini.

R9

Il est fortement déconseillé dans le cas général d'utiliser la mise à clé manuelle ou une clé pré-partagée (PSK) pour l'établissement d'un lien IPsec. Des mécanismes basés sur de la cryptographie asymétrique sont à privilégier. On privilégiera en particulier les mécanismes d'IGC qui permettent la révocation rapide des clés compromises, en particulier en cas de perte d'un poste. Les dérogations à ces recommandations doivent avoir fait l'objet d'une étude de sécurité rigoureuse.

6.4.3.3 Négociation des SP

IKE permet aussi de négocier les SP. Dans la plupart des cas, tous les paramètres des SP sont connus à l'avance et cette négociation ne présente que peu d'intérêt. Ce mécanisme prend toutefois tout son sens pour les situations de mobilité. Dans ce cas, en effet, l'adresse IP du client nomade n'est pas connue a priori : elle est attribuée par le réseau accueillant le poste nomade. Il est alors très utile de pouvoir adapter ce paramètre de la SP à la volée au moyen de la négociation IKE.

Dans les cas où un tel mécanisme de négociation n'est pas nécessaire, il est préférable d'employer une configuration statique (si les équipements le permettent) de manière à garder la maîtrise de la politique de sécurité. Dans le cas où une négociation des politiques de sécurité par IKE est utilisée, il est nécessaire de s'assurer par la politique de filtrage que le système ne se trouve jamais dans un état où il échange des données en clair. Concrètement, cela signifie interdire par des règles de filtrage réseau tout trafic qui n'utilise pas le protocole IKE, ESP et (le cas échéant) les protocoles qui seraient nécessaires au fonctionnement du réseau, tel qu'ICMP.

R10

On privilégiera la configuration statique des SP lorsque le cadre d'emploi le permet. À défaut, il est nécessaire de s'assurer que la politique de filtrage mise en œuvre garantit l'absence de flux en clair.

6.5 Utilisation d'IPsec avec un système de traduction d'adresses (NAT)

L'utilisation d'un système de traduction d'adresses (NAT) en conjonction avec IPsec peut poser plusieurs problèmes.

Tout d'abord, l'utilisation d'AH n'est pas possible, dans la mesure où le contrôle d'intégrité des en-têtes IP devient invalide dès lors que les adresses IP sources ou destinations sont modifiées.

Par ailleurs, certains mécanismes de NAT très courants nécessitent de pouvoir modifier les ports TCP ou UDP. Si le protocole transporté par IP est ESP, qui ne présente pas de port, un tel mécanisme ne peut fonctionner. La solution est l'emploi du « NAT-Traversal » (NAT-T) qui consistent à encapsuler le trafic IKE puis ESP dans des datagrammes UDP utilisant de manière standard le port 4500.

Enfin, il faut prendre garde à certaines extensions hors standard qui peuvent être incompatibles avec l'utilisation de NAT ou nécessiter l'utilisation de NAT-T même dans des cas où la modification de ports n'est pas nécessaire.

R11

S'il est nécessaire de recourir au NAT sur des flux IPsec, il est nécessaire d'activer le mécanisme de NAT-Traversal.

6.6 PFS : Perfect forward Secrecy

La propriété de PFS (Perfect forward Secrecy) est la caractéristique de certains protocoles cryptographiques qui garantit qu'un attaquant ayant enregistré des échanges chiffrés à un instant donné et parvenant à obtenir les secrets cryptographiques à une date ultérieure ne puisse pas pour autant déchiffrer les enregistrements effectués.

La PFS permet donc de mettre en place des fenêtres temporelles « étanches », en ce sens que l'impact d'une éventuelle attaque ne pourra pas (sous certaines hypothèses) s'étendre aux fenêtres déjà refermées. Il s'agit d'une mesure de « mitigation » du risque.

Cette propriété est obtenue (pour le cas d'IPsec) en employant un mécanisme d'échange de clé « Diffie-Hellman éphémère » ou sa variante sur courbe elliptique.

Le degré de granularité de cette protection (la fenêtre) est la session, délimitée par des échanges de clés IKE. Ainsi, à chaque échange de clés on acquiert la garantie que les échanges antérieurs à cet échange sont définitivement protégés même en cas de compromission ultérieure du secret. C'est, entre autre, pour cette raison qu'il est nécessaire de définir une plage d'utilisation des clés à la fois en temps et en volume de données.

Cette propriété n'est vérifiée que dans le cas de l'utilisation d'IKE ; elle ne l'est pas lors d'une mise à la clé manuelle. Il est possible avec certains équipements d'améliorer la granularité de cette propriété en utilisant un second échange de clé en phase 2 (plutôt que de dériver toutes les clés de celle négociée en phase 1), échange qui sera renouvelé plusieurs fois au cours de la durée de vie d'une SA. Cela a en pratique pour effet de raccourcir la « session » évoquée ci-dessus, en la renouvelant plus fréquemment. Il est généralement possible d'associer un critère temporel et un critère de quantité de données échangée : le premier quota atteint provoque un renouvellement de clés.

R12

Dès lors que cette possibilité est offerte par les équipements employés, il est recommandé de mettre en œuvre la propriété PFS en phase 2 en utilisant dans le « quick mode » l'échange de clé Diffie-Hellman éphémère classique ou sa variante sur courbes elliptiques.

R13

Dès lors que cette possibilité est offerte par les équipements employés, il est recommandé de forcer le renouvellement périodique des clés, par exemple toutes les heures et tous les 100 Go de données, afin de limiter l'impact de la compromission d'une clé sur le trafic des données.

Note : La définition exacte de la période de renouvellement (cryptopériode) relève d'un choix organisationnel et de l'analyse de risque propre à un déploiement.

6.7 Choix des paramètres

Le choix des algorithmes cryptographiques et le dimensionnement des clés est traité dans le référentiel général de sécurité (annexe B1 « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » disponible sur www.ssi.gouv.fr/rgs), seul document faisant foi.

R14

Il est fortement déconseillé d'employer la fonction de hachage MD5, le chiffrement DES, des clés RSA de taille inférieure à 2048 bits ou des clés ECDSA de taille inférieure à 200 bits.

R15

Il est déconseillé d'utiliser 3DES, SHA-1 ou ECDSA avec des clés de moins de 256 bits si des alternatives plus sécurisées telles qu'AES (AES-128 ou AES-256), SHA-2 (SHA-224, SHA-256, SHA-384 ou SHA-512) ou ECDSA avec des clés d'au moins 256 bits sont disponibles.

R16

On prendra garde au groupe de Diffie-Hellman employé. Les groupes 1 ou 2, très fréquemment proposés dans les configurations par défaut, ne sont plus d'une taille acceptable. On privilégiera les groupes ayant des modules de taille plus importante (comme les groupes 14 et 15) voire (si possible) les groupes construits sur des courbes elliptiques d'au moins 256 bits (comme la courbe `ecp256`, aussi nommée groupe 19 ou encore la courbe `ecp384bp`, normalisée sous l'appellation groupe 29).

RECOMMANDATIONS DE SÉCURISATION D'UN PARE-FEU STORMSHIELD NETWORK SECURITY (SNS) EN VERSION 2.7.2

GUIDE ANSSI

ANSSI-BP-031
27/12/2017

PUBLIC VISÉ :

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

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurisation d'un pare-feu Stormshield Network Security (SNS) en version 2.7.2** ». Il est téléchargeable sur le site `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`). Il est par conséquent diffusable sans restriction.

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

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	27/04/2016	Version initiale
2.0	27/12/2017	Intégration SNS v2.7.2

Table des matières

1
Préambule

Ce document a pour objectif de présenter les bonnes pratiques relatives au déploiement sécurisé des pare-feux Stormshield Network Security (SNS), en version physique ou en version virtuelle [1]. Les recommandations détaillées dans ce document traitent des fonctions

- d'administration ;
- de filtrage ;
- de chiffrement IPsec ;
- de supervision ;
- de sauvegarde ;
- de journalisation.

Ce document vient en complément des publications [6] et [10] de l'ANSSI relatives aux pare-feux.

Information

Les fonctionnalités présentées dans ce guide ne se limitent pas à celles évaluées lors de la qualification du produit. Les fonctionnalités non évaluées sont précisées dans le corps du présent document à l'aide de la formule « *Cette fonctionnalité n'est pas couverte par la cible de sécurité.* ».

L'utilisation des fonctionnalités non évaluées nécessite donc une analyse de risque complémentaire qui doit être portée auprès de la commission d'homologation du SI. C'est ensuite à l'autorité d'homologation d'accepter les risques résiduels ou de mettre en place les protections adaptées.

1.1 Dénominations

Les sigles présentés dans cette section, en rapport avec les pare-feux SNS, sont utilisés tout au long du document.

- **AC** : Autorité de Certification.
- **CRL** : *Certificate Revocation List*, liste de révocation de certificats.
- **CRLDP** : *CRL Distribution Point*, point de distribution de CRL.
- **DNS** : *Domain Name System*, service effectuant la traduction entre des noms de domaines et les adresses IP associées.

1. Les contraintes liées à la virtualisation ainsi que les bonnes pratiques sont expliquées dans le guide [4].

- **DR** : Diffusion Restreinte.
- **DSCP** : *Differentiated Services Code Point*, champ de l'entête d'un paquet IP utilisé pour différencier et prioriser les services lors d'une congestion.
- **FQDN** : *Fully Qualified Domain Name*, nom de domaine renseignant l'ensemble des domaines à traverser pour joindre la ressource.
- **FTP** : *File Transfer Protocol*, protocole de transfert de fichiers.
- **HTTP** : *HyperText Transfer Protocol*, protocole de transfert hypertexte.
- **HTTPS** : *HTTP Secure*, évolution sécurisée du HTTP grâce à la mise en place d'un canal SSL/TLS.
- **IDS** : *Intrusion Detection System*, mécanisme permettant de détecter un trafic malicieux et de lever une alarme.
- **IGC** : Infrastructure de Gestion de Clés.
- **IKE** : *Internet Key Exchange*, protocole d'échange de clé authentifiant entre correspondants.
- **IP** : *Internet Protocol*, protocole de communication de réseaux informatiques.
- **IPsec** : *Internet Protocol Security*, cadre de standards permettant de sécuriser des communications IP.
- **IPS** : *Intrusion Prevention System*, mécanisme permettant de détecter un trafic malicieux et de le bloquer.
- **LDAP** : *Lightweight Directory Access Protocol*, protocole d'accès à des services d'annuaire.
- **LDAPS** : *LDAP Secure*, évolution sécurisée du LDAP grâce à la mise en place d'un canal SSL/TLS.
- **NSRPC** : *NetAsq Secure Remote Protocol Client*, protocole d'administration Stormshield utilisant le port TCP 1300.
- **QoS** : *Quality of Service*, qualité de service.
- **SI** : Système d'Information.
- **SIEM** : *Security Information and Event Management*, gestionnaire d'informations de sécurité et d'évènements.
- **SNS** : *Stormshield Network Security*.
- **SSH** : *Secure SHell*, protocole de communication sécurisé.
- **SSL** : *Secure Sockets Layer*, protocole de sécurisation d'échanges.
- **URL** : *Uniform Ressource Locator*, chaîne de caractères utilisée pour adresser une ressource sur un réseau.
- **TCP** : *Transport Control Protocol*, protocole de transport.
- **TLS** : *Transport Layer Security*, évolution de SSL.
- **VLAN** : *Virtual Local Area Network*, réseau de commutation logique.
- **VPN** : *Virtual Private Network*, système permettant de créer un tunnel de communication entre deux équipements.

2
Administration du pare-feu

2.1 Comptes administrateurs

2.1.1 Utilisation de comptes nominatifs

Il est important de pouvoir assurer la traçabilité de l'ensemble des actions réalisées sur le pare-feu (voir le chapitre 10 pour les recommandations liées à la journalisation) afin de s'assurer qu'elles ont été menées par un administrateur légitime et autorisé.

R1

Utiliser des comptes nominatifs

Il est recommandé d'utiliser des comptes nominatifs pour les administrateurs, quels que soient leurs privilèges, lors d'une connexion à l'interface web ou au serveur d'administration (NSRPC).

Certaines opérations exceptionnelles ne sont pas réalisables depuis un compte nominatif. Ces opérations sont par exemple :

- la modification manuelle de fichiers de configuration ;
- l'usage de `tcpdump` en vue d'une analyse du trafic réseau ;
- la modification des droits accordés aux admininistrateurs.

Un compte administrateur local non nominatif (admin) est présent sur l'équipement et peut réaliser ces actions depuis l'interface web, la console locale ou par SSH.

R2

Protéger le compte administrateur local

Le compte administrateur présent sur l'équipement doit disposer d'un mot de passe fort (se référer au guide [3]) et ne doit être utilisé qu'afin de rétablir l'accès aux comptes nominatifs. Son mot de passe doit être conservé au coffre-fort et son utilisation doit être supervisée et limitée à un ensemble déterminé de personnes.

R3

Limiter l'administration par SSH

Le service SSH étant limité au seul compte administrateur, il ne doit être activé qu'à titre exceptionnel à partir du menu `Système` → `Configuration` → `Administration du Firewall`.

R4

Utiliser une authentification par mot de passe pour SSH

Lorsque l'accès SSH est activé à titre exceptionnel, il est recommandé d'utiliser une authentification par mot de passe et de modifier ce dernier à chaque utilisation.

2.1.2 Authentification locale

Les pare-feux SNS offrent la possibilité de créer un annuaire interne (menu `Utilisateurs` → `Configuration de l'annuaire`) permettant une authentification locale. Cette authentification est utilisée pour la connexion aux serveurs web et NSRPC. Dans ce cas, le pare-feu stocke les éventuels mots de passe ou leurs dérivés. Une compromission de l'équipement compromet alors également ces éléments secrets. Il est également possible de s'authentifier sur l'interface web d'administration à l'aide d'un certificat. Leur utilisation permet de ne stocker que des données publiques au sein du pare-feu. Les recommandations associées à l'utilisation de certificats sur des équipements SNS sont présentées dans la section 6. L'accès au serveur NSRPC n'autorise cependant qu'une authentification par mot de passe.

R5

Authentifier localement par certificat

Si l'authentification locale est utilisée, il est recommandé d'utiliser des certificats utilisateurs nominatifs comme moyen d'authentification à l'interface web d'un équipement SNS.

Les autorités de certification doivent alors avoir été ajoutées dans le menu `Objets` → `Certificats et PKI` et la méthode d'authentification *Certificat SSL* configurée dans le menu `Utilisateurs` → `Authentification` → `Méthodes disponibles` avec les autorités souhaitées.

R6

Définir une politique de mots de passe adaptée

Si un accès NSRPC est nécessaire à un administrateur, son mot de passe doit suivre une politique conforme au guide [3] et configurée dans le menu `Système` → `Configuration` → `Configuration générale`.

2.1.3 Authentification centralisée

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

La solution SNS peut utiliser une solution d'authentification centralisée. Sa mise en œuvre implique la gestion des utilisateurs sur un équipement distant. L'utilisation d'une telle solution permet de limiter les données stockées localement et de simplifier les procédures d'administration. Dans le cas de l'utilisation d'un annuaire externe, la configuration du pare-feu est détaillée à la section 4.4.

R7

Dédier un annuaire externe aux administrateurs

Conformément au guide [15], il est recommandé d'utiliser un annuaire externe et dédié à l'administration pour authentifier les administrateurs.

R8

Utiliser un compte d'accès restreint et sécurisé

Le compte utilisé par le pare-feu pour accéder à la solution d'authentification centralisée doit être limité à cette fonction, dédié au pare-feu et disposer d'une sécurité forte. En particulier, il ne doit avoir que des droits en lecture afin d'éviter toute modification des données de l'annuaire à partir de l'équipement SNS.

2.1.4 Droits d'accès

Un pare-feu offre de nombreuses fonctionnalités : filtrage, tunnels VPN, etc. Un administrateur dédié à une tâche précise ne doit avoir qu'un périmètre d'action limité. Cela permet de cloisonner les risques en cas de compromission de son compte, ainsi que limiter les modifications involontaires de configuration.

R9

Ajuster les droits d'administration

Il est recommandé de ne positionner que les droits strictement nécessaires aux tâches des différents administrateurs dans le menu `Système` → `Administrateur`.

Il n'est pas possible d'utiliser la valeur d'un attribut de l'annuaire afin de discriminer les différents profils de droits (administrateur complet, administrateur dédié à une fonction, superviseur, etc.). Il est cependant possible de déclarer des groupes d'utilisateurs au sein de l'annuaire et de leur appliquer un profil de droits sur le pare-feu. Chaque groupe doit correspondre à un besoin fonctionnel et bénéficier des droits adaptés sur le pare-feu. L'attribution de droits à un administrateur est alors effectuée par son affectation à un groupe. Cela se réalise dans l'annuaire de manière centralisée.

R10

Utiliser les groupes pour gérer les droits

Il est recommandé d'utiliser les groupes pour gérer les droits d'accès aux équipements SNS.

Attention

Seul le compte administrateur non nominatif peut modifier les droits des utilisateurs et groupes d'utilisateurs. Cette action doit donc rester exceptionnelle conformément à la section 2.1.1.

Information

Différentes méthodes d'authentification centralisée sont disponibles, cependant la gestion des autorisations par groupes d'utilisteurs n'a été testée que dans le cadre d'un annuaire externe.

2.2 Services d'administration

2.2.1 Configuration des adresses IP d'administration

Un accès non restreint aux interfaces d'administration du pare-feu augmente les risques de tentative d'intrusion et de manipulation par un équipement illégitime qui y aurait accès.

R11

Définir explicitement les sous-réseaux d'administration

Il est recommandé de définir explicitement les adresses IP ou les sous-réseaux d'administration autorisés à accéder aux interfaces d'administration d'un équipement dans le menu `Système` → `Configuration` → `Administration du Firewall`.

Les adresses IP et les sous-réseaux d'administration doivent être configurés à l'aide d'objets spécifiques, regroupés dans un groupe d'objets. Conformément à la section 5.4, l'utilisation de tels groupes d'objets permet une meilleure gestion des autorisations, en cohérence avec les règles de filtrage.

R12

Utiliser un groupe d'objets d'administration

Il est recommandé d'utiliser un groupe d'objets contenant l'ensemble des sous-réseaux et adresses IP autorisés à administrer le pare-feu.

2.2.2 Interface d'administration dédiée

Une interface d'administration mutualisée avec le réseau d'opérations augmente le nombre de personnes et d'équipements capables d'accéder à l'interface d'administration du pare-feu et augmente la charge de trafic que l'interface doit gérer. Le risque de voir l'interface d'administration attaquée ou injoignable est alors important. De plus, l'utilisation de VLANs ne garantit pas une étanchéité totale entre les réseaux configurés.

R13

Dédier une interface Ethernet à l'administration

Il est recommandé d'administrer un équipement SNS sur une interface Ethernet dédiée raccordée à un réseau d'administration. Le filtrage mis en œuvre devra être le plus restrictif possible.

Le guide [15] publié par l'ANSSI détaille les mesures recommandées concernant une administration sécurisée des SI.

2.2.3 Sécurité de l'interface web d'administration

La sécurité de l'interface web d'administration participe à la sécurité de l'équipement en protégeant en confidentialité et en intégrité les flux légitimes d'administration.

Par défaut, le mode `sslparanoiac` est activé, imposant l'utilisation de TLS 1.2 et de suites cryptographiques robustes. Il est possible de vérifier la configuration du paramétrage TLS de l'interface web d'administration à l'aide de la commande NSRPC `config auth show`. Les suites cryptographiques proposées par défaut sont les suivantes :

```
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
```

R14

Configuration des suites cryptographiques

Conserver la configuration par défaut des suites cryptographiques permet d'être conforme aux recommandations de l'ANSSI [8].

Information

L'utilisation de TLS 1.2 et de suites cryptographiques robustes nécessite un navigateur Internet récent.

R14 +

Durcir les paramètres TLS de l'interface d'administration

Il est recommandé de conserver uniquement les suites TLS avec `ECDHE` comme préconisé par le guide TLS [8].

La restriction des suites cryptographiques peut s'effectuer à l'aide de la commande NSRPC :

```
config auth https cipherlist="ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-SHA256,
ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-SHA384"
```

2.2.4 Modification du certificat de l'interface web d'administration

Par défaut, le certificat présenté à l'administrateur lorsqu'il se connecte à l'interface web d'administration est un certificat signé par l'AC NetAsq. La clé privée utilisée n'est alors pas maîtrisée, ni sur les critères de génération, ni sur l'utilisation qui peut en être faite.

R15

Remplacer le certificat de l'interface web

Il est recommandé de remplacer le certificat de l'interface web d'administration par un certificat issu d'une IGC maîtrisée [2] afin de renforcer la sécurité de son accès.

La configuration du certificat serveur utilisé par l'interface web d'administration de SNS se fait à partir du menu `Configuration` → `Système` → `Configuration` → `Administration du Firewall` → `Configurer le certificat SSL du service`.

Information

Afin qu'un administrateur puisse authentifier l'équipement sur lequel il se connecte, la clé publique de l'AC qui a signé le certificat doit être présente dans le magasin de certificats du navigateur utilisé par les administrateurs.

2.2.5 Administration via NSRPC

Dans le cas d'une connexion directe au serveur NSRPC, le pare-feu requiert l'accès en lecture à l'empreinte du mot de passe de l'utilisateur [3]. Un détournement de l'accès du pare-feu à l'annuaire peut alors entraîner la compromission de l'ensemble des empreintes des mots de passe stockés. L'empreinte est un élément critique, une attaque par force brute peut compromettre les mots de passe. Il est donc nécessaire de surveiller l'utilisation d'un tel compte dans le système d'information (connexion issue d'un autre équipement, requêtes illégitimes, etc.).

2. Se référer aux recommandations du RGS [11], en particulier les annexes A4 [14] et B1 [13].
3. Cette information est nécessaire au bon fonctionnement du protocole d'authentification utilisé.

Une console NSRPC est disponible depuis l'interface web. L'accès à cette console ne nécessite pas d'authentification supplémentaire. L'accès aux empreintes n'est pas nécessaire.

R16

Utiliser NSRPC depuis l'interface web

Il est recommandé d'utiliser les commandes NSRPC uniquement depuis le menu `Système` → `Console CLI` de l'interface web.

R16 -

Utiliser des comptes dédiés à la connexion NSRPC directe

Dans le cas d'un accès direct à la console NSRPC il est recommandé d'utiliser des comptes dédiés à cet usage et d'exposer uniquement les empreintes de ces comptes sur l'annuaire distant.

Information

Par défaut, les annuaires de type *Active Directory* et *OpenLDAP* n'autorisent pas la lecture des empreintes des mots de passe.

2.2.6 Choix des éléments de localisation

Plusieurs éléments de localisation sont présents sur l'équipement :

- la langue de l'interface web, qui peut être choisie sur l'écran de connexion ;
- la disposition du clavier de la console, configurable dans le menu `Système` → `Configuration` ;
- la langue des traces et des journaux, également configurable dans le menu `Système` → `Configuration`.

La langue des traces et des journaux modifie les messages disponibles dans le `Tableau de bord` et dans les fichiers de journalisation locaux et distants. Le choix de cette langue influe sur :

- leur compréhension par les exploitants ;
- les motifs recherchés par les systèmes de supervision ;
- les recherches effectuées dans la base de connaissance disponible sur le site internet de l'éditeur.

L'ensemble des messages existants est répertorié dans le menu `Notifications` → `Evènements systèmes` et leurs traductions sont disponibles dans le dossier `/usr/Firewall/System/Language/` de l'équipement. Chaque message émissible possède un numéro d'index lié à l'erreur correspondante. Ce numéro est donc identique au sein de l'ensemble des traductions.

R17

Unifier la langue des traces et des journaux

Il est recommandé de configurer une langue identique sur l'ensemble des équipements SNS pour la langue des traces et journaux. Ceci permet d'en simplifier la lecture et facilite l'intégration dans les outils de supervision.

R18

Utiliser une langue comprise par les exploitants

Il est conseillé de configurer un équipement dans une langue maîtrisée par les exploitants.

Information

La base de connaissance de l'éditeur Stormshield est composée en grande partie de pages en anglais. Cette base est accessible depuis l'espace personnel Stormshield [2].

2.3 Fonctionnalités système

2.3.1 Option Diffusion Restreinte

En cas d'utilisation d'un pare-feu SNS dans un contexte de sensibilité de niveau « Diffusion Restreinte », des contraintes supplémentaires doivent être appliquées afin de respecter les règles de protection appropriées [9]. En particulier, la gestion des primitives cryptographiques matérielles doit être adaptée lorsque que le jeu d'instructions du (co)processeur ne fournit pas les garanties suffisantes sur leur utilisation et leur protection (risques d'émission ou de fuite de données). L'utilisation de cette option implique en contrepartie une baisse des performances de chiffrement et de déchiffrement des pare-feux équipés de tels (co)processeurs.

R19

Option Diffusion Restreinte

Il est nécessaire d'activer le mode `Diffusion Restreinte` dans le menu `Système` → `Configuration` → `Configuration générale` lorsque le pare-feu est positionné sur un réseau de cette même sensibilité et que ses fonctions cryptographiques sont exploitées.

Information

Certains modèles de pare-feu SNS utilisent un processeur dont le jeu d'instructions cryptographiques offre des garanties suffisantes pour protéger des données de niveau DR. Il est conseillé de se rapprocher de l'éditeur Stormshield afin de connaître la liste des équipements concernés.

3
Configuration réseau

3.1 Désactivation des interfaces non utilisées

L'accès à des interfaces réseau inutilisées sur un équipement SNS augmente sa surface d'attaque car une connexion sur une telle interface ne perturbe pas le bon fonctionnement du pare-feu mais en permet un accès illégitime. De plus, une interface active est utilisable dans les différents menus et augmente le risque d'erreurs de configuration.

R20

Désactiver les interfaces non utilisées

Il est recommandé de désactiver les interfaces réseau non utilisées depuis le menu `Réseau → Interfaces`.

3.2 Configuration de l'antispoofing IP

3.2.1 Principe de l'antispoofing IP

Le *spoofing* IP consiste à usurper une adresse IP légitime dans le but de contourner les règles de filtrage mises en place. Ceci consiste par exemple à envoyer depuis un réseau externe des paquets ayant pour source une adresse IP interne à destination d'une autre adresse IP interne. Sans vérification des interfaces utilisées, le pare-feu interprète la requête comme légitime et provenant du réseau interne vers le réseau interne. Le trafic malicieux est alors routé comme du trafic interne légitime.

Afin de se protéger de ce type d'attaque, les mécanismes d'*antispoofing* sont activés par défaut. Ils consistent à vérifier sur chaque interface d'entrée la légitimité de l'adresse IP source des paquets. Cette légitimité repose sur la topologie réseau définie par :

- les interfaces réseau, pour les réseaux directement connectés ;
- la table de routage, pour les réseaux distants.

Information

En plus d'être un élément indispensable à la sécurité, l'*antispoofing* IP est extrêmement efficace pour détecter des erreurs de configuration réseau (mauvaise configuration de règles de routage par exemple).

3.2.2 Antispoofing sur les interfaces réseau

Un pare-feu SNS utilise la notion d'interface « interne » pour identifier les interfaces qui alimentent le mécanisme d'*antispoofing*. Le menu `Réseau → Interface → Configuration de l'interface` permet de configurer le type d'interface : un bouclier apparaît lorsqu'une interface est protégée par l'*antispoofing*. Dès lors, une telle interface n'acceptera que des paquets dont l'adresse IP source provient du réseau de commutation de l'interface. De plus, les autres interfaces du pare-feu refuseront ces mêmes paquets en entrée. Ces règles d'*antispoofing* sont appliquées avant même l'évaluation de la politique de filtrage réseau.

Information

Il est possible de compléter la liste des adresses IP autorisées à accéder à une interface « interne » en utilisant l'*antispoofing* par la table de routage décrit à la section 3.2.3.

R21

Déclarer les interfaces internes

Afin de profiter des mécanismes d'*antispoofing*, il est recommandé de déclarer une interface « interne ».

Attention

Des règles implicites de filtrage autorisent l'administration des équipements à partir des interfaces internes. Ces règles devront êtres désactivées comme expliqué à la section 5.2.

3.2.3 Antispoofing par la table de routage

La définition des routes statiques renseigne le pare-feu sur la topologie réseau et complète implicitement les mécanismes d'*antispoofing*. Toute route à destination d'un réseau distant joignable par une interface « interne » est ajoutée aux tables d'*antispoofing*. Ainsi si des paquets dont l'adresse IP source est déclarée joignable par une interface « interne » sont reçus sur une autre interface, ils seront rejetés avant même l'évaluation de la politique de filtrage réseau en place sur le pare-feu. Les routes utilisant des interfaces « externes » ne sont pas protégées car, en général, elles servent à répondre à des équipements dont les adresses IP sources ne sont pas connues à l'avance.

R22

Définir des routes statiques pour les réseaux internes

Il est nécessaire de définir des routes statiques pour l'ensemble des réseaux internes connus auxquels les interfaces du pare-feu n'appartiennent pas afin de profiter des mécanismes d'*antispoofing*. Ces routes sont reconnaissables dans le menu `Réseau → Routage → Routage statique` par la présence d'un bouclier.

Attention

Il est nécessaire de déclarer des routes pour l'intégralité des réseaux distants joignables par les interfaces « internes ». Dans le cas contraire, leurs paquets seront systématiquement rejetés par le pare-feu.

3.2.4 Antispoofing sur un bridge

Un *bridge* permet de connecter plusieurs interfaces physiques sur un même réseau. Le pare-feu applique toutefois ses mécanismes d'*antispoofing* indépendamment sur chacune des interfaces du *bridge*.

Lorsque les équipements sont sur le même réseau de commutation que le pare-feu, celui-ci maintient à jour une table (dite table des hôtes) contenant chaque adresse IP rencontrée et l'interface physique associée. Si une adresse est détectée sur une autre interface que celle renseignée, une alerte est alors levée.

Attention

La table des hôtes n'est renseignée qu'à partir du premier paquet envoyé par un équipement. L'*antispoofing* du *bridge* ne protège donc pas un interlocuteur directement connecté et n'ayant encore émis aucun trafic.

Dans le cas de réseaux distants, des règles de routage sont nécessaires, précisant l'interface physique utilisée. L'*antispoofing* par la table de routage détaillé au paragraphe 3.2.3 est employé.

3.2.5 Règles complémentaires

Certaines configurations ne peuvent pas être prises en compte par les mécanismes d'*antispoofing* natifs de l'équipement. En particulier, un certain nombre de plages d'adresses particulières définies dans la RFC 5735 sont pré-configurées dans l'équipement au sein d'un groupe spécifique. Ces plages concernent des réseaux privés et ne devraient pas être utilisées sur une interface publique

R23

Compléter les règles d'antispoofing

Il est recommandé de compléter autant que possible les règles d'*antispoofing* citées précédemment par des règles de filtrage déduites de la topologie réseau. Par exemple, il est recommandé d'interdire explicitement les plages d'adresses du groupe RFC 5735 en provenance d'Internet.

4
Configuration des services

4.1 Accès Internet

Certaines fonctionnalités d'un équipement SNS nécessitent des mises à jour régulières (activées par défaut dans le menu `Système → Active Update`). L'absence totale de mises à jour empêcherait le pare-feu d'obtenir des correctifs de sécurité et le renouvellement de bases d'informations. Ces mises à jour peuvent être réalisées :

- hors ligne par la mise en place d'un miroir interne ;
- en ligne, à travers un serveur proxy ou en direct.

Si la mise à jour se fait en ligne, il y aura autant de flux de gestion que d'équipements SNS dans le SI. Cela peut occasionner une surconsommation de la bande passante. L'utilisation d'un miroir interne permet alors de restreindre le nombre d'équipements autorisés à accèder à Internet.

R24

Mettre à jour depuis un miroir interne

Il est recommandé de mettre à jour régulièrement les services par l'activation des mises à jour automatiques et d'utiliser un miroir interne.

Pour une utilisation en ligne, il est recommandé de s'assurer que la connexion vers le serveur de mise à jour est uniquement utilisée par le pare-feu, vers cette seule destination et à cette seule fin. Cela peut se réaliser par la configuration d'un serveur proxy authentifiant. Le compte d'accès utilisé au niveau du proxy doit être un compte dédié et disposer d'accès restreints aux besoins de l'équipement (filtrage d'URL et de flux IP strictement nécessaires aux opérations de mise à jour d'équipements SNS [4]).

R24 -

Mettre à jour au travers d'un proxy

En l'absence de miroir interne, l'équipement SNS doit accéder au miroir en ligne sur Internet au travers d'un proxy authentifiant avec un compte dédié et une politique de filtrage adaptée.

4.2 DNS

L'utilisation de certains services (par exemple *proxy web*) nécessite la résolution de noms de domaine. Dans le cas d'une compromission des serveurs DNS utilisés, un attaquant peut alors rediriger

4. À savoir les URL update{1,2,3,4}.stormshield.eu et licence{1,2,3,4}.stormshield.eu.

les flux vers des correspondants illégitimes.

R25

Choisir des serveurs DNS maîtrisés

Il est recommandé de configurer des résolveurs DNS maîtrisés dans le menu `Système → Configuration → Paramètres réseaux`

R25 -

Modifier les serveurs DNS par défaut

Il est recommandé de remplacer les résolveurs DNS configurés par défaut par ceux du fournisseur d'accès si aucun n'est maîtrisé dans le SI.

La base d'objets d'un équipement SNS permet de créer des objets de type statique ou dynamique. Ces derniers dépendent d'un nom de domaine régulièrement résolu par le pare-feu. Il en existe par défaut une quinzaine qui portent un nom se terminant par netasq.com ou stormshield.eu dont une partie est représentée sur la figure 4.1 [5]. Cela génère des requêtes DNS inutiles et intempestives qui ne peuvent pas être bloquées par des règles de filtrage.

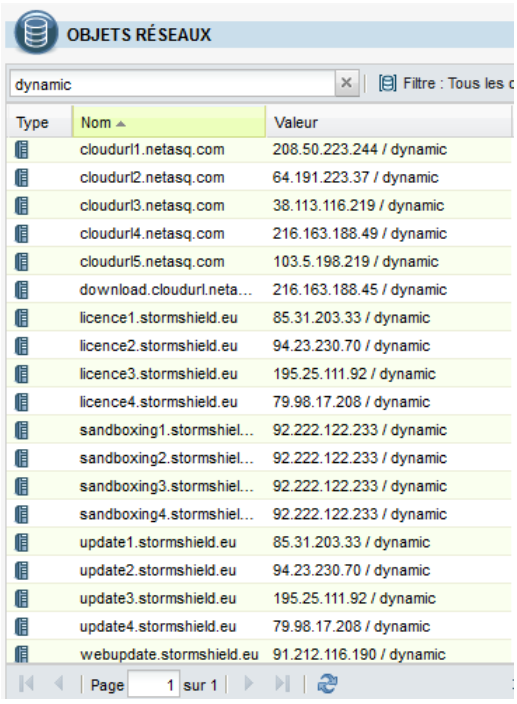


FIGURE 4.1 – Liste des objets dynamiques de type « Machine ».

L'utilisation d'un miroir interne (recommandation R24) permet à un équipement SNS de ne pas avoir à contacter directement les serveurs de mise à jour de l'éditeur Stormshield. De plus, l'utilisation de serveurs DNS maîtrisés (recommandation R25) permet de déporter la gestion des adresses des autres services de l'éditeur (gestion des licences, etc.).

R26

Limiter l'usage des objets dynamiques

Il est recommandé de supprimer les objets dynamiques non utilisés et de reconfigurer les objets restants en mode statique dans le menu `Objets → Objets réseaux`.

5. Ces noms peuvent évoluer en fonction des mises à jours de l'éditeur.

4.3 NTP

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

Certaines fonctionnalités sont fortement liées à l'heure du système, notamment la journalisation et la gestion des certificats. La configuration manuelle de l'heure ne permet pas une bonne intégration de l'équipement dans un SI. De plus, la seule utilisation de l'horloge interne ne garantit pas l'absence de dérive sur une longue période.

R27

Synchroniser l'heure du système

Il est recommandé d'activer la synchronisation NTP des équipements SNS et d'utiliser plusieurs serveurs de temps fiables.

4.4 Utilisation d'un annuaire externe

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

Diverses fonctionnalités, dont l'authentification des administateurs, nécessitent la connexion à un annuaire. Lorsque ce dernier est externe au SNS, la sécurité (confidentialité et intégrité) des flux échangés doit être assurée et l'authentification des équipements (pare-feu et serveur d'annuaire) doit être réalisée. Dans le cas contraire, un attaquant peut obtenir des informations de connexion.

R28

Configurer LDAP de manière sécurisée

Si le service LDAP est configuré, il est recommandé :

- d'utiliser le protocole LDAPS ;
- d'installer un certificat provenant d'une IGC maîtrisée sur le serveur LDAP ;
- d'importer l'AC correspondante sur l'équipement SNS ;
- d'utiliser l'AC précédemment importée pour valider la connexion au serveur LDAP.

La mise en place d'une authentification à partir d'un annuaire externe se réalise en plusieurs étapes :

- activer l'utilisation de l'annuaire (menu `Configuration` → `Utilisateurs` → `Configuration de l'annuaire`), choisir son type puis paramétrer l'accès :
  - l'adresse de l'annuaire ;
  - la base DN ;
  - le port de communication ;
  - l'identifiant et le mot de passe du compte d'accès du pare-feu sur l'annuaire. Ce compte doit respecter la recommandation R8 ;

- définir la structure de l'annuaire (onglet `Structure`). La correspondance entre les attributs manipulés par l'équipement SNS et ceux présents dans l'annuaire LDAP doit être établie. L'attribut Stormshield `member` (qui contient la liste des identifiants appartenant à un groupe) doit en particulier correspondre à son équivalent dans l'annuaire LDAP ;
- définir LDAP comme méthode d'authentification par défaut (menu `Configuration` → `Utilisateurs` → `Authentification`).

Information

En version 2.7.2, la solution SNS ne permet de configurer qu'un seul annuaire. Il n'est donc pas possible d'utiliser la méthode LDAP pour authentifier des administrateurs et des utilisateurs tout en respectant les règles de séparation des annuaires du guide [15]. Si seuls des administrateurs s'authentifient via l'annuaire LDAP, cet annuaire doit par contre leur être dédié.

5
Politique de filtrage réseau et de NAT

5.1 Nommage de la politique de filtrage réseau

Par défaut, les politiques de filtrage présentes sur un équipement SNS ne portent pas de nom explicite, à l'exception de deux d'entre-elles (Pass all, Block all). Cette pratique ne permet pas à un administrateur de facilement comprendre le rôle du pare-feu, ni de savoir quelle politique appliquer si plusieurs sont configurées. L'application d'une convention de nommage permet de :

- refléter la fonction du pare-feu dans le nom de la politique de filtrage (accès Internet, isolation d'un partenaire, etc.) ;
- minimiser les erreurs de manipulation (activation de la mauvaise politique) ;
- disposer d'une configuration homogène au niveau de l'intitulé des politiques de filtrage réseau de l'ensemble des pare-feux présents au sein du SI.

R29

Renommer la politique de production

Il est recommandé d'appliquer une politique de nommage des profils de filtrage réseau comme détaillé dans le guide [6].

5.2 Règles implicites

Par défaut, le pare-feu est configuré avec des règles implicites de filtrage, évaluées avant les règles de filtrage définies manuellement. Ces règles ont pour but de simplifier la configuration en autorisant des requêtes ou des accès particuliers. Le menu `Politique de sécurité` → `Filtrage et NAT` ne contient alors pas toutes les règles appliquées par le pare-feu. Par conséquent, il est possible qu'une règle créée par un administrateur ne soit jamais évaluée à cause de la présence d'une règle implicite contraire.

R30

Désactiver les règles implicites

Il est recommandé de désactiver la totalité des règles de flux implicites, incluant celles concernant les flux sortants issus des services hébergés par le pare-feu. Cela se réalise dans le menu `Politique de sécurité` → `Règles implicites`.

Attention

Afin d'éviter de perdre les capacités d'administration, il est nécessaire de créer de nouvelles règles de filtrage avant de désactiver les règles implicites correspondantes. Ces règles doivent autoriser, en fonction des besoins, le trafic HTTPS, NSRPC ou SSH entre le pare-feu et les groupes définis à la section 2.2.1 sur les interfaces définies à la section 2.2.2.

Information

La commande `sfctl -s filter` passée en console permet d'afficher l'ensemble des règles de filtrage appliquées. En l'occurrence, il est possible de constater que la désactivation des flux implicites des services hébergés ne bloque pas les requêtes DNS émises par le SNS. L'application de la recommandation R26 limite ces flux.

5.3 Analyse protocolaire

Certains flux malveillants peuvent avoir les mêmes caractéristiques réseau que des flux autorisés. Le blocage de ces flux est impossible par de simples règles de filtrage sans impact sur le trafic légitime. L'équipement SNS est doté de capacités d'analyses protocolaires permettant un filtrage fin. L'inspection effectuée sur les flux traités par une règle de filtrage peut être paramétrée suivant un des trois niveaux disponibles : Firewall, IPS ou IDS.

Au niveau Firewall, le pare-feu n'effectue que des vérifications sommaires de conformités. En particulier, il contrôlera le respect du sens d'établissement des connexions. Il ne vérifiera ni les drapeaux utilisés, ni les numéros de séquence, ni les options TCP.

Attention

Au niveau Firewall, lorsqu'une session est abandonnée par le pare-feu, il envoie un paquet de réinitialisation possédant un numéro de séquence nul. Le correspondant, ne pouvant le relier à une connexion existante, n'en clôturera aucune.

Au niveau IPS, le pare-feu effectue des vérifications supplémentaires sur le respect des protocoles, ainsi que des analyses reposant sur des signatures d'attaques déjà connues. Ces analyses sont réalisées grâce à des modules d'inspection dédiés à chaque protocole. Suivant le réglage mis en place, le module concerné pourra bloquer les flux identifiés comme malveillants.

Le niveau IDS réalise les mêmes inspections que le niveau IPS, mais ne lèvera que des alarmes si du trafic semble malveillant, sans le bloquer. Le niveau IDS peut être utilisé en pré-production pour analyser les flux qui transitent dans un système et ainsi faciliter l'action de l'administrateur dans sa tâche visant à configurer les modules d'inspection.

Aux niveaux IPS et IDS, il existe différents modes de fonctionnement :

- par défaut, les modules d'inspection sont chargés automatiquement, en fonction des ports utilisés dans les règles de filtrage et des caractéristiques du trafic observé par l'équipement. Dans la suite, nous parlerons alors de « mode automatique » ;

- il est également possible de limiter le chargement de ces modules en indiquant ceux à utiliser dans la règle de filtrage. Dans ce cas, le pare-feu n'effectuera que les analyses correspondant au protocole demandé. Nous utiliserons dans ce document le terme de « mode transport » dès lors que les modules indiqués sont uniquement des protocoles de transport (TCP, UDP…) ;
- les modules peuvent aussi concerner un protocole applicatif particulier. Nous utiliserons par la suite la notion de « mode applicatif ». Dès lors que les modules chargés ont fait l'objet d'une évaluation dans le cadre de la qualification [6], nous utiliserons la dénomination « mode applicatif qualifié ».

Le niveau IPS en mode automatique est sélectionné par défaut à la création d'une règle de filtrage. Cependant, le chargement de modules d'analyses protocolaires augmente la charge processeur du pare-feu ainsi que sa surface d'attaque. Dans la mesure du possible, il convient de faire réaliser les fonctions d'analyse protocolaire par des équipements dédiés comme des serveurs proxy afin de limiter le risque de compromission du pare-feu.

R31

Adapter l'inspection au rôle de l'équipement

Il est recommandé d'utiliser les niveaux Firewall, IPS en mode transport ou IPS en mode applicatif qualifié en cohérence avec le rôle joué par l'équipement dans l'architecture du système d'information considéré. En particulier, il convient d'être vigilant quant à son exposition aux menaces, à son rôle et à la criticité des ressources à protéger.

Le niveau d'analyse et le mode associé sont à définir pour chaque règle de filtrage et varient en fonction du rôle de l'équipement. Par exemple :

- si l'équipement est utilisé exclusivement en tant que passerelle VPN en bordure de SI et qu'il est lui-même protégé par d'autres pare-feux, le niveau Firewall permet de dédier ses ressources aux fonctions cryptographiques tout en réduisant sa surface d'attaque ;
- si le pare-feu est situé entre un SI d'entreprise et le réseau Internet, le niveau IPS en mode transport permet de limiter la surface d'attaque de l'équipement tout en assurant un filtrage fin des connexions ;
- si le pare-feu protège des serveurs applicatifs joignables uniquement depuis le réseau interne d'une entreprise, le niveau IPS en mode applicatif qualifié peut être utilisé.

La colonne `Inspection de sécurité` des règles de filtrage (menu `Filtrage et NAT`) permet de choisir le niveau d'inspection, Firewall, IPS ou IDS. Dans les cas de l'IPS et de l'IDS, la colonne `Protocole` permet de limiter le niveau d'analyse. L'option `Type de protocole` positionnée à `Protocole IP` permet de choisir un protocole de transport dans le menu `Protocole IP`. Si cette option est positionnée à `Protocole applicatif`, le menu du même nom permet de choisir le protocole applicatif sur lequel l'équipement agira. Un seul protocole (applicatif ou de transport) peut être choisi par règle de filtrage.

Les niveaux IPS et IDS reposent sur l'utilisation de Profils d'inspection. Ces profils permettent de configurer le comportement du pare-feu en fonction du trafic traité (types d'alarmes à lever,

6. Il s'agit des modules liés aux protocoles suivants : FTP, HTTP (incluant WebDAV), SIP, SMTP, DNS, Modbus, S7 et UMAS.

blocage du flux). Avant le passage en production de l'inspection protocolaire, dans un environnement réputé sain (typiquement un environnement de pré-production), il est souhaitable de désactiver les alarmes qui seraient inutilement générées par le trafic légitime afin de ne pas polluer la supervision de sécurité après le passage en production. L'utilisation de multiples profils doit permettre d'ajuster les configurations au contexte d'emploi. Il est en particulier recommandé de créer des profils d'inspection plus fins et donc plus restrictifs pour les applications les plus critiques.

R32

Adapter les profils d'inspection en fonction du contexte d'emploi du pare-feu

Lorsque l'analyse protocolaire est active, il est recommandé d'ajuster au mieux la politique aux réseaux à protéger en s'appuyant sur différents profils d'inspection.

Parmi les profils d'inspection pré-configurés, deux sont utilisés par défaut : le profil `00` en entrée et le profil `01` en sortie. Le choix du profil se fait à chaque règle de filtrage, à l'onglet `Inspection de sécurité`. La configuration de ces profils se fait dans le menu `Protection applicative` → `Profils d'inspection`, en sélectionnant `Accèder aux profils`. Chaque profil est alors basé sur les politiques définies au menu `Protection applicative` → `Protocoles`. Ces politiques définissent les analyses générales réalisées sur les différents protocoles : les ports par défaut, les commandes à restreindre, le type d'analyse à effectuer, etc. De plus, le menu `Protection applicative` → `Applications et protections` définit les analyses plus spécifiques comme la recherche de *buffer overflow*, de format d'encodage, etc. Ce menu propose une vue par profil ou par contexte.

5.4 Politique de filtrage

Sur un équipement Stormshield, il peut être nécessaire d'utiliser les mêmes objets à plusieurs reprises, s'ils apparaissent dans plusieurs règles de filtrages ou lorsque ces dernières viennent en complément d'un menu de configuration. Par exemple, un même sous-réseau peut apparaître dans plusieurs règles de filtrage (réseau de postes de travail vers un serveur de mail, vers un proxy web, etc.), ou en tant que réseau d'administration (se référer à la section 2.2.1) et au sein d'une règle de filtrage explicite corrélée (conformément à la section 5.2).

Lors d'éventuels changements (par exemple de plan d'adressage), ajouts (nouveaux sous-réseaux pour accueillir de nouveaux postes de travail) ou suppressions (restriction du nombre de postes d'administration), les mises à jour doivent être réalisées à chacune des occurrences, ce qui augmente les risques d'erreur de configuration et d'oubli. L'utilisation d'objets et de groupes d'objets permet un traitement global et simultané sur l'ensemble de la configuration lors d'un changement.

R33

Utiliser des groupes d'objets

Il est recommandé d'utiliser des groupes d'objets lors de la définition des règles de filtrage en cohérence avec les autres menus.

Dans ce cas, il est possible de maîtriser par exemple :

- un groupe d'administration comprenant les adresses IP des postes d'administration ;

- un groupe des postes utilisateur comprenant les sous-réseaux IP utilisés ;
- un groupe de service comprenant les adresses IP des serveurs internes ;
- un groupe métier comprenant les ports utilisés par les applications métier ;
- etc.

Il est alors suffisant de retirer ou ajouter un élément à un groupe pour s'adapter à une nouvelle situation.

Par ailleurs, les bonnes pratiques relatives à la définition d'une politique de filtrage réseau sont détaillées dans un guide spécifique [6]. Ce document a pour objectif principal de présenter l'organisation à adopter afin de garantir une politique de filtrage pérenne et maîtrisée.

6
Certificats et PKI

Plusieurs cas d'usage impliquent l'utilisation de certificats par des équipements SNS, dont :

- la publication de l'interface d'administration web en HTTPS ;
- l'authentification par certificat des administrateurs pour l'accès à l'interface web d'administration de SNS ;
- l'authentification d'utilisateurs et de passerelles dans le cadre de la mise en place de tunnels VPN IPsec ;
- l'authentification d'utilisateurs et de passerelles dans le cadre de la mise en place d'un service de VPN SSL/TLS ;
- la connexion à un annuaire externe en LDAPS.

6.1 Utilisation d'une IGC

Lorsqu'un équipement est impliqué dans un mécanisme d'authentification, ce dernier peut reposer sur des certificats issus d'une IGC. La confiance placée dans cette IGC détermine alors la confiance du certificat utilisé et donc la fiabilité de l'authentification. En cas d'absence de solution externe de gestion des certificats, les pare-feux SNS offrent la possibilité de générer une autorité de certification ainsi que des certificats signés par cette autorité. Dans ce cas, les clés privées sont générées par et stockées sur le pare-feu. La compromission du pare-feu compromet alors également ces éléments secrets.

R34

Utiliser une IGC maîtrisée externe

Il est recommandé d'utiliser une IGC maîtrisée externe à l'équipement SNS pour générer les certificats utilisés par le pare-feu. Cette IGC ainsi que les AC utilisées doivent être conformes aux préconisations du RGS [12].

R34 -

Utiliser l'IGC de l'équipement

En l'absence d'IGC externe, il est possible d'utiliser l'IGC présente dans l'équipement. Dans ce cas

- les éléments secrets générés doivent être supprimés du pare-feu après leur export vers les équipements destinataires ;
- les administrateurs de l'IGC doivent être uniquement dédiés à ce rôle (voir la recommandation R9)

Attention

Lorsque l'IGC interne à l'équipement est configurée, la compromission de l'équipement SNS permet à un attaquant de se forger une identité qui sera considérée comme légitime sur le SI. Il est donc important de limiter cette fonction aux équipements les moins exposés possible à des réseaux non maîtrisés.

6.2 Gestion des CRLs dans le cadre d'un tunnel IPsec

Un certificat peut être révoqué par son AC avant son expiration prévue. Cela arrive par exemple lorsqu'une clé privée est compromise ou qu'un administrateur quitte la société. L'acceptation d'un tel certificat permet alors à un utilisateur ou équipement illégitime de bénéficier d'une authentification sur le pare-feu. La mise en place par l'IGC de CRLs permet d'avertir les équipements concernés de la révocation de certificats. Par défaut l'absence de CRL n'est pas bloquante pour établir un VPN IPsec, elle est simplement signalée dans les journaux de l'équipement.

R35

Imposer la vérification des CRLs

Il est recommandé d'imposer la vérification de CRLs pour la mise en œuvre des tunnels IPsec.

Le changement de ce comportement est à effectuer en modifiant le paramètre `CRLrequired` puis en relançant le service IPsec. Cela se réalise par les commandes NSRPC suivantes :

```
config ipsec update slot=01 CRLrequired=1
config ipsec activate
```

Ce paramètre est stocké dans le fichier `/Firewall/ConfigFiles/VPN/01/`. En mode console, le service IPsec peut être la commande :

```
envpn 00 && envpn 01
```

Dans les deux cas, la valeur `01` utilisée en exemple représente le numéro de la configuration IPsec employée.

Les CRLs récupérées sont stockées localement dans le répertoire de leur AC (ou de leur AC déléguée) correspondante et renommées en `CA.crl.pem`.

6.2.1 Importation automatique de CRLs

Cette fonctionnalité n'est pas couverte par la cible de sécurité.

Bien qu'une CRL ait une durée de validité, il est important de vérifier fréquemment que de nouveaux certificats n'ont pas été révoqués. Cette fréquence de mise à jour de la CRL doit être adaptée à l'usage de l'authentification par certificat. Si les mises à jour sont trop espacées, le pare-feu peut authentifier des certificats révoqués et créer un accès illégitime. Par exemple, une récupération

toutes les 6 heures permet de diminuer fortement le délai pendant lequel un certificat révoqué peut être utilisé.

R36

Adapter le rafraichissement automatique des CRLs

Il est recommandé d'adapter le temps de rafraichissement en fonction de la réactivité recherchée. Si différents services nécessitent des délais différents, le plus court doit être utilisé.

Par défaut, lorsque l'URL d'une CRL est ajoutée et activée, la récupération du fichier est réalisée une fois par jour. Il est possible de forcer la mise à jour à l'aide de la commande console `checkcrl`. Il est également possible de modifier la fréquence de récupération des CRLs en ajoutant une entrée dans le fichier `/ConfigFiles/Event/rules` faisant appel à la commande `checkcrl`.

Par ailleurs, le champ `CRLDP` contenu dans le certificat d'une AC n'est pas exploité par un pare-feu SNS. Il ne permet donc pas de configurer automatiquement ses points de distribution lors de l'importation d'une AC.

R37

Configurer l'URL de récupération de la CRL et activer la récupération automatique

Il est recommandé de configurer l'URL de récupération automatique de la CRL de chaque AC et activer cette fonctionnalité dans le menu `Système` → `Configuration`.

Les points de distribution de CRLs associées à une AC peuvent être positionnés soit via l'interface web d'administration de SNS en éditant l'onglet `CRL` de l'AC concernée, soit en ligne de commande grâce à la commande :

```
pki ca checkcrl add caname=<nom de l'AC> uri=<URL de la CRL>
```

L'URL du point de distribution peut être de type HTTP, HTTPS, LDAP, LDAPS et FTP.

Information

Pour que l'équipement puisse résoudre le FQDN de l'URL du point de distribution de la CRL, un objet de type `host` correspondant au FQDN doit être défini dans la base d'objets de l'équipement.

6.2.2 Importation manuelle de CRL

Il peut être impossible d'importer automatiquement une CRL. Le cas se présente si un tunnel VPN est nécessaire afin de l'obtenir, et que la précédente n'est plus valide ou n'a jamais été importée. L'importation d'une CRL peut alors être réalisée manuellement. Cette opération implique l'intervention d'un administrateur et la manipulation de fichiers. Elle nécessite donc des procédures organisationnelles strictes et devrait rester une opération exceptionnelle.

R37 -

Importer manuellement une CRL

Si une importation automatique est impossible, il est recommandé d'importer manuellement la CRL.

L'importation manuelle d'une CRL s'effectue via l'interface web d'administration, dans le menu `Objets` → `Certificats et PKI` → `Ajouter` → `Importer un fichier`. Le fichier de CRL doit être importé au format PEM ou DER et son nom ne doit pas comporter d'extension. À l'importation, le fichier de CRL est copié dans le répertoire de l'AC à laquelle il est associé, puis converti au format PEM et renommé en `CA.crl.pem`.

Il est également possible de copier directement un fichier de CRL au format PEM dans le répertoire de l'AC, en le nommant `CA.crl.pem`.

7
VPN IPsec

Certains échanges de flux doivent parfois être réalisés au travers de réseaux non maîtrisés ou de sensibilité inférieure aux données transmises. Dans de tels cas, les risques et conséquences de fuite ou de modification de données sont accrus. Il est alors nécessaire de s'assurer que les données sont échangées entre entités authentifiées, de manière intègre et confidentielle. Ces besoins peuvent être couverts par la mise en place de tunnels IPsec chiffrés. Cette section décrit la politique de configuration à appliquer sur un pare-feu SNS utilisé comme passerelle chiffrante.

7.1 Profils de chiffrement

La confidentialité et l'intégrité des flux échangés sur un VPN (site-à-site ou client-à-site) reposent sur l'utilisation d'algorithmes cryptographiques robustes négociés entre les deux parties. L'utilisation de profils de chiffrement (menu `VPN` → `VPN IPsec` → `Profils de chiffrement`) permet d'expliciter les algorithmes autorisées. Bien que le profil pré-configuré *StrongEncryption* soit compatible avec les exigences du RGS [13], il est conseillé de redéfinir manuellement des profils de chiffrement IKE et IPsec.

Les tableaux 7.1 et 7.2 donnent des exemples de profil de chiffrement compatibles avec les préconisations du RGS. Les cryptopériodes indiquées dans ces tableaux ne sont pas directement issues du RGS mais données à titre indicatif. Elles doivent être définies en fonction de la politique de sécurité de l'organisme.

Paramètre	Valeur
Algorithme de chiffrement	AES 256
Fonction de hachage	SHA 256
Groupe Diffie-Hellman	Groupe 14 (2048 bits)
Cryptopériode	21600s

TABLE 7.1 – Exemple de profil de chiffrement IKE compatible avec le RGS

Paramètre	Valeur
Algorithme de chiffrement	AES 256
Fonction de hachage	SHA 256
Groupe Diffie-Hellman	Groupe 14 (2048 bits)
Cryptopériode	3600s

TABLE 7.2 – Exemple de profil de chiffrement IPsec compatible avec le RGS

R38

Utiliser des algorithmes robustes pour IKE et IPsec

Il est recommandé d'utiliser au moins les algorithmes AES 256, SHA 256 et le groupe Diffie-Hellman 14 dans les profils de chiffrement IKE et IPsec.

7.2 Échange de clés et authentification

7.2.1 Protocole IKE

La protection offerte par un tunnel VPN IPsec dépend de la mise en place d'une suite cryptographique robuste et un mécanisme d'échange de clés fiable. La négociation dynamique des algorithmes et des tunnels IPsec peut se faire grâce au protocole IKEv2 sur les pare-feux SNS en version 2.0.0 et supérieure. L'utilisation des protocoles récents est conforme aux préconisations de l'ANSSI [7].

R39

Utiliser la version 2 du protocole IKE

Si tous les correspondants des tunnels IPsec sont compatibles, il est recommandé d'utiliser le protocole IKE dans sa version 2.

Information

En version 2.7.2, un pare-feu SNS ne peut pas établir simultanément plusieurs tunnels exploitant des versions différentes du protocole IKE. L'ensemble des tunnels actifs doivent utiliser la même version.

7.2.2 Négociation en IKEv1

Dans le cas d'utilisation de la version 1 du protocole IKE, deux modes de négociation sont proposés par l'équipement SNS :

- le mode « principal » disponible lors d'une authentification par certificats ou par clé partagée ;
- le mode « aggressif » disponible lors d'une authentification par clé partagée lorsque que les identités des deux extrémités (*local ID*, *remote ID*) sont renseignées.

La méthode « aggressive » est plus rapide. Cependant, les identités des extrémités sont transmises en clair. L'anonymat des correspondants n'est donc pas assuré.

R39 -

Utiliser le mode de négociation « principal » en cas d'utilisation d'IKEv1

Il est recommandé d'utiliser le mode de négociation dit « principal » lors de l'utilisation de l'IKEv1.

7.2.3 Renégociation en IKEv2

À l'expiration des éléments secret, le comportement par défaut d'IKEv2 est de supprimer la politique IKE concernée, puis de ré-authentifier les correspondants. Dans un soucis de disponibilité,

l'option *make-before-break* permet de forcer la renégociation de la session IKE avant son expiration, évitant une coupure du tunnel.

R40

Utilisation de l'option Make-Before-Break

Lorsque tous les correspondants IKE distants supportent le recouvrement d'associations de sécurité, il est recommandé d'utiliser la fonction *Make-Before-Break* afin de limiter les coupures de tunnel.

La configuration de ce comportement peut être réalisée à l'aide des commandes NSRPC suivantes, où `XX` doit être remplacé par le numéro de la configuration IPsec utilisée.

```
config ipsec update slot=XX MakeBeforeBreak=1
config ipsec activate
```

Ce comportement peut également être obtenu en éditant le fichier de configuration de la politique IPsec utilisée[7]. La valeur du champ `MakeBeforeBreak` est alors à modifier de `0` à `1`. La prise en compte de cette modification est obtenue en réinitialisant la configuration IPsec à l'aide des commandes suivantes :

```
envpn 00 && envpn XX
```

Information

Le mécanisme de renouvellement de session IKE étant différent en IKEv1, ce paramètre n'a pas d'influence sur les tunnels utilisant cette version du protocole.

7.2.4 Authentification

Pour éviter toute usurpation, et ce quel que soit le type de tunnel configuré (site-à-site ou client-à-site), il est nécessaire d'authentifier le correspondant distant lors de la création du tunnel. Cette authentification réalisée par le protocole IKE peut se faire à l'aide d'une clé partagée ou de certificats. L'utilisation d'une clé partagée ne permet cependant pas d'identifier avec précision le correspondant ni de lui appliquer des droits fins. L'utilisation d'une IGC permet son identification. Une meilleure maîtrise des droits est alors disponible ainsi que des fonctionnalités supplémentaires.

R41

Utiliser l'authentification mutuelle par certificat

Il est recommandé de mettre en œuvre une authentification mutuelle par certificat des correspondants d'un tunnel VPN IPsec en renseignant les autorités de certification acceptées dans le menu `VPN` → `VPN IPsec` → `Identification`.

R41 -

Utiliser une clé partagée robuste

Si une authentification par clé partagée est choisie pour un VPN IPsec, il est recommandé de mettre en œuvre une clé conforme aux recommandations du RGS [7] et du guide relatif aux mot de passe [3].

7. Il s'agit du fichier `/Firewall/ConfigFiles/VPN/XX`, où `XX` représente le numéro de la politique IPsec.

Attention

Si une authentification par clé partagée est choisie, il est impératif de respecter les prérequis suivants :

- le secret doit disposer d'une entropie d'au moins 128 bits [8] (22 caractères aléatoires en utilisant comme source les minuscules, les majuscules et les chiffres) ;
- le secret doit respecter les règles relatives à la génération des mots de passe décrites dans le guide de l'ANSSI [3] ;
- un secret différent doit être utilisé pour chacun des tunnels site-à-site ;
- le secret doit être renouvelé régulièrement, sa cryptopériode [9] doit être définie en fonction de la politique de sécurité de l'organisme.

7.3 Politiques de routage et de filtrage sortant, et configuration d'un VPN IPsec

Lorsque l'équipement SNS est utilisé en tant que passerelle VPN, la bonne définition des règles de routage et de filtrage est critique pour garantir la confidentialité et l'intégrité des flux. Quatre fonctions sont fortement liées :

- le routage ;
- la politique de filtrage ;
- la NAT avant IPsec ;
- la politique IPsec.

Dans le cadre de la mise en œuvre de tunnels IPsec, il est nécessaire d'avoir une route permettant de joindre les réseaux distants accessibles au travers des tunnels. Dans le cas contraire, le paquet est supprimé à l'étape de routage et n'atteint pas l'étape de chiffrement IPsec.

Pour éviter toute fuite de données, il est recommandé de configurer une route avec comme passerelle une IP fictive sur sa boucle locale [10] (par exemple, un objet de type machine ayant comme adresse 127.42.42.42). Après l'application de la politique de IPsec, la politique de routage sera réévaluée en fonction du paquet chiffré. Cependant, en cas d'erreur sur la politique IPsec, les paquets seront détruits au lieu de sortir en clair.

Le séquencement des fonctions de routage, de filtrage, de NAT avant IPsec et de politique IPsec représenté sur la figure 7.1 a un impact direct sur la confidentialité des flux [11]. Il est indispensable d'écrire les règles les plus spécifiques pour la politique de filtrage et les règles les moins spécifiques pour la politique IPsec.

8. Se référer à l'annexe B1 du RGS pour plus de précisions [13].
9. Durée maximale durant laquelle perdre la confidentialité et l'intégrité du trafic est accepté si le secret venait à être compromis.
10. Cette technique est également appelée *blackholing*.
11. Ce séquencement n'est qu'une partie du cheminement complet du paquet dans l'équipement. En effet, lorsqu'il est chiffré, le paquet est ensuite traité par les fonctions de routage, de filtrage, de NAT après IPsec.

FIGURE 7.1 – Briques fonctionnelles

R42

Configurer les tunnels IPsec de manière sécurisée

Lorsqu'un VPN IPsec est configuré, il est recommandé de :

- configurer une route statique à destination de la boucle locale (*blackholing*) pour joindre les réseaux distants accessibles au travers de tunnels IPsec ;
- s'assurer que la politique IPsec n'est jamais désactivée y compris lors de phases transitoires ;
- s'assurer que les règles de filtrage sont toujours plus spécifiques que les règles de NAT avant IPsec ;
- s'assurer que les règles de NAT avant IPsec sont toujours incluses dans la politique IPsec ;
- s'assurer qu'en l'absence de règles de NAT, les règles de filtrage sont toujours plus spécifiques que la politique IPsec.

Attention

Idéalement, des équipements distincts devraient être mis en œuvre afin de dissocier les fonctions de chiffrement, de filtrage des flux clairs et de filtrage des flux chiffrés.

Les exemples ci-dessous permettent d'illustrer l'intérêt de la recommandation précédente. Ils s'appliquent sur le pare-feu SNS en tant que passerelle VPN pour des flux en sortie du LAN local et à destination d'un LAN distant au travers d'un tunnel IPsec établi avec une passerelle VPN distante. L'architecture est représentée sur la figure 7.2.

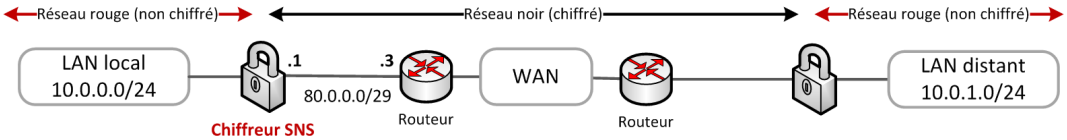


FIGURE 7.2 – Schéma d'architecture

Dans chaque exemple sont données les configurations des briques fonctionnelles SNS traversées par un paquet réseau (Figure 7.1). Le paquet réseau rentre avec une source et une destination spécifiques . Les fonctions traversées sont, dans l'ordre :

- le routage ;
- le filtrage ;
- la NAT avant IPsec ;
- la politique IPsec.

Le résultat obtenu est décrit par le paquet de sortie, à savoir s'il est :

- chiffré ;
- clair (non chiffré) ;
- détruit ;
- filtré.

Un code couleur noir, rouge, vert est appliqué pour représenter respectivement : le cas nominal, le cas d'erreur (clair), le comportement après correction.

Pour chaque exemple trois cas (**C**) sont représentés :

C1 : configuration ne respectant pas la recommandation, les paramètres d'entrée sont nominaux.

C2 : mise en évidence des problèmes liés à la configuration précédente. Une modification des entrées ou de la configuration est réalisée. Cette modification est repérée par l'utilisation d'un texte rouge.

C3 : configuration proposée afin de ne pas tomber dans le problème précédent. Cette modification est repérée par l'utilisation d'un texte rouge.

7.3.1 Politique IPsec toujours active

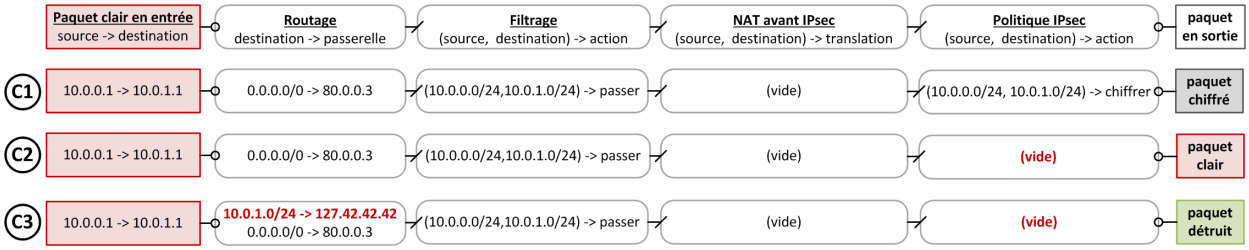


FIGURE 7.3 – Politique IPsec toujours active, route à destination de la boucle locale

L'exemple représenté figure 7.3 illustre la nécessité d'utiliser une route à destination de la boucle locale pour les réseaux IPsec distants. Dans le cas **C1**, les paquets passent en premier dans la table de routage. Elle contient une route valide vers le LAN distant (la route par défaut dans l'exemple traité). Ils passent ensuite dans la politique de filtrage qui accepte les paquets puis dans la politique IPsec qui se charge de l'encapsulation, du chiffrement et de la protection en intégrité des flux. La source et la destination des paquets chiffrés sont différentes de celles des paquets clairs. En particulier, la destination du paquet chiffré est la passerelle VPN distante. La table de routage est de nouveau traversée [12], elle contient une route valide vers la passerelle IPsec (la route par défaut). Les paquets sont émis chiffrés.

La politique IPsec passe ensuite d'un état activé (**C1**) à un état désactivé (**C2**). L'état désactivé peut être permanent ou transitoire, ce dernier cas se produit lors de la désactivation puis de la réactivation de la politique IPsec.

Dans le cas **C2**, les paquets passent en premier dans la table de routage. Elle contient une route valide vers le LAN distant. Ils passent ensuite dans la politique de filtrage qui accepte les paquets.

12. La route à destination du LAN distant n'est pas utilisée. Seule la route à destination de la passerelle VPN distante est utilisée.

Cependant, aucune politique IPsec n'étant définie, les paquets sont envoyés en clair au prochain saut c'est à dire par la passerelle par défaut définie dans la table de routage. Il y a fuite d'informations.

La solution présentée dans le cas **C3** consiste à définir une route à destination de la boucle locale [13], également appelée *blackholing*. En l'absence de politique IPsec, le paquet sera détruit par l'équipement au lieu d'être envoyé à la passerelle par défaut.

R42 +

Ne pas utiliser de route par défaut

Si l'ensemble des réseaux utilisés sont connus, il est recommandé de ne pas utiliser de route par défaut et de privilégier des routes explicites pour joindre l'ensemble des correspondants distants. Ainsi seuls les paquets ayant une route explicitement définie pourront sortir en clair.

Attention

Les plans d'adressage doivent être choisis afin d'éviter toute confusion entre les réseaux rouges et noirs tels que mentionnés dans la figure 7.2, et pour faciliter la création des routes.

7.3.2 Règles de filtrage toujours plus spécifiques que la politique IPsec

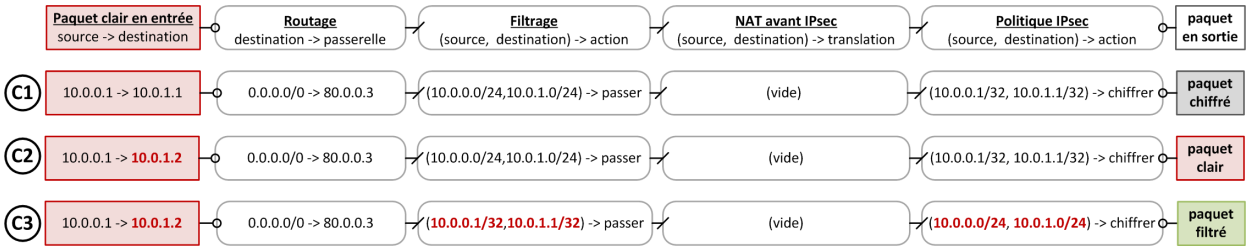


FIGURE 7.4 – Règles de filtrage toujours plus spécifiques que la politique IPsec

L'exemple représenté figure 7.4 illustre la nécessité de définir une politique de filtrage toujours plus spécifique que la politique IPsec. Dans le cas **C1**, la politique de filtrage est définie en /24 alors que la politique IPsec est en /32. L'administrateur désire, par exemple, définir un contexte cryptographique par couple d'adresses IP, tout en gardant une politique de filtrage commune. Dans un premier temps, seules deux machines communiquent entre elles. Les paquets traversent la politique de filtrage puis la politique IPsec et sont émis chiffrés.

Dans le cas **C2**, un équipement est rajouté sur le réseau, la configuration du pare-feu n'est pas modifiée. Les paquets à destination de cette nouvelle adresse IP sont acceptés par la politique de filtrage et non sélectionnés par la politique IPsec et les paquets sont donc émis en clair. Il y a fuite d'informations.

La correction mise en œuvre dans le cas **C3** consiste à positionner une politique de filtrage en /32 et une politique IPsec en /24. La politique de filtrage est ainsi plus restrictive que la politique IPsec. Les paquets seront soit filtrés soit chiffrés mais ils ne pourront pas être émis en clair.

13. Prendre une adresse IP particulière facilite la maintenance de la configuration (par exemple, 127.42.42.42).

Lorsqu'une politique IPsec est utilisée afin d'interconnecter des réseaux, sa fréquence de modification doit être faible et les réseaux utilisés peuvent être étendus contrairement à une politique de filtrage pouvant être fréquemment modifiée et très spécifique.

7.3.3 Règles de NAT avant IPsec incluses dans la politique IPsec

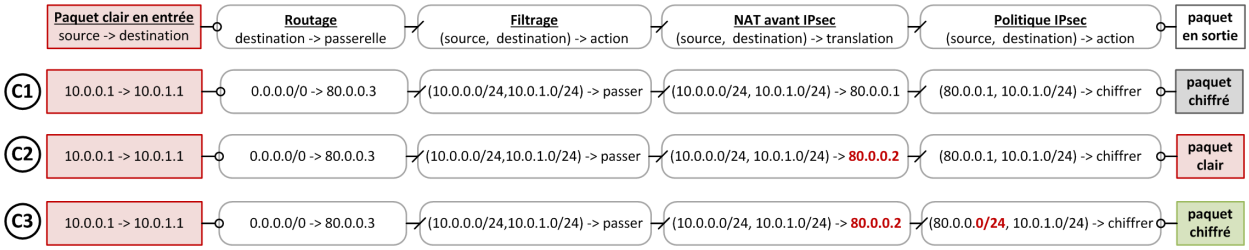


FIGURE 7.5 – Règles de NAT avant IPsec incluses dans la politique IPsec

L'exemple représenté figure 7.5 illustre la nécessité de définir des règles de NAT avant IPsec incluses dans la politique IPsec. Dans le cas **C1**, une règle de NAT avant IPsec est appliquée. Son résultat est un critère de sélection de la politique IPsec. Toute modification de cette règle a un impact direct sur la confidentialité des données. Les paquets sont acceptés par la politique de filtrage puis modifiés par la règle de NAT avant IPsec et enfin sélectionnés par la politique IPsec. Ils sont émis chiffrés.

Dans le cas **C2**, la règle de NAT avant IPsec est modifiée. Les paquets sont acceptés par la politique de filtrage puis modifiés par la règle de NAT avant IPsec. L'adresse IP de sortie est modifiée, elle n'est plus sélectionnée par la politique IPsec et les paquets sont donc émis en clair. Il y a fuite d'informations.

La solution présentée dans le cas **C3** consiste à définir une politique IPsec plus large que la règle de NAT utilisée. Si l'adresse IP de sortie est modifiée, le paquet sera toujours sélectionné par la politique IPsec et sera chiffré par l'équipement.

Information

La règle de NAT doit s'accompagner d'une publication ARP si la ou les adresses utilisées n'appartiennent pas aux interfaces du pare-feu.

7.3.4 Règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec

L'exemple représenté figure 7.6, illustre la nécessité de définir des règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec. Dans le cas **C1**, le réseau source de la règle de NAT avant IPsec est en /25 alors que le réseau source dans la règle de filtrage est en /24. Les paquets proviennent d'une adresse source incluse à la fois dans le /24 et dans le /25. Les paquets sont acceptés par la règle de filtrage puis la règle de NAT avant IPsec est appliquée et enfin la politique IPsec. Les paquets sont émis chiffrés.

Dans le cas **C2**, l'adresse IP source est incluse dans le /24 mais non incluse dans le /25. Les paquets sont acceptés par la politique de filtrage et non sélectionnés par les règles de NAT avant IPsec. La politique IPsec n'est pas appliquée et les paquets sont donc émis en clair. Il y a fuite d'information.

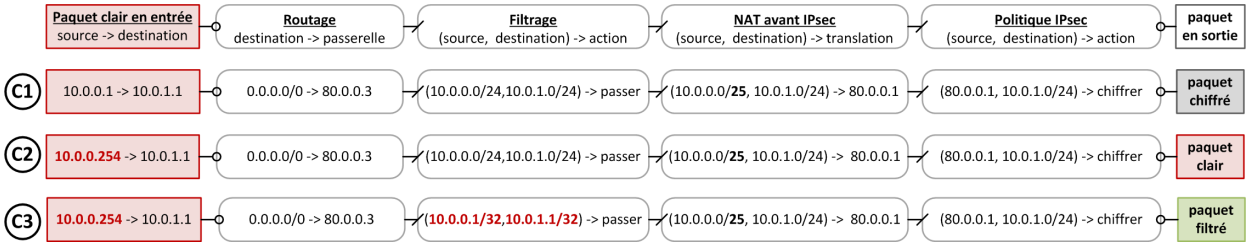


FIGURE 7.6 – Règles de filtrage toujours plus spécifiques que les règles de NAT avant IPsec

La correction mis en œuvre dans le cas **C3** consiste à positionner une politique de filtrage en /32. La politique de filtrage est ainsi plus restrictive que les règles de NAT avant IPsec. Les paquets seront soit filtrés, soit chiffrés.

7.4 Politique de filtrage entrant dans le cas d'un VPN IPsec

Un attaquant sur le réseau peut envoyer des flux au pare-feu en usurpant l'adresse rouge d'un correspondant légitime. Ces messages sans encapsulation doivent être identifiés et rejetés. Le blocage peut s'opérer grâce à une règle de filtrage n'autorisant le flux clair que s'il provient d'un tunnel VPN IPsec. Si le tunnel n'est pas monté, il sera systématiquement rejeté. Cette configuration a lieu dans le menu `Politique de sécurité` → `Filtrage et NAT` → `Filtrage` : dans l'édition d'une règle de filtrage, la valeur `Tunnel VPN IPsec` doit être renseignée dans le champ `Source` → `Configuration avancée` → `Via`.

R43

S'assurer de la provenance des flux entrants

Renseigner la provenance des flux dont la source est accessible uniquement au travers d'un tunnel VPN afin de filtrer le trafic arrivant en clair avec la même adresse source.

Par ailleurs, les politiques de sécurité de chaque tunnel IPsec assurent que les flux transitent au travers du tunnel qui leur est légitime.

7.4.1 Antispoofing sur un tunnel IPsec

Les extrémités de tunnels VPN IPsec sont considérées par un SNS comme des interfaces. À ce titre, le statut d'interface interne, expliqué à la section 3.2.2, leur est également applicable. Le menu `Protection applicative` → `Profils d'inspection` permet d'activer cette option, qui, associée à une définition des routes et des règles de filtrage, augmente la sécurité du réseau.

R44

Déclarer les interfaces VPN internes

Il est recommandé de déclarer les interfaces VPN « internes » afin de profiter des mécanismes d'*antispoofing*.

7.5 Cas des tunnels d'accès nomade

À la différence d'un tunnel site-à-site configuré entre deux passerelles VPN, un tunnel client-à-site est configuré entre une passerelle VPN et un équipement nomade. Dans le premier cas, les adresses des extrémités sont connues et les flux à chiffrer proviennent de sous-réseaux distincts. Dans le second, l'équipement nomade possède une adresse inconnue et se trouve être à la fois l'extrémité du tunnel et le correspondant distant des flux de données. Il n'est donc pas possible de renseigner sur la passerelle VPN l'adresse publique du correspondant distant.

La configuration de tels tunnels est réalisable à partir du menu `VPN → VPN IPsec → Anonyme - Utilisateurs nomades`. Il y est possible de laisser le correspondant choisir son adresse IP rouge, ou de lui en fournir une. Dans le premier cas, il est difficile de maîtriser les routes et les règles de filtrage, et de s'assurer qu'il n'y ait pas de conflit d'adresse entre deux correspondants. Dans le second cas, le mode *Config* permet au pare-feu SNS d'envoyer au client l'adresse IP rouge qu'il doit utiliser, protégeant des risques évoqués.

R45

Configuration des tunnels nomades

Dans le cas de tunnels nomades, il est recommandé d'utiliser le mode *Config* afin de maîtriser les adresses rouges distantes. Ce mode peut être défini dès la création de la politique d'accès VPN ou *a posteriori* depuis le menu `VPN → VPN IPsec → Anonyme - Utilisateurs nomades`.

7.6 Dead-Peer-Detection

Ce mécanisme effectue une vérification périodique de l'état du tunnel IKE grâce à des échanges de messages chiffrés. Si un correspondant ne répond pas aux requêtes envoyées par son pair, il sera alors considéré comme injoignable et l'émetteur clora le tunnel IKE de son côté ainsi que les tunnels IPsec liés. Il existe différents modes d'utilisation de ce mécanisme :

- en mode *inactif*, le pare-feu ne surveille pas l'état du correspondant et n'envoie pas de réponse s'il est sollicité ;
- en mode *passif*, le pare-feu ne surveille pas l'état du correspondant et envoie une réponse s'il est sollicité ;
- en modes *bas* ou *haut*, le pare-feu surveille l'état du correspondant et envoie une réponse s'il est sollicité. En mode *haut*, les requêtes seront plus fréquentes qu'en mode *bas*.

R46

Activer le mécanisme de Dead-Peer-Detection

Pour un VPN IPsec, il est recommandé de mettre en œuvre le mécanisme de *Dead-Peer-Detection* en mode *haut* ou *bas*.

R46 -

Utiliser le mode DPD passif

Si la mise en œuvre du *Dead-Peer-Detection* sur l'extrémité distante n'est pas connue, il est conseillé d'utiliser le mode passif permettant de répondre si une requête DPD est reçue.

7.7 KeepAlive

Lorsqu'un tunnel IPsec n'est pas utilisé, il peut être clos après une durée prédéfinie afin de libérer les ressources sur les équipements. Cependant, si du trafic doit transiter par ce tunnel, il est alors nécessaire de recommencer les négociations. Cela engendre de la latence et une légère perte de paquets. Le mécanisme de *KeepAlive* permet de générer artificiellement du trafic dans un tunnel IPsec afin de maintenir ce dernier actif. Ce flux n'a pas d'utilité une fois reçu et peut être filtré sans en conserver de traces.

R47

Configuration du KeepAlive

Il est recommandé d'activer la fonction de *KeepAlive* et de filtrer le flux émis par l'équipement distant.

Le paramètrage de cette fonction s'effectue dans le menu `VPN` → `VPN IPsec` → `Politique de chiffrement - Tunnels` tel que représenté sur la figure 7.7. En survolant l'entête d'une colonne quelconque du tableau, une flèche apparaît. Cliquer dessus puis aller dans le menu `Colonnes` permet de choisir d'afficher la colonne *KeepAlive*. Il est alors possible de modifier l'intervalle de temps entre deux requêtes du mécanisme. La valeur zéro indique qu'il n'est pas utilisé.

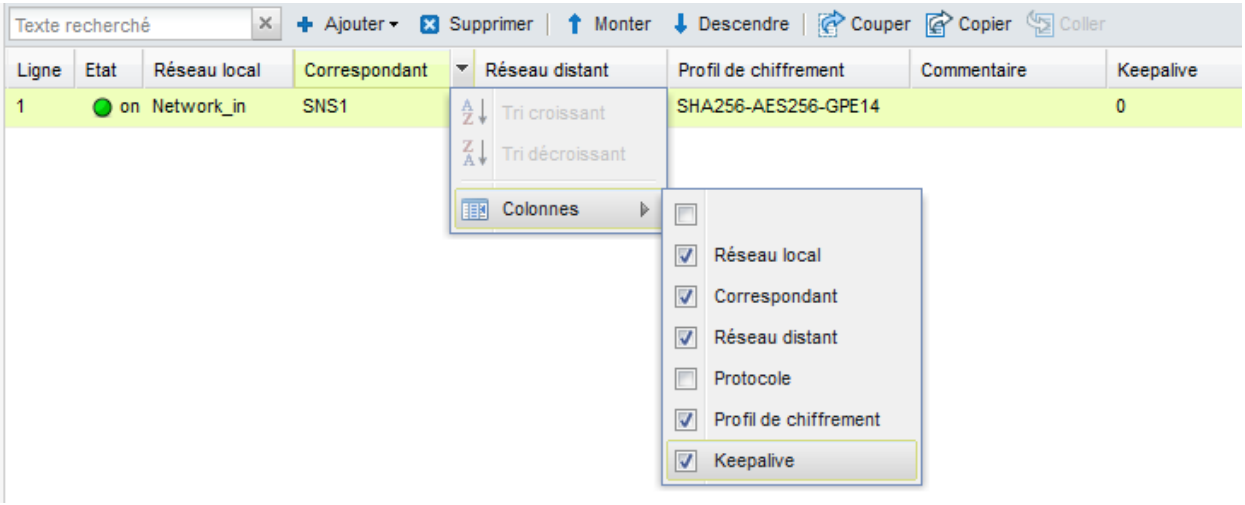


FIGURE 7.7 – Affichage du champ *KeepAlive*

7.8 Gestion du champ DSCP

Le champ DSCP, présent dans l'entête IP, est utilisé pour la gestion de la congestion. Dans le cas d'une encapsulation IPsec, le comportement par défaut d'un pare-feu SNS est de répliquer la valeur de ce champ de l'en-tête originel dans l'en-tête du paquet chiffré correspondant. La modification de ce champ peut perturber le transit du flux sur un réseau d'opérateur.

R48

Conserver le champ DSCP

En dehors d'un besoin de sécurité renforcée, il est recommandé de conserver le paramètrage par défaut du champ DSCP.

Cependant, en cas de besoin d'un niveau de sécurité élevé, la recopie du champ DSCP peut constituer un canal caché. Il est alors important de maîtriser la valeur de ce champ avant la sortie du pare-feu. Une manière de le maîtriser consiste à utiliser l'équipement SNS pour en modifier la valeur. Cela est réalisable dans l'onglet `Qualité de service` du menu `Action` d'une règle de filtrage passante. Lorsque l'option `Forcer la valeur` est activée, le menu `Nouvelle valeur DSCP` est disponible. La valeur sélectionnée est utilisée comme valeur du champ DSCP des paquets filtrés. Cette opération est à appliquer sur les règles de filtrage des flux chiffrés sortants.

R48 +

Maîtriser le champ DSCP

Dans un contexte nécessitant un niveau de sécurité accru, il est recommandé de modifier le champ DSCP des flux sortants à une valeur arbitraire.

Attention

La modification du champ DSCP d'un paquet chiffré ne peut être effective que si les règles implicites de sortie des services hébergés sont désactivées, comme expliqué à la section 5.2, et qu'une règle de filtrage explicite est créée.

Information

L'opérateur de transit peut, dans son réseau, prioriser les paquets en fonction de la valeur du champ DSCP. L'utilisation de la valeur 0 permet de conserver un comportement nominal.

Information

Dans le cas où

- plusieurs connexions transitent au sein d'un tunnel ;
- l'extrémité distante du tunnel recopie la valeur du champ DSCP des paquets clairs sur les paquets chiffrés ;
- le traitement de la QoS sur le réseau de transit produit un réordonnancement des paquets ;
- l'extrémité locale possède une fenêtre anti-rejeu trop faible,

alors une perte de paquets légitimes peut apparaître. Ces pertes peuvent être réduites par la modification du paramètre `ReplayWSize`. Cela peut être effectué grâce à la commande NSRPC `config ipsec profile phase2 update replaywsize=XX` où XX est une valeur comprise entre 0 et 33554400 par incrément de 8. Cette valeur peut être également ajouté manuellement au fichier `/Firewall/ConfigFiles/VPN/01` où la valeur 01 correspond au numéro de la configuration IPsec utilisée.

8
Supervision

Cette section est issue de la version 1.0 de la présente note. Sa mise à jour fera l'objet d'une version ultérieure du document.

8.1 Configuration des éléments de base

Il est recommandé de configurer correctement les paramètres SNMP `Emplacement(syslocation)` et `Contact(syscontact)` présents au niveau du menu `Notifications` → `Agent SNMP` → `Général`, cela facilite la cartographie des équipements dans les outils de supervision et d'alerte.

8.2 Configuration de SNMPv3

R49

Utiliser SNMPv3

Il est recommandé d'utiliser la version 3 du protocole SNMP car elle apporte des mécanismes d'authentification et de chiffrement. L'algorithme de chiffrement AES ainsi que la fonction de hachage SHA1 doivent être utilisés pour apporter aux échanges un niveau de sécurité acceptable mais cependant non conforme au RGS.

Voici un exemple de commande d'interrogation permettant de vérifier le bon fonctionnement de la configuration SNMPv3 d'un équipement SNS qui utilise les paramètres de configuration mentionnés précédemment :

```
snmpwalk -v 3 -u user_snmp -l authPriv -a SHA -x AES ip_admin_SNS
```

Les OID ainsi que leurs valeurs doivent être renvoyés par l'équipement.

Attention

Il est préférable de positionner les mots de passe dans le fichier de configuration plutôt que dans la ligne de commande, puis de les supprimer.

L'utilitaire `snmpwalk` est disponible sur de nombreuses plateformes, il permet d'interroger le service SNMP d'un équipement, voici en détail les paramètres utilisés dans cet exemple :

`-v 3` correspond à la version du protocole SNMP utilisée ;

`-u user_smp` correspond au paramètre `Nom d'utilisateur` renseigné sur l'équipement ;

`-l authPriv` indique que la requête SNMP est chiffrée et authentifiée ;

`-a SHA` précise le type de fonction de hachage utilisé pour l'authentification. Le mot de passe employé est à positionner dans le fichier de configuration. La variable à renseigner est `defAuthPassphrase` [14] ;

`-x AES` indique l'algorithme utilisé pour le chiffrement. Le mot de passe employé est à positionner dans le fichier de configuration. La variable à renseigner est `defPrivPassphrase`.

Attention

Les traps SNMP émises par l'équipement passent dans une règle de flux implicite.

Cette règle est incluse dans la règle des services hébergés présente dans le menu `Règles Implicites`.

L'interrogation de l'équipement en SNMP nécessite la configuration d'une règle de flux. Seuls les serveurs de supervision doivent être autorisés à interroger l'équipement en SNMP.

Par ailleurs, l'accès SNMP se fait en lecture seule uniquement.

R50

Filtrer l'interrogation SNMP

Il est recommandé de n'autoriser que les serveurs de supervision à interroger les équipements en SNMP.

8.3 Utilisation d'OID spécifiques

Des indicateurs « classiques » (interface, disque, mémoire) peuvent être obtenus en interrogeant les équipements SNS sur des OID appartenant à la MIB standard ; il est également possible d'interroger l'équipement sur des OID spécifiques à la technologie SNS (politique, haute disponibilité, VPN) [1]. La construction de templates de supervision utilisant des indicateurs issus de ces deux MIB est recommandée afin de disposer d'une vision précise de l'état des pare-feux.

Voici par exemple la requête d'interrogation SNMP permettant de récupérer le nom de la politique de filtrage réseau activée sur un équipement SNS :

```
snmpwalk -v 3 -u user_snmp -l authPriv -a SHA -x AES \
  ip_admin_SNS .1.3.6.1.4.1.11256.1.8.1.1.3.1
```

Le pare-feu retournera une réponse de la forme :

```
iso.3.6.1.4.1.11256.1.8.1.1.3.1 = STRING :"POL-PROD-SITE1-FW1"
```

La valeur `.1.3.6.1.4.1.11256.1.8.1.1.3.1` représente l'OID par lequel le nom de la politique de sécurité est accessible dans la MIB SNS. La chaine de caractères `"POL-PROD-SITE1-FW1"` correspond au nom donné à la politique par l'administrateur du pare-feu interrogé.

14. Le mot de passe doit faire au moins 8 caractères et doit respecter les règles de robustesse présentées dans la note technique relative à la sécurité des mots de passe [3].

La liste des OID qu'il peut être pertinent de superviser sur un équipement SNS est donnée dans le tableau 8.1.

OID	Description
Informations générales	
.1.3.6.1.4.1.11256.1.0.1.0	Hostname
.1.3.6.1.4.1.11256.1.0.2.0	Version de Stormshield
.1.3.6.1.4.1.11256.1.0.3.0	Numéro de série
.1.3.6.1.2.1.1.3.0	Uptime
CPU	
.1.3.6.1.2.1.25.3.3.1.2	Pourcentage d'utilisation du CPU durant la dernière minute
Charge	
.1.3.6.1.4.1.2021.10.1.3.1	Charge durant la dernière minute
Mémoire	
.1.3.6.1.4.1.2021.4.5.0	Quantité de mémoire de l'équipement
.1.3.6.1.4.1.2021.4.11.0	Quantité de mémoire libre
.1.3.6.1.4.1.2021.4.6.0	Quantité de mémoire utilisée
Espace disque	
.1.3.6.1.2.1.25.2.3.1.5.**31**	Nombre de blocs total de **« /»**
.1.3.6.1.2.1.25.2.3.1.6.**31**	Nombre de blocs utilisés sur **« /»**
.1.3.6.1.2.1.25.2.3.1.5.**35**	Nombre de blocs total de **« /log »**
.1.3.6.1.2.1.25.2.3.1.6.**35**	Nombre de blocs utilisés sur **« /log »**
Interfaces réseaux	
.1.3.6.1.2.1.25.3.2.1.3.**262145**	Nom de l'interface em0 (id **262145**)
.1.3.6.1.2.1.25.3.2.1.5.**262145**	Etat de l'interface em0 au niveau Stormshield (2=activée, 5=désactivée)
.1.3.6.1.2.1.2.2.1.8.**1**	Etat du lien connecté à l'interface em0/id=1 (1=lien ok, 2=lien nok)
Tunnels	
.1.3.6.1.4.1.11256.1.13.2.2	Nombre de tunnels VPN montés (état « mature »)

Table 8.1 – Liste des OID Stormshield

9
Sauvegarde

Cette section est issue de la version 1.0 de la présente note. Sa mise à jour fera l'objet d'une version ultérieure du document.

9.1 Configuration des sauvegardes automatiques

9.1.1 Configuration via CLI

Il est recommandé de mettre en place un mécanisme de sauvegarde automatique qui exporte sur un serveur distant la configuration de l'équipement SNS. L'interface web d'administration permet l'exportation à destination d'un server WebDAV.

Il est également possible d'activer une sauvegarde automatique locale en ligne de commande. Il n'est cependant pas possible d'exporter automatiquement les fichiers de sauvegarde générés sur un serveur distant (SSH par exemple), le fichier généré localement doit être transféré à l'aide d'un script personnalisé. Le fichier de sauvegarde ne doit pas être récupéré en SSH par une connexion initiée par un serveur distant car cela nécessiterait l'usage du compte admin de l'équipement ce qui est fortement déconseillé. Il est recommandé de réaliser un script sur l'équipement SNS qui se connecte en SSH sur un serveur distant et transfère le fichier de sauvegarde.

R51

Mettre en place une sauvegarde automatique

Il est recommandé de mettre en place une sauvegarde automatique de la configuration. Cette sauvegarde devrait être exportée en SSH de l'équipement avec une connexion initiée par celui-ci.

La commande `config autobackup` permet de paramétrer et d'activer la sauvegarde locale automatique de l'équipement. Voici un exemple de configuration d'une sauvegarde automatique locale chiffrée déclenchée tous les jours :

```
config autobackup set state=1 distantbackup=0 \
  period=1d backuppassword=my_password
```

Une fois cette sauvegarde paramétrée, il est nécessaire de l'activer :

```
config autobackup activate
```

La mise en place de sauvegardes automatiques à l'aide de ces commandes va générer le fichier `backup.na.enc` dans le répertoire `/data/Autobackup/`. Ce fichier est écrasé à chaque nouvelle

sauvegarde, il est donc nécessaire de le transférer avant par un canal sécurisé sur un équipement distant.

Attention

Le fichier de sauvegarde porte toujours l'extension `.enc` qu'il soit ou non chiffré par un mot de passe. Il est identique au fichier de sauvegarde qui serait généré à partir de l'interface web d'administration (Menu `Système` → `Maintenance` → `Sauvegarder`).

9.2 Ouverture des fichiers de sauvegarde

Les fichiers de sauvegarde Stormshield (extension `.na` ou `.na.enc`) ne peuvent pas être décompressés directement à partir d'un gestionnaire d'archive standard. Ce type de fichier doit être ouvert au préalable à l'aide de l'utilitaire en ligne de commande `decbackup` ; cet outil est présent sur les équipements (disponible dans le `PATH` ou dans le dossier `/usr/Firewall/sbin`). Il est également disponible sous Linux [15], ce qui permet d'ouvrir les fichiers de sauvegarde y compris lorsque l'on ne dispose pas d'un équipement SNS.

La syntaxe est la suivante :

```
decbackup -i backup.na/na.enc -o backup.tar.gz [-p password]
```

Le fichier de sortie est une archive qui comprend l'ensemble des fichiers de configuration de l'équipement (ceux présents dans `/usr/Firewall/ConfigFiles`).

15. Il faut en faire la demande à l'éditeur.

10
Journalisation

Cette section est issue de la version 1.0 de la présente note. Sa mise à jour fera l'objet d'une version ultérieure du document.

10.1 Politique de journalisation

Avant de configurer les journaux sur un équipements SNS, il est nécessaire de définir une politique de journalisation. Celle-ci devra notamment spécifier les types d'évènements qu'il est pertinent de journaliser ainsi que leur lieu d'archivage.

Sur un équipement SNS, il est possible de définir de façon indépendante :

- les types d'évènements journalisés sur le support de stockage local lorsqu'il existe (onglet `Stockage local` du menu `Traces - syslog`). Dans ce cas, ces évènements seront directement consultables à partir de l'interface web d'administration de l'équipement SNS. Il est recommandé de mettre en place un écrasement automatique de ces évènements ;
- les types d'évènements envoyés sur un (ou plusieurs) serveur syslog (onglet `Syslog` du menu `Traces - syslog`). Ces évènements ne sont pas directement consultables à partir de l'interface web d'administration de l'équipement SNS, ils sont destinés à être injectés dans un SIEM ou à être archivés.

10.2 Journaux à collecter

Voici une liste non exhaustive des types de journaux qu'il est recommandé de collecter par syslog. Le cas d'usage supposé est un pare-feu/VPN IPsec, l'IDS et l'IPS n'étant pas activés :

- les évènements relatifs à la politique de filtrage (paquets rejetés, etc.) ;
- les connexions réseaux ;
- les éléments relatifs aux VPN IPsec (mise en place et destruction de tunnel, etc.) ;
- les évènements d'authentification (tentatives avortées, réussites, échecs, etc.) ;
- les évènements d'administration (démon `serverd`) (connexion d'administrateurs, modification de configuration) ;
- les statistiques ;
- les évènements systèmes ;

- les alarmes.

R52

Définir une politique de journalisation

Il est recommandé de définir une politique de journalisation locale et une politique de journalisation centralisée [5].

11
Gestion du parc

Cette section est issue de la version 1.0 de la présente note. Sa mise à jour fera l'objet d'une version ultérieure du document.

Pour l'administration de plusieurs équipements SNS, il est recommandé de mettre en place un SI d'administration conforme aux préconisations du guide [15]. Ce SI d'administration devrait notamment être utilisé pour :

- accéder à distance aux services d'administration de l'équipement (HTTPS, NSRPC [16]) à partir des postes d'administration ;
- transférer les journaux générés par l'équipement SNS à destination du serveur central de journalisation ;
- faire circuler les flux de supervision échangés entre l'équipement SNS et le serveur central de supervision ;
- transférer les fichiers de sauvegarde de l'équipement SNS en direction du serveur central de sauvegarde.

16. Les outils appropriés utilisent le port TCP 1300.

Liste des recommandations

Bibliographie

[1] *Management Information Base pour SNS*.
Page web, Stormshield, février 2015.
https://www.stormshield.eu/landing/mibs/.

[2] *Espace personnel Stormshield*.
Page web, Stormshield, novembre 2017.
https://www.mystormshield.eu/.

[3] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[4] *Problématiques de sécurité associées à la virtualisation des systèmes d'information*.
Note technique DAT-NT-011/ANSSI/SDE/NP v1.1, ANSSI, septembre 2013.
https://www.ssi.gouv.fr/virtualisation.

[5] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[6] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://www.ssi.gouv.fr/politique-filtrage-parefeu.

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

[8] *Guide TLS*.
Guide SDE-NT-035 v1.1, ANSSI, août 2016.
https://www.ssi.gouv.fr/nt-tls.

[9] *Instruction interministérielle n° 901*.
Référentiel Version 1.0, ANSSI, décembre 2006.
https://www.ssi.gouv.fr/ii901/.

[10] *Définition d'une architecture de passerelle d'interconnexion sécurisée*.
Guide Version 1.0, ANSSI, décembre 2011.
https://www.ssi.gouv.fr/architecture-interconnexion.

[11] *RGS : Référentiel Général de Sécurité*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[12] *RGS : Annexe A1 Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques*.
Référentiel Version 1.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[13] *RGS : Annexe B1 Mécanismes cryptographiques*.
Référentiel Version 1.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[14] *RGS : Annexe A4 Politique de certificats/LCR/OCSP et algorithmes cryptographiques*.
Référentiel Version 1.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[15] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Note technique DAT-NT-022/ANSSI/SDE/NP v1.0, ANSSI, février 2015.
https://www.ssi.gouv.fr/securisation-admin-si.

ANSSI-BP-031
Version 2.0 - 27/12/2017

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

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

Paris, le 5 juin 2012

N° DAT-NT-001/ANSSI/SDE/NP

Nombre de pages du document : 10

Note technique

Recommandations de sécurité relatives aux mots de passe

Informations

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
Division assistance technique, CERT Fr	DAT	SDE	5 juin 2012

Évolutions du document :

Version	Date	Nature des modifications
1.0	23 mai 2012	Version initiale
1.1	5 juin 2012	Corrections de forme

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

Préambule

Malgré le développement de mécanismes d'authentification intrinsèquement plus robustes, l'usage des mots de passe est encore relativement répandu, notamment pour l'authentification sur Internet.

L'ANSSI recommande très fortement, dans tous les cas où cela est possible, l'utilisation de technologies d'authentification forte (utilisation de certificats d'authentification sur carte à puce, utilisation de schéma d'authentification à plusieurs facteurs etc.). Cependant, l'utilisateur n'est pas toujours maître des choix qui s'offrent à lui en matière d'authentification. L'objet de ce document est donc de guider l'utilisateur dans le choix de mots de passe adéquats.

De quoi dépend la robustesse d'un mot de passe ?

Les préconisations que l'on peut retrouver dans les guides de bonne pratique en matière de robustesse de mots de passe sont parfois contradictoires. Certaines recommandations préconisent le choix de mots de passe de 12 caractères alphanumériques, d'autres de 16 lettres, etc.

En réalité, il n'existe pas de règle universelle. La robustesse d'un mot de passe dépend en pratique :
- de la force intrinsèque du mot de passe, c'est à dire sa complexité intrinsèque [1] ;
- du mécanisme mis en oeuvre pour vérifier le mot de passe et de ses caractéristiques techniques (temps de vérification, mécanisme cryptographique sous-jacent notamment) ;
- du modèle d'attaquant considéré. La résistance contre tous les types d'attaquants imaginables est intrinsèquement plus difficile à atteindre que la simple résistance aux attaques opportunistes par lesquelles l'attaquant va essayer les mots de passe les plus triviaux les uns après les autres sans connaissance a priori du système cible ;
- éventuellement, en fonction des mécanismes techniques mis en oeuvre et du modèle d'attaquant, du nombre d'authentification ratées autorisées avant blocage d'un compte protégé par le mot de passe ;
- des mécanismes d'alerte éventuels. Certains systèmes permettent à l'utilisateur de prendre connaissance de manière sûre du nombre d'échecs d'authentification infructueux. D'autres léveront une alerte à destination d'un administrateur ou bloqueront le compte de l'utilisateur concerné.

Compte-tenu de ce qui précède, il n'existe pas de recette miracle pour déterminer à coup sûr ce qu'est un bon mot de passe. Prenons quelques exemples plus concrets :

Exemple 1 : Certains systèmes d'authentification historiques découpaient systématiquement tous les mots de passe de moins de 14 caractères en deux blocs de 7 caractères, sur lesquels étaient appliqués un mécanisme de vérification similaire. Sans rentrer dans les détails techniques, le choix d'un tel mécanisme avait pour conséquence le fait que tous les mots de passe de moins de 14 caractères étaient à peu de chose près équivalents en termes de robustesse. Choisir un mot de passe de 14 caractères n'était pas réellement plus sûr que de prendre un mot de passe de 8 caractères (cf. Annexe).

Exemple 2 : Certains systèmes d'authentification disposent d'un mécanisme doublant le temps de vérification du mot de passe après chaque échec d'authentification. Ainsi, le temps de vérification du mot de passe devient rédhibitoire pour un attaquant après seulement quelques essais infructueux. Cette mesure est efficace, mais uniquement contre un attaquant de niveau basique essayant tous les mots de passe les plus probables les uns après les autres. Il n'est pas rare que l'observation des échanges

1. Voir sur le site www.securite-informatique.gouv.fr les fiches techniques "Mot de passe" et "Calculer la force d'un mot de passe".

entre l'utilisateur et la machine sur laquelle il cherche à s'authentifier fournisse suffisamment d'information à l'attaquant pour rechercher le bon mot de passe a posteriori (on parle de recherche hors-ligne).

Exemple 3 : Certains systèmes d'information imposent à l'utilisateur de prendre un mot de passe extrêmement compliqué mais le transmettent ensuite en clair sur le réseau. La complexité du mot de passe choisi sur l'utilisateur n'a donc qu'un impact limité sur la sécurité du système dans son ensemble, dès lors que l'attaquant a la possibilité d'écouter le échanges sur le réseau.

Au final, la définition d'une politique de mot de passe est une opération complexe. Cette politique doit être ajustée le plus précisément possible afin de garantir le respect des objectifs de sécurité sans imposer des contraintes irréalistes pour les utilisateurs.

Les recommandations minimales à respecter !

A minima, l'ANSSI estime que les 8 recommandations suivantes doivent s'appliquer indépendamment de tout contexte. Lorsque les systèmes d'information utilisés le permettent, certaines doivent être imposées techniquement.

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

Pour en savoir plus

Pour approfondir les méthodes d'attaque sur mots de passe et disposer ainsi de plus d'éléments justifiant ces recommandations, le lecteur est invité à lire l'annexe de ce document qui est une mise à jour d'une note d'information publiée en 2005 par le CERTA [2].

2. CERTA-2005-INF-001.

Annexe à la note DAT-NT-001/ANSSI/SDE du 5 juin 2012.

1 Introduction

L'utilisation de mots de passe forts est l'une des briques de base dans la sécurisation d'un système d'information. Malheureusement cette première étape est souvent absente dans la politique de sécurité. Il est par conséquent assez fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut.

Cette note a pour but :
- de sensibiliser les utilisateurs de système d'information sur l'intérêt d'avoir des mots de passe forts ;
- de sensibiliser les administrateurs sur l'intérêt de mettre en place un contrôle systématique de la qualité des mots de passe ;
- de sensibiliser les concepteurs d'application sur l'importance d'une politique complète et cohérente concernant l'utilisation et la gestion des mots de passe ;
- de préciser les limites de la sécurité apportée par les mots de passe.

2 Les différentes attaques sur les mots de passe

Afin d'éviter qu'un mot de passe ne soit facilement retrouvé par un outil conçu à cet effet, il peut être intéressant de connaître les différentes méthodes utilisées par les outils automatisés pour découvrir les mots de passe. Dans la plupart des cas, ce sont les empreintes (valeur de sortie d'une fonction de hachage) des mots de passe qui sont stockées sur le système. Les attaques sur les mots de passe consistent donc à calculer des empreintes et à les comparer à celles contenues dans les fichiers de mots de passe.

En outre, toute faiblesse dans les schémas de mot de passe peut faciliter ces attaques. Il convient donc d'en tenir compte pour choisir le bon mot de passe. Par exemple, pour les systèmes Microsoft, lorsque le `Hash LM` est utilisé, si un attaquant a récupéré le hash du mot de passe, il pourra récupérer le mot de passe originel en un temps très raisonnable à l'aide, par exemple, des Rainbow Tables. En effet, dans ce mode, il n'y a pas de différences entre les minuscules et les majuscules et la complexité ne peut pas dépasser 7 caractères par construction. Aussi, dans les paramètres de sécurité locaux Windows, il convient d'empêcher le stockage `Hash LM` après changement de mot de passe. Le schéma qui suit illustre le principe de fonctionnement du `Hash LM` :

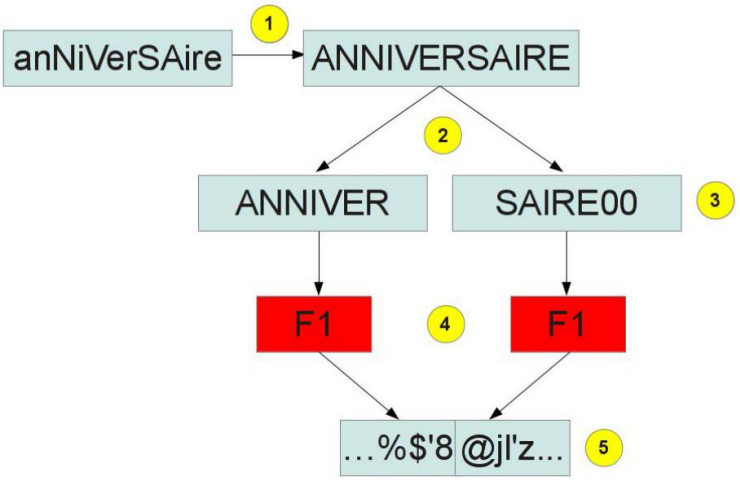


FIGURE 1 – Description du `Hash LM`

1. La casse du mot de passe n'est pas gérée. Il peut donc être considéré que tout est en majuscules.
2. Le mot de passe est séparé en 2 mots de 7 caractères.
3. Lorsque le mote de passe a une longueur inférieure à 14 caractères, il est complété par des caractères null.
4. Une fonction de hashage est appliquée à chaque mot.
5. Les deux hashs concaténés constituent le `Hash LM`.

2.1 Attaques par force brute

Cette attaque consiste à tester toutes les combinaisons possibles d'un mot de passe. Plus il existe de combinaisons possibles pour former un mot de passe, plus le temps moyen nécessaire pour retrouver ce mot de passe sera long.

Un mot de passe, d'une longueur minimale de douze caractères et constitué d'au moins trois des quatre groupes de caractères enoncés ci-dessus (minuscules, majuscules, caractères spéciaux et chiffres), ne pourra pas en général être découvert par cette attaque dans un temps raisonnable [3].

2.2 Attaques par dictionnaires

Cette attaque consiste à tester une série de mots issus d'un dictionnaire. Il existe toutes sortes de dictionnaires disponibles sur l'Internet pouvant être utilisés pour cette attaque (dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...). En utilisant un mot de passe n'ayant aucune signification cette attaque ne donnera aucun résultat.

Cependant, plusieurs règles de transformation des mots du dictionnaire sont utilisées par les outils automatisés pour augmenter le nombre de combinaisons possibles. Citons par exemple :
- le remplacement d'un ou de plusieurs caractères du mot du dictionnaire par une majuscule (`bUreAU`) ;
- le remplacement de certains caractères par des chiffres comme par exemple le `S` en `5` (`mai5on`) ;
- l'ajout d'un chiffre au début ou à la fin d'un mot (`arbre9`) ;
- l'ajout des mots de passe déjà découverts.

Il est possible d'utiliser des dictionnaires contenant une liste de mots de passe et leur empreinte associée établie selon ces règles. Même si cette possibilité accélère le temps nécessaire pour retrouver un mot de passe, elle nécessite plus de moyens comme une place plus importante en mémoire.

La solution idéale pour un individu malintentionné qui souhaiterait retrouver des mots de passe le plus rapidement possible serait d'avoir une liste exhaustive de tous les mots de passe possibles et de leur empreinte associée. Un tel dictionnaire n'est pas enviseageable car il nécessiterait une place en mémoire bien trop importante. Cependant sur les algorithmes de chiffrement faibles (cf. exemple précédent du `Hash LM` sur les systèmes Microsoft Windows), il est possible d'utiliser les attaques par compromis temps/mémoire.

2.3 Attaques par compromis temps/mémoire

Les attaques par compromis temps/mémoire sont des solutions intermédiaires permettant de retrouver un mot de passe plus rapidement qu'avec une attaque par force brute et avec moins de mémoire

3. Compte tenu des moyens à la disposition de tout à chacun au moment de la rédaction de ce document.

qu'en utilisant une attaque par dictionnaire. Ces compromis sont réalisés à partir de chaînes construites à l'aide de fonctions de hachage et de fonctions de réduction. Pour retrouver un mot de passe, il faudra d'abord retrouver à quelle chaîne appartient l'empreinte recherchée. Une fois que la chaîne aura été retrouvée il sera alors facile de retrouver le mot de passe, à partir du début de cette chaîne.

Par ailleurs, des méthodes efficaces s'appuyant sur les statistiques comme le calcul de la probabilité d'apparition d'une lettre dans un mot de passe selon celle qui la précède [4] permettent de fixer certains paramètres pour optimiser les attaques.

2.4 Attaques indirectes

D'autres attaques assez connues car très pratiquées (en particulier le filoutage et les logiciels de captures des frappes au clavier) consistent non pas à déterminer le mot de passe par une recherche technique mais à le capturer au moment où il est saisi, ou encore à se le faire communiquer en usant de supercherie.

Face à ces attaques, la qualité (ou « force ») du mot de passe doit être complétée par des mesures organisationnelles essentielles :

- procédures robustes de création de compte (initialisation et première fourniture du mot de passe) ;
- sensibilisation et bonne information des utilisateurs afin qu'ils détectent les tentatives pour leur soutirer leur mot de passe ;
- procédures robustes de réinitialisation en cas d'oubli ou perte du mot de passe par un utilisateur ;
- ne pas réutiliser des mots de passe identiques sur des systèmes différents. En particulier, ne pas mettre le même mot de passe sur une application peu protégée et sur une application sensible.

3 Comment créer un bon mot de passe ?

Un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

Néanmoins, un bon mot de passe doit être facile à retenir pour rester fort. En effet, si un mot de passe est trop compliqué à retenir, l'utilisateur trouvera différentes astuces comme, par exemple, l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier lui permettant de s'authentifier. Pour ne pas mettre bêtement en danger la sécurité du SI, il existe différents moyens mnémotechniques pour fabriquer et retenir des mots de passe forts.

3.1 Méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase *« J'ai acheté huit cd pour cent euros cet après midi »* deviendra `ght8CD%E7am`.

3.2 Méthode des premières lettres

Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation `« un tiens vaut mieux que deux tu l'auras »` donnera `1tvmQ2tl'A`.

4. Utilisation des chaînes de Markov.

4 Pourquoi et comment bien gérer les mots de passe ?

4.1 Politique de gestion des mots de passe

Les mots de passe sont souvent la seule protection d'une station de travail. Il est donc indispensable de mettre en œuvre une politique de gestion des mots de passe intégrée à la politique de sécurité du système d'information.

Cette politique de gestion de mots de passe devra être à la fois technique et organisationelle. Les éléments suivants pourront, entre autres, y être inscrits.

4.1.1 Sensibilisation à l'utilisation de mots de passe forts

Les utilisateurs d'un système d'information doivent être sensibilisés à l'utilisation de mots de passe forts afin de comprendre pourquoi le risque d'utiliser des mots de passe faibles peut entraîner une vulnérabilité sur le système d'information dans son ensemble et non pas sur leur poste uniquement.

4.1.2 Mot de passe initial

Le mot de passe initial doit être de préférence fourni sur un canal sûr. Lorsque ce mot de passe initial est fourni par l'administrateur du système ou lorsqu'il est communiqué sur un canal non confidentiel, il doit être changé dès la première connexion de l'utilisateur.

L'administrateur qui a fourni un mot de passe sur un canal non sûr doit avoir une vigilance plus soutenue afin de s'assurer que le mot de passe n'est pas utilisé par un tiers.

4.1.3 Renouvellement des mots de passe

Les mots de passe doivent avoir une date de validité maximale. A partir de cette date l'utilisateur ne doit plus pouvoir s'authentifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps.

4.1.4 Les critères prédéfinis pour les mots de passe

Plusieurs critères peuvent être définis et mis en œuvre dans de nombreux systèmes pour s'assurer de la qualité des mots de passe. Ces critères sont, par exemple :

- une longueur minimale obligatoire prédéfinie ;
- l'impossibilité de réutiliser les n derniers mots de passe ;
- le nombre de tentatives possibles avant verrouillage de compte ;
- la manière de déverrouiller un compte qui a été bloqué. Pour éviter les dénis de service liés au blocage de tous les comptes sur un système d'information, il peut être intéressant que le déblocage des comptes se fasse de manière automatique après un certain délai ;
- la mise en place d'une veille automatique avec un déblocage par saisie du mot de passe.

4.1.5 Confidentialité du mot de passe

Un mot de passe sert à s'authentifier sur un système. Dans ce but, il est important de veiller à ne pas divulguer son mot de passe. Un mot de passe ne doit jamais être partagé ni stocké dans un fichier ni sur papier sans protection adaptée. Ainsi, il est possible que la politique de sécurité demande

aux utilisateurs d'un système d'information de stocker les mots de passe sur papier dans un lieu sûr (enveloppe cachetée dans un coffre ignifugé) pour le cas ou un problème surviendrait.

4.1.6 Configuration des logiciels

Une large majorité de logiciels comme par exemple les logiciels de navigation Internet proposent d'enregistrer les mots de passe, par le biais d'une petite case à cocher `«retenir le mot de passe»`, pour éviter à l'utilisateur la peine d'avoir à les ressaisir. Ceci pose plusieurs problèmes de sécurité notamment lorsqu'une personne mal intentionnée prend le contrôle de l'ordinateur d'un utilisateur, il lui suffit de récupérer le fichier contenant la liste des mots de passe enregistrés pour pouvoir se connecter sur des sites à accès protégé.

4.2 Utilisation de mots de passe différents

Il est important de garder à l'esprit qu'un mot de passe n'est pas inviolable dans le temps. C'est pour cette raison qu'il est nécessaire de changer régulièrement son mot de passe et qu'il est important de ne pas utiliser le même mot de passe pour tous les services vers lesquels on se connecte.

En effet, si le poste de travail est compromis et qu'un renifleur de clavier est installé, un utilisateur mal intentionné peut récupérer tous les mots de passe entrés au clavier durant la période pendant laquelle le renifleur de clavier était installé (même si ces mots de passe sont forts) et accéder à l'ensemble des services nécessitant ces mots de passe. Tant que les mots de passe capturés n'ont pas été changés, des accès malveillants sont possibles, l'impact de l'attaque est durable.

C'est pourquoi changer régulièrement de mots de passe, *à partir de machines saines*, permet de diminuer la durée de l'impact de l'attaque.

4.3 Utilisation de mots de passe non rejouables (`One Time Password`)

Il est possible d'utiliser des solutions permettant de s'authentifier à un système par le biais d'un mot de passe ne pouvant être utilisé qu'une seule fois. Cette solution présente l'avantage que lorsqu'un mot de passe est découvert, il ne peut pas être réutilisé. Cette technique reste toutefois vulnérable aux attaques de l'intercepteur (*man in the middle*).

4.4 Mettre en place un contrôle systématique des mots de passe

Pour s'assurer de l'absence de mots de passe faibles, il peut être intéressant pour un administrateur, s'il y est autorisé, de réaliser des tests sur la robustesse des mots de passe utilisés sur son système d'information. Des outils commerciaux ou gratuits sont disponibles sur l'Internet. Le choix de l'outil le plus adapté dépend du type de mots de passe que l'on désire analyser. Une telle démarche peut être très utile à des fins de sensibilisation des utilisateurs.

5 Lorsque possible, préférer l'usage de certificats d'authentification sur carte à puce !

L'utilisation de certificats de clés publiques sur les postes clients et serveurs permet de détecter l'intercepteur (*man in the middle*), mais reste vulnérable au vol sur le poste de travail du code porteur ou de la clé privée si elle n'est pas protégée dans un matériel adéquat (par exemple une carte à puce).

Si le client peut disposer d'un certificat d'authentification et d'une clef privée stockée sur une carte à puce qualifiée par l'ANSSI, alors il est préférable d'utiliser ce dispositif plutôt qu'un mot de passe pour l'authentification. À titre d'exemple, le schéma infra illustre un cas d'usage associant une clé privée stockée sur carte à puce et un protocole d'authentification robuste : Kerberos.

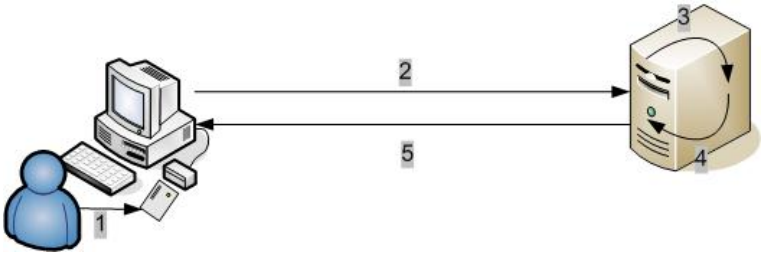


FIGURE 2 – Authentification Kerberos sur un réseau Microsoft

1. L'utilisateur saisit un code PIN après avoir introduit sa carte à puce.
2. Une demande de ticket signée avec sa clé privée stockée sur la carte à puce est émise vers le KDC [5]. Le certificat de l'utilisateur est aussi envoyé.
3. Le KDC s'assure que l'utilisateur existe dans le domaine Active Directory.
4. Le TGT [6] et la clé de session sont chiffrés par le KDC avec la clé publique de l'utilisateur.
5. Le tout est adressé au client Windows qui peut alors le déchiffrer avec la clé privée de l'utilisateur.

Il est important de rappeler que, dans le cadre des échanges entre autorités administratives et entre une autorité administrative et les citoyens, l'annexe B3 du référentiel général de sécurité fixe l'ensemble des règles techniques à respecter en matière d'authentification dont celles liées à l'emploi de certificats.

5. Key Distribution Center.
6. Ticket Granting Ticket.

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

GUIDE ANSSI

ANSSI-PA-022
11/05/2021

PUBLIC VISÉ :

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

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations relatives à l'administration sécurisée des systèmes d'information »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [28].

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

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

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	20/02/2015	Version initiale
2.0	24/04/2018	Prise en compte des retours d'expérience, réorganisation des chapitres & refonte graphique
3.0	11/05/2021	Ajout d'un chapitre sur l'administration par des tiers et l'assistance à distance, mises à jour détaillées en annexe A

Table des matières

1
Introduction

1.1 Objectif du guide

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

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

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

1.2 Organisation du guide

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

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

1.3 Convention de lecture

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

Pour certaines recommandations de ce guide, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles

permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

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

R -

Recommandation alternative de premier niveau

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

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

Recommandation renforcée complémentaire

Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée en priorité aux entités qui sont matures en sécurité des systèmes d'information.

La liste récapitulative des recommandations est disponible en page 63.

2
Les administrateurs, acteurs clés de la sécurité du système d'information

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

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

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

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

Actions d'administration

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

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

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

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

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

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

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

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

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

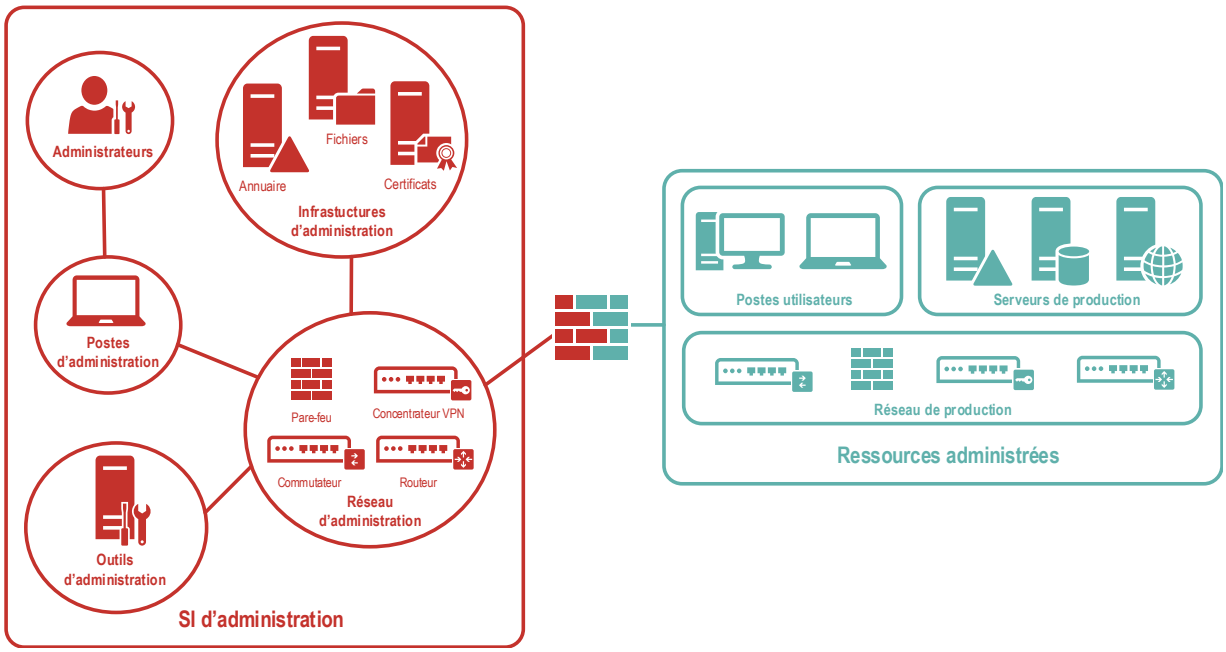


FIGURE 2.1 – Représentation fonctionnelle d'un SI d'administration et de ressources administrées

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

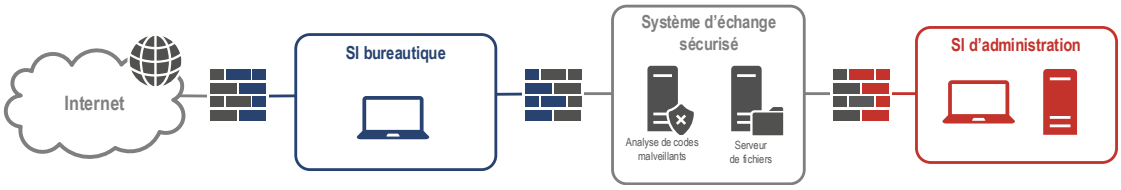


FIGURE 2.2 – Représentation fonctionnelle d'un système d'échange sécurisé

2.2 Droits et devoirs des administrateurs

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

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

R1

Informer les administrateurs de leurs droits et devoirs

Un administrateur doit être informé de ses droits et devoirs, notamment en s'appuyant sur la charte informatique de l'entité.
Il est recommandé d'élaborer une charte informatique spécifique applicable aux administrateurs.

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

R2

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

En tant que ressource humaine critique pour le SI, un administrateur doit être formé à l'état de l'art, dans ses domaines de compétences et en sécurité des systèmes d'information (ex. : sécurité des systèmes, sécurité des réseaux, infrastructure de gestion de clés).
Le guide d'hygiène informatique de l'ANSSI [13] doit être connu.

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

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

R3

Disposer d'une documentation des SI à jour

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

3
Généralités sur le système d'information d'administration

3.1 Analyse de risque et objectifs de sécurité

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

3.1.1 Analyse de risque

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

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

R4

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

Avant toute étude des mesures techniques à mettre en œuvre, une analyse de risque doit être menée en portant une attention particulière sur les besoins de sécurité du SI d'administration et ses interconnexions.
Dans une démarche d'amélioration continue, il est recommandé que l'analyse de risque et la mise en œuvre des mesures induites soient revues au moins une fois par an.

3.1.2 Objectifs de sécurité

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

Scénario d'attaque

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

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

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

3.2 Zones de confiance et zones d'administration

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

Zone de confiance

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

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

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

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

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

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

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

R5

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

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

3.3 Produits qualifiés par l'ANSSI

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

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

R6

Privilégier l'utilisation de produits qualifiés par l'ANSSI

D'une manière générale, il est recommandé que les matériels et les logiciels utilisés pour protéger le SI d'administration soient qualifiés par l'ANSSI au niveau requis par les besoins de sécurité.
À défaut, il est recommandé qu'ils disposent d'un autre visa de sécurité délivré par l'ANSSI [4].

Attention

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

3. La qualification des produits par l'ANSSI comporte trois niveaux : élémentaire, standard et renforcé.
4. Se reporter à `https://www.ssi.gouv.fr/visa-de-securite`.

3.4 Confiance dans le cloisonnement des environnements virtualisés

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

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

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

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

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

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

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

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

R7

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

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

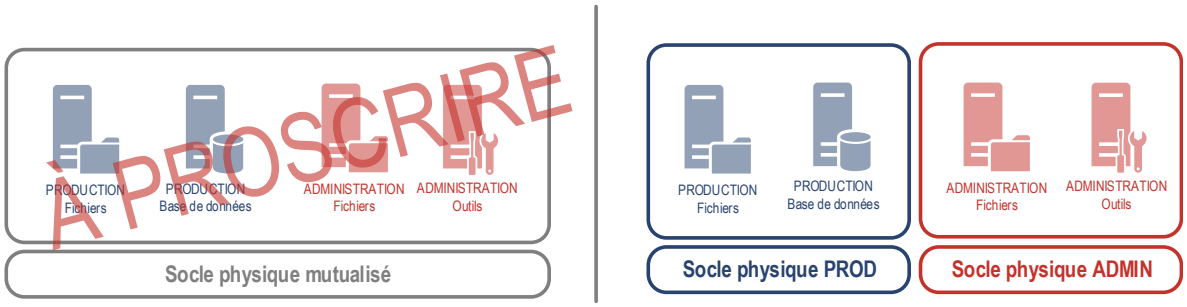


FIGURE 3.1 – Cloisonnement des socles physiques de virtualisation pour des serveurs

Attention

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

4
Poste d'administration

4.1 Maîtrise du poste d'administration

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

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

R8

Gérer et configurer le poste d'administration

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

Attention

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

4.2 Architecture du poste d'administration

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

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

5. Terme français équivalent : AVEC – Apportez votre équipement personnel de communication.
6. On convient de parler de SI bureautique au sens large, c'est-à-dire tout ce qui n'est pas le SI d'administration.

4.2.1 Un poste d'administration dédié

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

R9

Utiliser un poste d'administration dédié

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

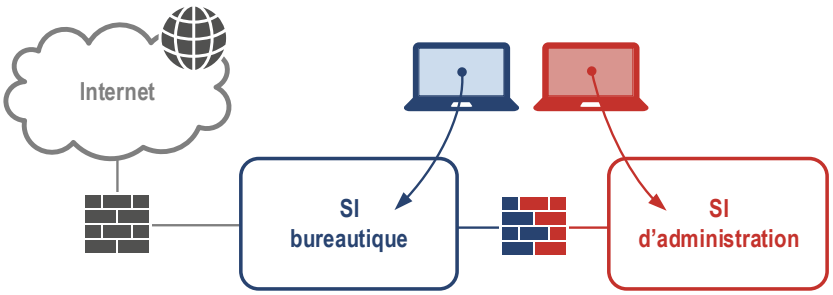


FIGURE 4.1 – Poste d'administration dédié

4.2.2 Un poste d'administration multi-niveaux

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

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

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

R9 -

Utiliser un poste d'administration multi-niveaux

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

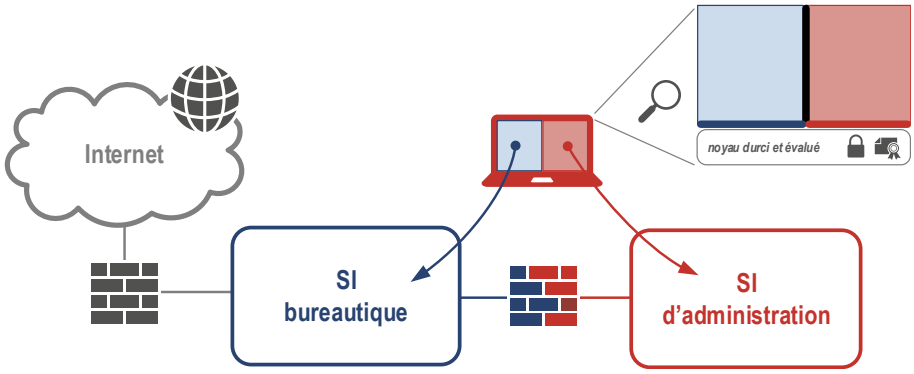


FIGURE 4.2 – Poste d'administration multi-niveaux

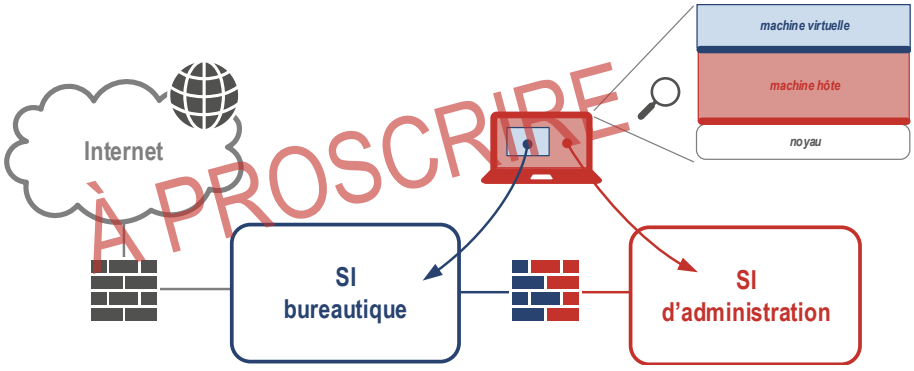


FIGURE 4.3 – Poste d'administration hébergeant une machine virtuelle bureautique

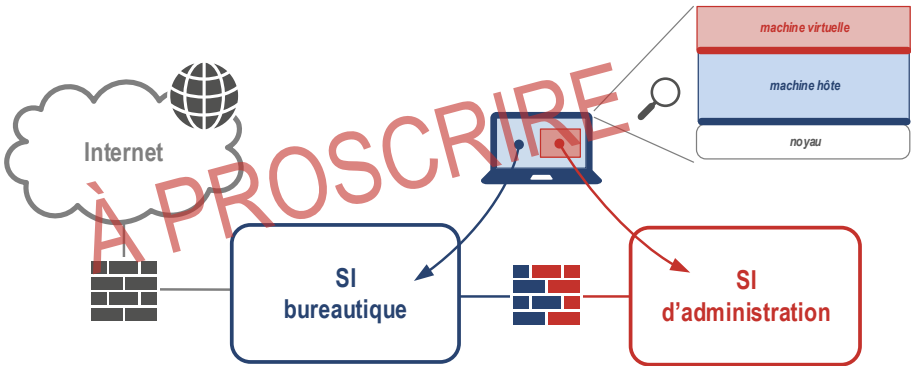


FIGURE 4.4 – Poste bureautique hébergeant une machine virtuelle d'administration

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

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

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

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

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

Attention

Il est à noter que la solution inverse, qui consiste à accéder depuis un poste bureautique à un poste d'administration par connexion à distance, est à proscrire (cf. figure 4.6).
En effet, le poste bureautique ayant potentiellement accès à Internet, sa compromission pourrait permettre à un attaquant d'espionner les actions effectuées depuis le poste (frappes clavier, copies d'écran), en particulier les connexions initiées vers le poste d'administration (ex. : adresse IP, mot de passe).
Un attaquant pourrait alors rejouer ces connexions et, par rebond, accéder aux outils d'administration puis au SI administré.

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

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

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

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

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

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

R9 - -

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

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

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

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

Attention

Il est à noter que cette solution est déconseillée pour l'administration d'infrastructures critiques (ex. : hyperviseurs, annuaires).
Par ailleurs, pour être en mesure de réagir dans les meilleurs délais en cas de crise, il est recommandé de disposer d'une procédure pour désactiver l'accès distant au SI bureautique depuis les postes d'administration.

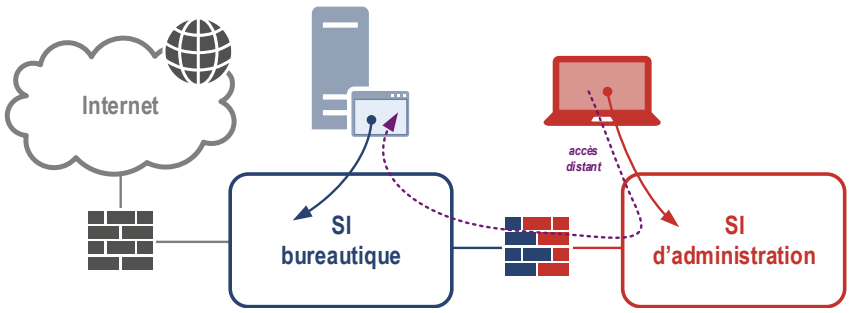


FIGURE 4.5 – Poste d'administration physique avec accès distant à un environnement bureautique virtualisé

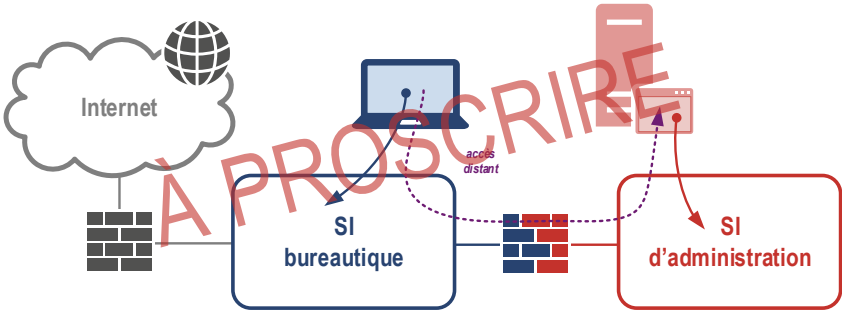


FIGURE 4.6 – Poste bureautique physique avec accès distant à un environnement d'administration virtualisé

Information

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

4.3 Mesures de sécurisation du poste d'administration

Information

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

4.3.1 Accès à Internet

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

R10

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

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

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

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

4.3.2 Sécurisation logicielle

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

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

R11

Durcir le système d'exploitation du poste d'administration

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

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

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

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

R12

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

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

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

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

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

R13

Limiter les logiciels installés sur le poste d'administration

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

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

4.3.3 Chiffrement

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

R14

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

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

Attention

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

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

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

5
Réseau d'administration

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

5.1 Protection des ressources d'administration

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

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

R15

Connecter les ressources d'administration sur un réseau physique dédié

Les ressources d'administration (ex. : postes d'administration, serveurs outils) doivent être déployées sur un réseau physiquement dédié à cet usage.
Le cas échéant, il est recommandé que les postes d'administration s'authentifient pour accéder au réseau d'administration.

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

R15 -

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

À défaut d'un réseau physique dédié, les ressources d'administration doivent être déployées sur un réseau logique dédié à cet usage en mettant en œuvre des mécanismes de chiffrement et d'authentification de réseau, à savoir le protocole IPsec. En complément, des mécanismes de segmentation logique (VLAN) et de filtrage réseau sont recommandés pour limiter l'exposition du concentrateur VPN IPsec aux seuls postes d'administration.
Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

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

R16

Appliquer un filtrage interne et périmétrique au SI d'administration

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

Information

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

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

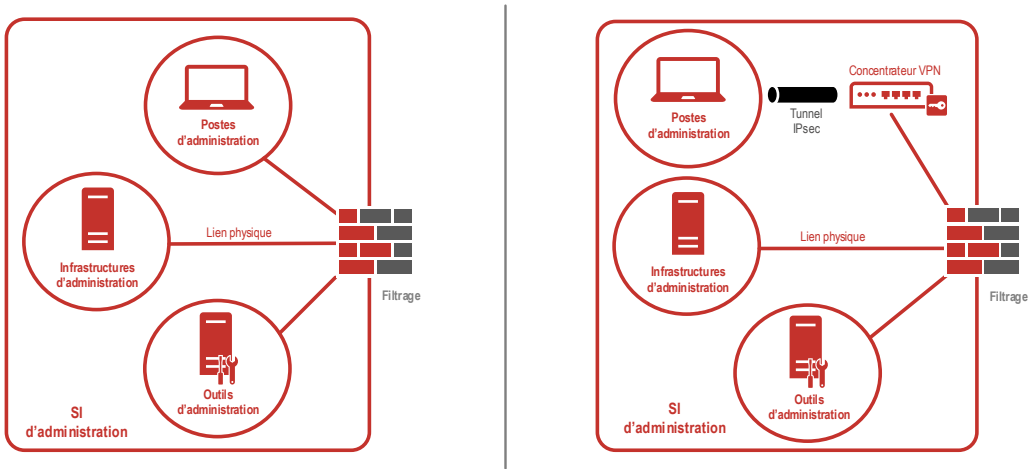


FIGURE 5.1 – Réseaux d'administration avec fonction de filtrage

5.2 Accès aux ressources administrées

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

5.2.1 Sécurisation locale de l'accès aux ressources administrées

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

R17

Appliquer un filtrage local sur les ressources administrées

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

Information

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

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

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

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

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

R18

Dédier une interface réseau physique d'administration

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

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

R18 -

Dédier une interface réseau virtuelle d'administration

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

i

Information

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

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

R19

Appliquer un filtrage entre ressources d'administration et ressources administrées

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

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

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

R20

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

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

5.2.3 Cas d'un réseau étendu

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

R21

Protéger les flux d'administration transitant sur un réseau tiers

Si les flux d'administration circulent à travers un réseau tiers ou hors de locaux avec un niveau de sécurité physique adéquat (ex. : portion de fibre noire traversant l'espace public), ceux-ci doivent être chiffrés et authentifiés de bout en bout jusqu'à atteindre une autre zone du SI d'administration ou une ressource à administrer. Dans ce cas, un tunnel IPsec doit être établi.
Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

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

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

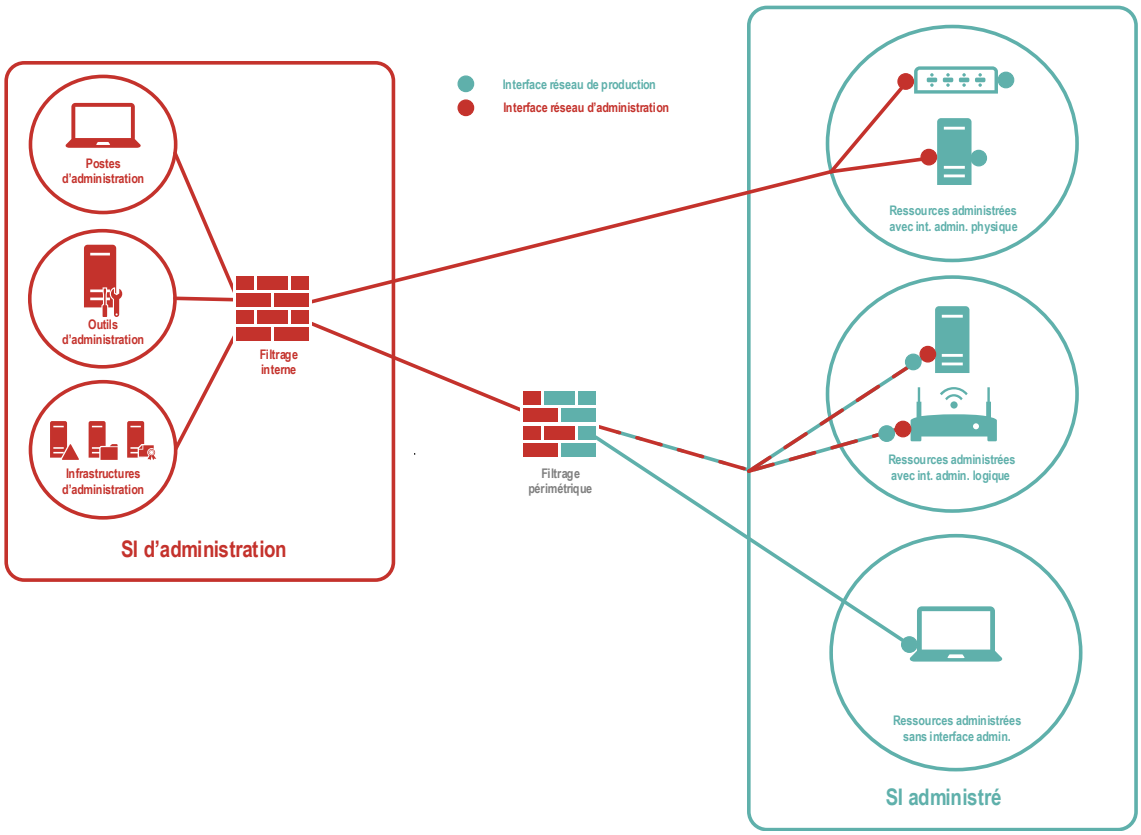


FIGURE 5.2 – Administration, sur un réseau local, à travers des interfaces d'administration dédiées (physiques ou logiques) ou une interface de production

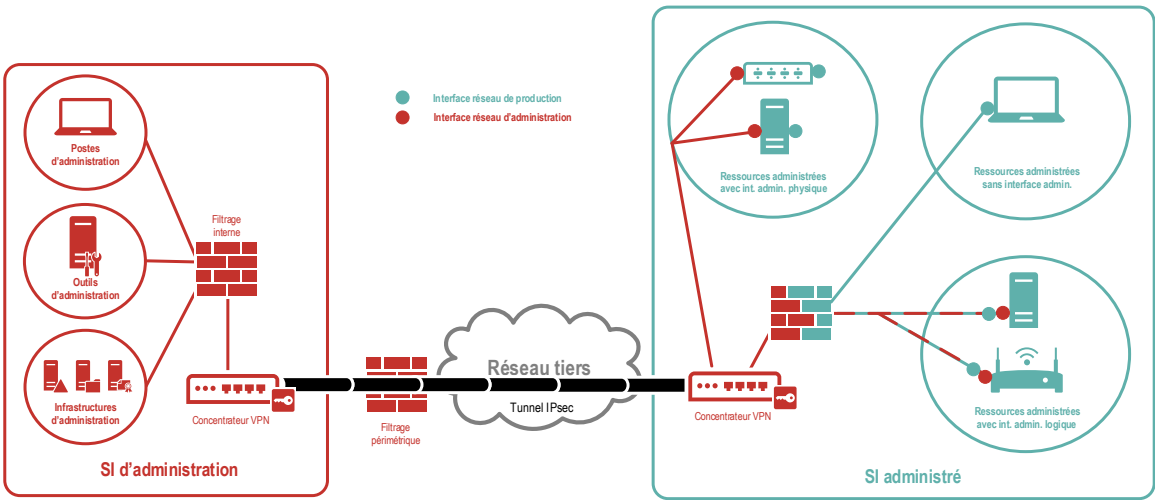


FIGURE 5.3 – Administration, sur un réseau étendu, à travers des interfaces d'administration dédiées (physiques ou logiques) ou une interface de production

6
Outils d'administration

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

6.1 Cloisonnement des outils d'administration

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

6.1.1 Outils d'administration locaux

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

6.1.2 Outils d'administration centralisés

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

R22

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

Les outils d'administration doivent être déployés par zone d'administration en fonction du juste besoin opérationnel. Cette mesure peut se traduire par la mise en œuvre de serveurs outils dédiés, intégrant par exemple les outils d'administration proposés par des éditeurs ou des équipementiers (ex. : client lourd ou service Web interagissant avec les ressources administrées).
Les recommandations de sécurisation logicielle des postes d'administration (R10, R11, R12, R13, R14) doivent être appliquées, dès que possible, aux serveurs outils d'administration.

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

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

R23

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

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

6.2 Sécurisation des flux d'administration

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

R24

Utiliser des protocoles sécurisés pour les flux d'administration

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

Attention

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

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

R24 -

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

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

6.3 Rupture ou continuité des flux d'administration

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

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

R25

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

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

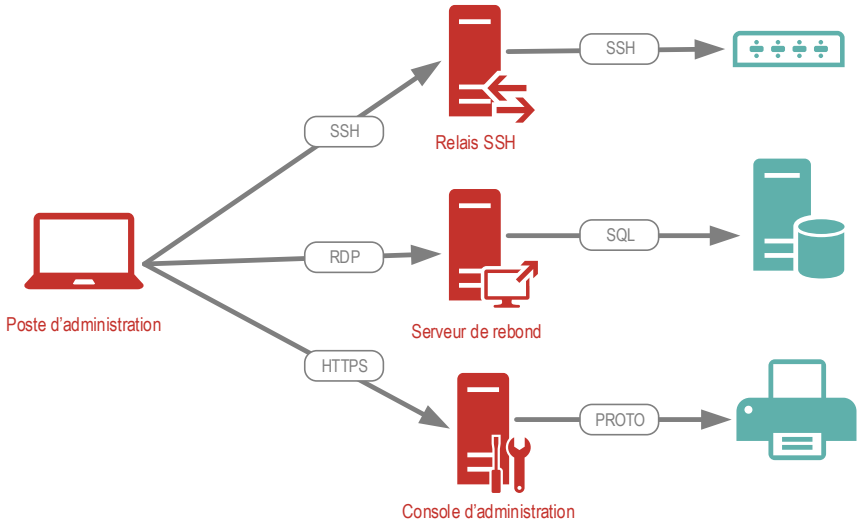


FIGURE 6.1 – Administration avec rupture protocolaire

Information

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

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

R26

Renoncer à la rupture protocolaire pour les besoins en confidentialité

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

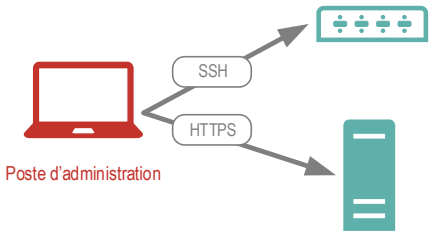


FIGURE 6.2 – Administration sans rupture protocolaire

7
Identification, authentification et droits d'administration

7.1 Identification

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

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

R27

Utiliser des comptes d'administration dédiés

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

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

R28

Protéger l'accès aux annuaires des comptes d'administration

Le ou les annuaires contenant les comptes d'administration doivent être protégés en confidentialité et en intégrité et ne pas être exposés sur des environnements de moindre confiance.
Dans le cas général, il est recommandé de déployer un ou plusieurs annuaires dédiés, au sein du SI d'administration, pour gérer les comptes d'administration et le contrôle d'accès aux ressources administrées.
Dans le cas spécifique d'un SI administré reposant sur Microsoft Active Directory, il est recommandé en premier lieu d'adopter un modèle de gestion des comptes à privilèges (ex. : modèle en trois *Tiers*) pour cet annuaire et de de sécuriser sa configuration (cf. les points de contrôle Active Directory [4]).

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

R29

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

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

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

R30

Utiliser par défaut des comptes d'administration individuels

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

Information

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

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

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

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

R31

Journaliser les événements liés aux comptes d'administration

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

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

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

R32

Prévoir un processus de gestion des comptes d'administration

Un processus organisationnel et technique de gestion des comptes d'administration et des privilèges associés doit être mis en œuvre et intégrer une procédure de contrôle et de révision régulière.
Sur l'aspect organisationnel, ce processus doit être suffisamment résilient pour pallier l'absence d'un ou plusieurs acteurs. Les entités opérationnelles doivent être associées en phase de conception et sont ensuite responsables de son application.
Sur l'aspect technique, les comptes d'administration ne doivent pas être créés, modifiés ou supprimés automatiquement depuis un outil exposé sur un SI bureautique.

7.2 Authentification

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

R33

Se référer au RGS pour choisir les mécanismes d'authentification

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

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

R34

Modifier les mots de passe par défaut des comptes natifs

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

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

R35

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

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

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

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

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

Attention

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

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

R36

Privilégier une authentification double facteur pour les actions d'administration

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

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

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

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

R37

Utiliser des certificats électroniques de confiance pour l'authentification

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

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

R38

Mettre en œuvre une gestion centralisée de l'authentification

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

7.3 Droits d'administration

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

R39

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

Les droits d'administration doivent être mis en œuvre sur l'annuaire des comptes d'administration en respectant le principe du moindre privilège.
Dans le cas spécifique des droits les plus privilégiés sur l'annuaire lui-même, seuls des administrateurs du SI d'administration peuvent en disposer.

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

R40

Attribuer les droits d'administration à des groupes

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

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

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

R41

Déployer des politiques de sécurité

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

8
Maintien en condition de sécurité

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

R42

Réaliser scrupuleusement le MCS du SI d'administration

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

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

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

R43

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

Pour la récupération des mises à jour (ex. : correctifs de sécurité ou signatures antivirales), il est recommandé de mettre en œuvre, au sein d'une DMZ, des serveurs relais dédiés au SI d'administration.
Seuls les flux initialisés depuis ces dépôts relais vers Internet doivent permettre le téléchargement des mises à jour. Des mécanismes de filtrage par liste d'autorisations permettent de restreindre l'accès aux seules sources officielles.

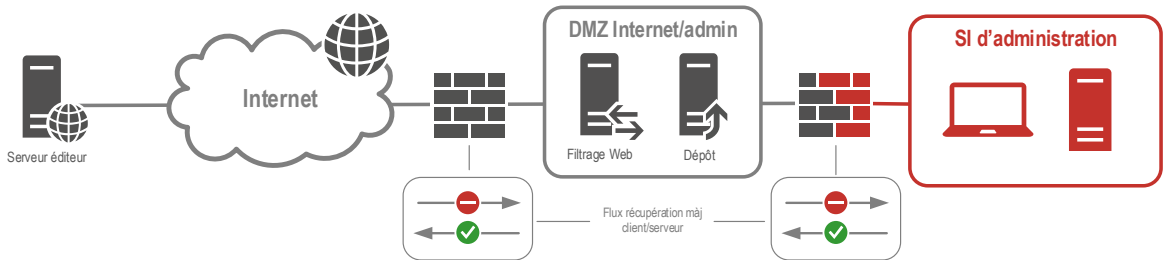


FIGURE 8.1 – Architecture de récupération et mise à disposition des mises à jour

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

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

R44

Valider les correctifs de sécurité avant leur généralisation

Il est recommandé que les administrateurs procèdent à la qualification des correctifs de sécurité avant leur mise en production et leur généralisation.
Une procédure d'urgence doit également être prévue pour réagir en cas de crise nécessitant l'application d'un correctif de sécurité au plus vite.

9
Sauvegarde, journalisation et supervision de la sécurité

9.1 Sauvegarde

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

R45

Définir une politique de sauvegarde du SI d'administration

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

9.2 Journalisation et supervision de la sécurité

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

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

R46

Dédier une zone d'administration à la journalisation

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

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

R47

Centraliser la collecte des journaux d'événements

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

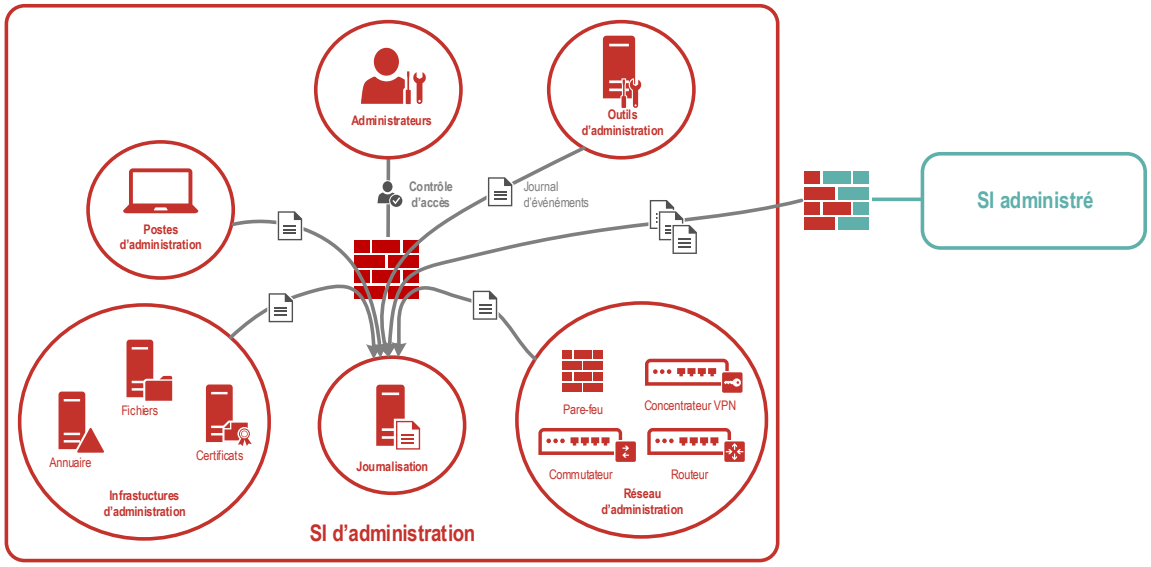


FIGURE 9.1 – Représentation fonctionnelle de la journalisation au sein du SI d'administration

Information

En complément, il est recommandé de s'approprier le guide afférent de l'ANSSI [14] et d'en appliquer les principes et les recommandations.
Pour aller plus loin sur la remontée des journaux d'événements et la supervision de sécurité, le référentiel d'exigences PDIS [25] (Prestataire de détection des incidents de sécurité) constitue un guide de bonnes pratiques.

10
Administration à distance et nomadisme

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

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

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

Attention

La mise en œuvre d'administration à distance nécessite une plus forte maîtrise du poste d'administration et de sa configuration. En effet, cette pratique augmente sensiblement les risques de compromission du SI, en particulier en cas de vol ou de perte du poste.
Les mesures de sécurité décrites dans la section 4.3 doivent donc être obligatoirement et *intégralement* mises en œuvre sur le poste d'administration utilisé dans le cadre de l'administration à distance, y compris le chiffrement des périphériques de stockage.

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

R48

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

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

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

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

R49

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

Un tunnel VPN IPsec doit être mis en œuvre entre le poste d'administration nomade, ou le site distant, et le SI d'administration.
Tous les flux entrants et sortants doivent transiter à travers ce tunnel. Toute configuration de type *split tunnelling* [9] est à proscrire strictement.
Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [16] doivent être appliquées.

Attention

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

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

R50

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

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

Information

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

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

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

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

R51

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

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

Attention

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

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

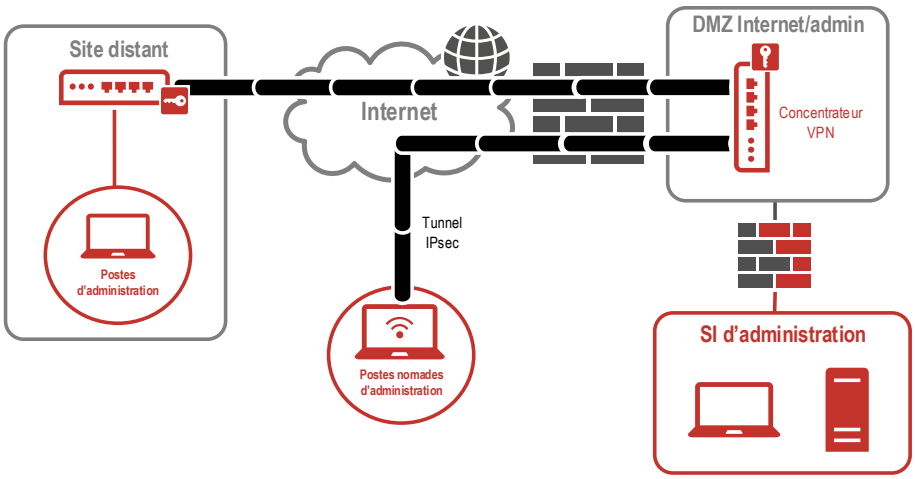


FIGURE 10.1 – Administration à distance et nomadisme

11
Systèmes d'échanges sécurisés

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

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

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

R52

Déployer des systèmes d'échanges sécurisés

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

11.1 Échanges au sein du SI d'administration

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

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

R53

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

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

11.2 Échanges en dehors du SI d'administration

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

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

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

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

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

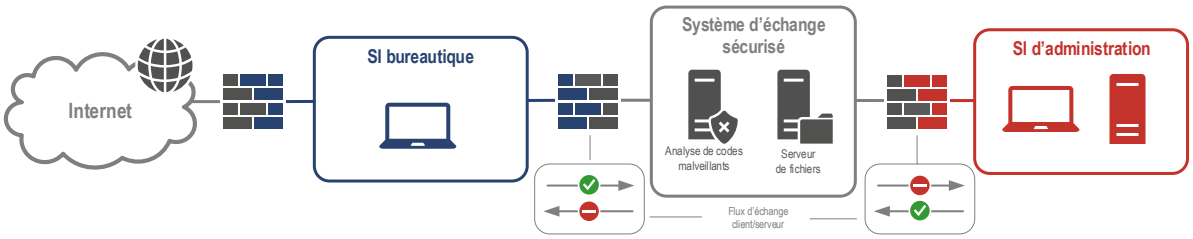


FIGURE 11.1 – Représentation fonctionnelle d'un système d'échange externe

Information

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

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

R54

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

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

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

R55

Limiter au strict besoin opérationnel l'accès au système d'échange externe

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

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

R56

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

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

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

R57

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

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

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

R58

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

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

12
Administration par des tiers et assistance à distance

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

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

Dans ce chapitre, on distingue volontairement :

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

12.1 Administration par des tiers

12.1.1 Qualification PAMS

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

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

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

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

R59

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

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

12.1.2 Administration ponctuelle à distance par des tiers

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

Attention

Les mesures proposées ici permettent uniquement de réduire le risque de compromission du SI d'administration de l'entité depuis le poste de travail d'un administrateur tiers, non maîtrisé par l'entité.
Il est donc bien entendu que ces cas d'usage doivent constituer des exceptions et être intégrés à l'analyse de risque du SI d'administration. Cette section et les recommandations associées ne constituent *en aucun cas* une alternative à l'ensemble des recommandations précédentes, notamment pour l'administration réalisée par des administrateurs internes.

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

R60

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

Afin de disposer d'un cadre juridique, il est recommandé de rédiger, au sein du contrat liant les parties, les exigences de sécurité imposées au prestataire, et idéalement intégrer la description de la solution technique d'accès à distance au SI de l'entité.
Il est recommandé de s'appuyer sur le référentiel d'exigences PAMS [26].

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

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

R61

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

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

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

Attention

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

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

R62

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

Pour l'accès à distance des administrateurs tiers, il est recommandé de dédier une chaîne d'accès, distincte notamment de celle des administrateurs disposant de moyens d'accès maîtrisés. En particulier, les équipements (ex. : concentrateurs VPN, serveurs de rebond) doivent être physiquement dédiés et ne pas être mutualisés avec des équipements utilisés par d'autres populations (utilisateurs, administrateurs internes).
Dans la mesure du possible, les équipements de filtrage et de commutation sont physiquement dédiés, en priorité les équipements périmétriques. À défaut, un cloisonnement logique est réalisé.

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

R63

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

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

R63 -

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

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

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

R64

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

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

R65 +

Dédier un annuaire aux comptes d'accès des administrateurs tiers

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

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

R66

Activer à la demande les comptes des administrateurs tiers

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

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

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

R67

Renforcer l'authentification des administrateurs tiers

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

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

R68

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

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

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

R69

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

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

Information

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

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

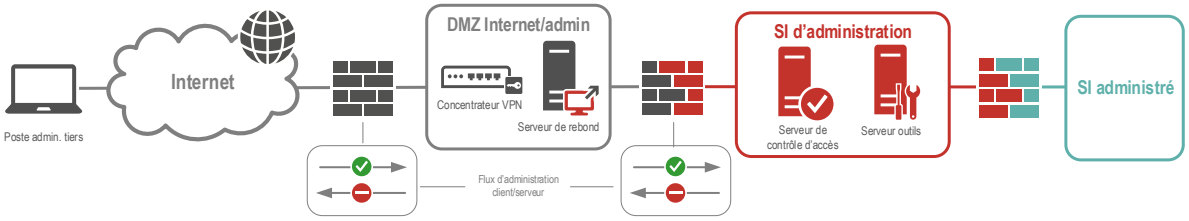


FIGURE 12.1 – Exemple d'architecture d'administration à distance par des tiers

12.2 Assistance à distance

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

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

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

Attention

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

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

12.2.1 Utilisation d'un boîtier matériel d'acquisition vidéo

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

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

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

R70

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

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

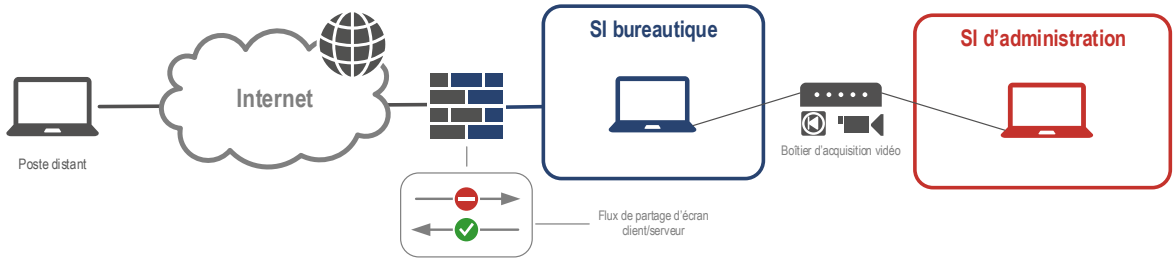


FIGURE 12.2 – Utilisation d'un boîtier matériel d'acquisition vidéo unidirectionnelle pour l'assistance à distance

12.2.2 Mise en œuvre d'une solution logicielle collaborative dédiée

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

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

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

R71

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

Pour les besoins d'assistance à distance, il est recommandé de mettre en œuvre en DMZ une infrastructure dédiée de partage d'écran. Le cas échéant, toutes les fonctions interactives vis-à-vis du poste d'administration (ex. : prise de contrôle distante) doivent être désactivées de sorte qu'aucune action d'administration ne puisse être réalisée depuis le poste de travail distant.
Les recommandations R64, R65+, R66, R67 et R69 doivent s'appliquer dans ce contexte d'assistance à distance.

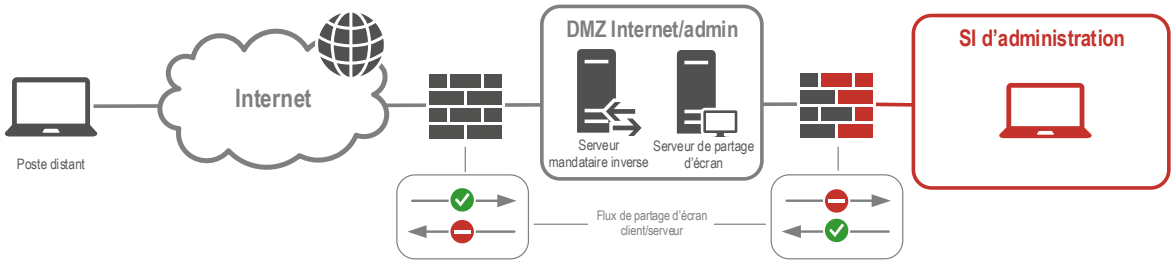


FIGURE 12.3 – Utilisation d'une solution logicielle dédiée pour l'assistance à distance

13
Cas particuliers d'architectures de SI d'administration

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

13.1 Utilisation d'un bastion

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

Attention

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

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

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

Attention

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

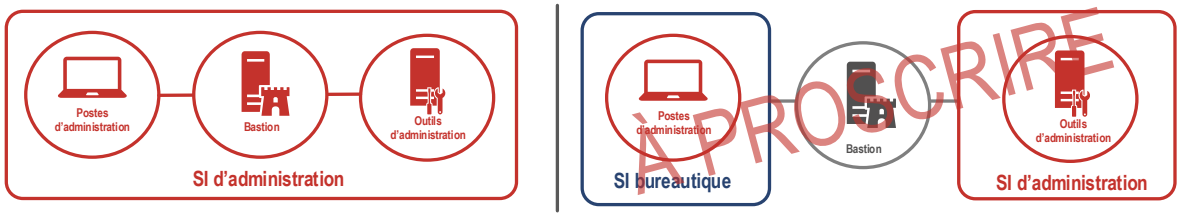


FIGURE 13.1 – Intégration d'un bastion dans un SI d'administration

13.2 Possible mutualisation du poste d'administration

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

Information

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

Attention

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

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

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

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

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

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

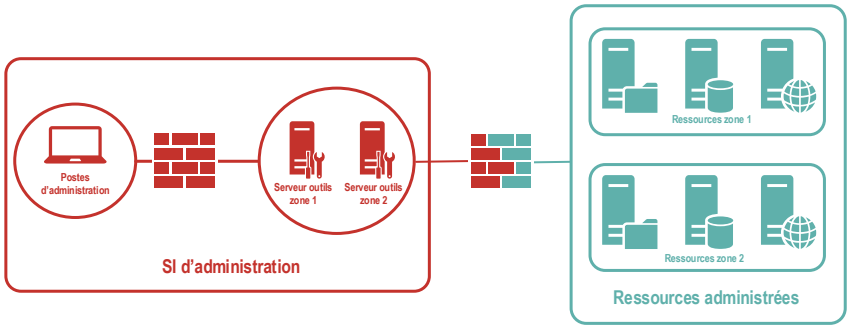


FIGURE 13.2 – Mutualisation du poste d'administration pour deux zones de confiance homogène

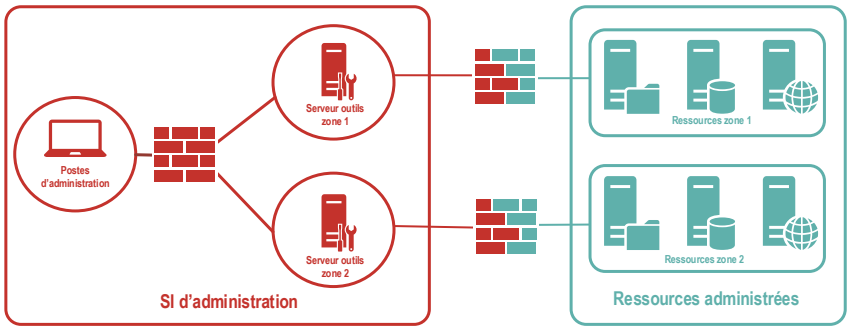


FIGURE 13.3 – Mutualisation du poste d'administration pour deux zones de confiance hétérogène

13.3 Une ou plusieurs solutions de poste d'administration ?

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

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

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

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

Attention

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

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

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

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

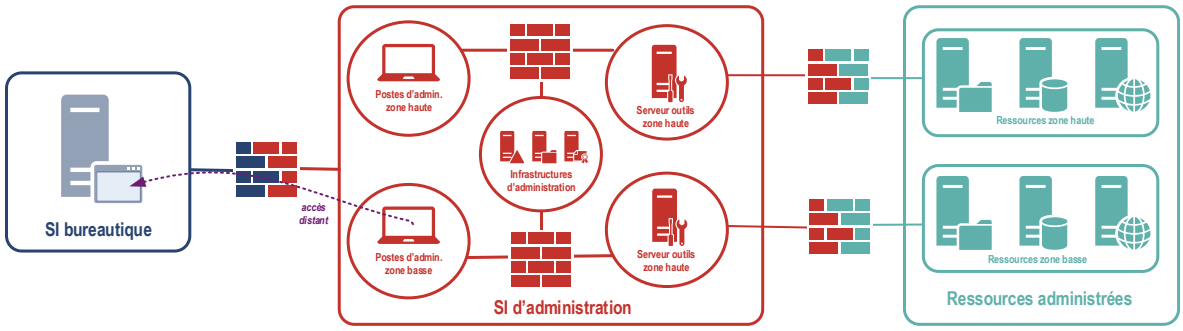


FIGURE 13.4 – SI d'administration intégrant deux solutions de poste d'administration

13.4 Administration des ressources d'administration

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

Pour cela, il est recommandé :

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

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

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

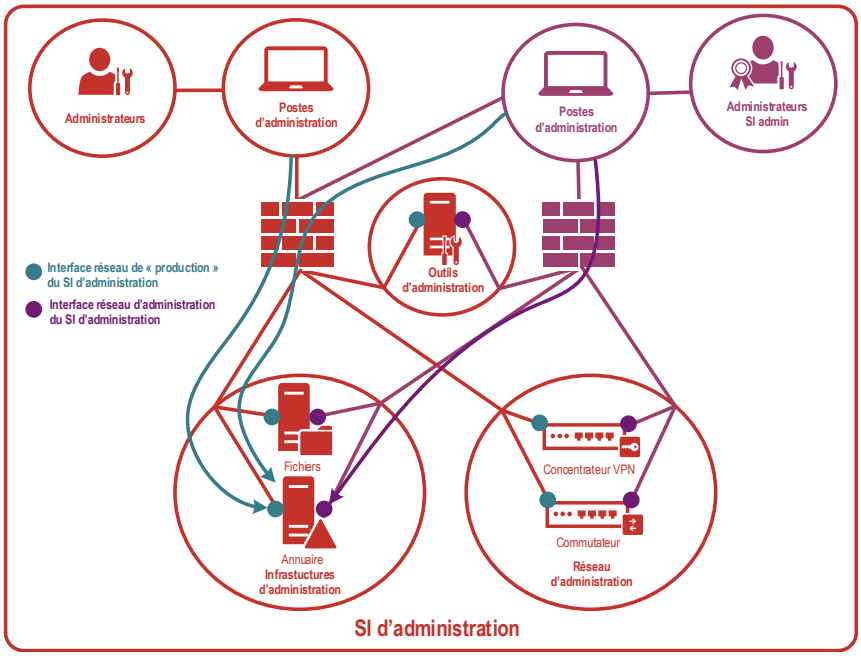


FIGURE 13.5 – Administration des ressources d'administration

13.5 Administration d'un SI déconnecté

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

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

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

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

13.6 Administration de ressources dans un cloud public

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

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

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

La figure 13.6 illustre un exemple de cette architecture.

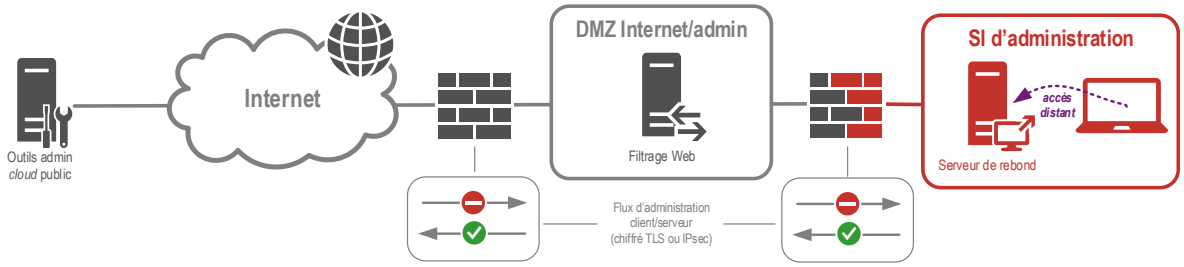


FIGURE 13.6 – Administration de ressources dans un *cloud* public

Liste des recommandations

Annexe A
Évolutions du guide

A.1 Nouvelles recommandations

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

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

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

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

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

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

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

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

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

Attention

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

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

Annexe B
Aspects juridiques

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

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

- **loyauté :** l'administrateur étant investi de larges pouvoirs de surveillance sur les données qui circulent sur les systèmes d'information de l'entreprise, le respect de règles d'éthique est attendu de sa part. Compte tenu de la « dépendance » de l'entreprise à l'égard de ce type de fonctions, la jurisprudence a tendance à se montrer plus sévère en cas de non-respect par l'administrateur de ses obligations. Des sanctions pénales peuvent être prononcées à son encontre [12], tout comme la faute grave peut être retenue dans le cadre d'une procédure de licenciement [13] ;
- **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 [14] ;
- **confidentialité :** l'administrateur est tenu à une obligation particulière de confidentialité [15], tenant notamment au secret professionnel. Il ne doit pas divulguer les informations auxquelles il aurait pu avoir accès lors de l'exercice de ses fonctions, a fortiori lorsqu'elles sont couvertes par le droit à la vie privée ou le secret des correspondances, à moins qu'une disposition législative ne l'impose (ex. en cas de découverte de contenus illicites).

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

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

12. Condamnation pour accès et maintien frauduleux à un système de traitement automatisé de données, atteinte au secret des correspondances émises par voie électronique : TGI Annecy, 4 décembre 2015, Tefal et autres.
13. CA Paris, 4 octobre 2007, n° 06/02095, Association ARFP pour le téléchargement de fichiers contrefaits ; CA Paris, 29 octobre 2008, n° 06/14072, JurisData n° 2008-373540 ou CA Paris 10 avril 2014, n°11/04388, JurisData n°201-007648, consultation d'informations personnelles relatives aux dirigeants et collègues et téléchargement de musique, consultation de sites pornographiques.
14. Cass. Soc. 10 mai 2012, n° 11-11060 ; CA Metz, 24 février 2014, n°14/00120.
15. Cass. Soc., 17 juin 2009, n° 08.40274.
16. Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), applicable à partir du 25 mai 2018.

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

D'autres réglementations, sectorielles le cas échéant, peuvent trouver à s'appliquer. À titre d'exemple, l'arrêté du 3 novembre 2014 [19] 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 [20]. 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 [21].

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

Attention

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

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

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

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

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

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

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

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

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

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

Attention

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

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

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

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

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

Annexe C
Glossaire

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

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

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

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

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

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

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

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

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

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

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

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

25. RDP (*Remote Desktop Protocol*) : protocole d'accès à distance proposé par les solutions Microsoft.
26. ICA (*Independent Computing Architecture*) : protocole d'accès à distance proposé par les solutions Citrix.
27. *Windows PowerShell* : suite logicielle incluant un interpréteur de commandes associé au langage du même nom pour l'administration automatisée des systèmes Windows.

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

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

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

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

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

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

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

Bibliographie

[1] *Guide pour les employeurs et les salariés*.
Guide, CNIL, 2010.
https://www.cnil.fr.

[2] *Supply chain attacks. Menaces sur les prestataires de service et les bureaux d'études.*
Rapport CERTFR-2019-CTI-004, ANSSI, octobre 2019.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-CTI-004.pdf.

[3] *Instruction générale interministérielle n°1300*.
Référentiel, SGDSN, novembre 2020.
https://www.ssi.gouv.fr/igi1300.

[4] *Points de contrôle Active Directory*.
Page Web CERTFR-2020-DUR-001, ANSSI, juin 2020.
https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001.

[5] *Recommandations de sécurité relatives à un système GNU/Linux*.
Note technique DAT-NT-002/ANSSI/SDE/NP v1.1, ANSSI, juillet 2012.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

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

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

[8] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation*.
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.
https://www.ssi.gouv.fr/windows10-vsm.

[9] *Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10*.
Guide ANSSI-BP-036 v1.2, ANSSI, juillet 2017.
https://www.ssi.gouv.fr/windows10-collecte-donnees.

[10] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*.
Note technique DAT-NT-013/ANSSI/SDE/NP v2.0, ANSSI, janvier 2017.
https://www.ssi.gouv.fr/windows-restrictions-logicielles.

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

[12] *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information*.
Guide Version 1.0, ANSSI, décembre 2010.
https://www.ssi.gouv.fr/infogerance.

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

[14] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[15] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://www.ssi.gouv.fr/politique-filtrage-parefeu.

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

[17] *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.
https://www.ssi.gouv.fr/nettoyage-politique-fw.

[18] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide.

[19] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet*.
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.
https://www.ssi.gouv.fr/guide-pare-feux-internet.

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

[21] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.
https://www.ssi.gouv.fr/passerelle-interconnexion.

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

[23] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901.

[24] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Note technique DAT-NT-022/ANSSI/SDE/NP v1.0, ANSSI, février 2015.
https://www.ssi.gouv.fr/securisation-admin-si.

[25] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf.

[26] *Prestataires d'administration et de maintenance sécurisées. Référentiel d'exigences*.
Référentiel Version 1.0, ANSSI, avril 2020.
https://www.ssi.gouv.fr/uploads/2020/09/anssi-pams-referentiel-v1.0.pdf.

[27] *Qualification*.
Page Web Version 1.0, ANSSI, mars 2016.
https://www.ssi.gouv.fr/visa-de-securite/qualification.

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

ANSSI-PA-022
Version 3.0 - 11/05/2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN