RECOMMANDATIONS SUR LE NOMADISME NUMÉRIQUE

GUIDE ANSSI

ANSSI-PA-054
17/10/2018

PUBLIC VISÉ :

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

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations sur le nomadisme numérique »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

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	17/10/2018	Version initiale

Table des matières

1
Préambule

1.1 Pourquoi ce guide ?

Le développement du nomadisme et du télétravail ne cesse de prendre de l'ampleur ces dernières années, et est aujourd'hui au centre des réflexions des directions informatiques.

Un nombre croissant d'espaces de cotravail (ou *co-working*) voit également le jour, par souci de réduction des coûts immobiliers, et par volonté de flexibilité.

Cela amène à réfléchir sur la manière de sécuriser ces accès distants au système d'information (SI) de l'entité, afin de gérer les besoins de confidentialité et d'intégrité des données, ainsi que l'authentification des utilisateurs.

Ce guide n'a pas pour objectif d'être exhaustif sur la sécurité générale d'une infrastructure informatique, mais bien de se focaliser sur les particularités du nomadisme, afin d'adapter le niveau de sécurité à cette nouvelle façon de travailler.

Face à ces enjeux, il est devenu important de sensibiliser l'ensemble des acteurs du nomadisme, et de prendre en compte dans la politique de sécurité des systèmes d'information (PSSI) :

- l'ouverture du SI de l'entité pour les accès distants ;
- la maîtrise des nouveaux flux liés au nomadisme ;
- la maîtrise des équipements de connexion des utilisateurs.

Le guide rappelle dans un premier temps les définitions et les risques liés au nomadisme, puis les différents éléments d'une infrastructure de connexion nomade sont étudiés, afin d'en faire ressortir les bonnes pratiques.

1.2 À qui s'adresse ce guide ?

Ce guide s'adresse avant tout aux RSSI [1], DSI [2], administrateurs et équipes d'exploitation des systèmes d'informations des structures publiques (services de l'État et collectivités territoriales) et privées (entreprises).

Les types de SI concernés par ce guide sont les SI connectés (directement ou indirectement) à Internet, traitant d'informations sensibles et non-sensibles. Une annexe aborde le cas particulier des SI « Diffusion Restreinte ».

Attention

Les SI contenant ou susceptibles de contenir des informations relevant du secret de la défense nationale au sens de l'IGI 1300 (Intruction générale interministérielle N°1300 sur la protection du secret de la défense nationale)[16] ne sont pas concernés par ce guide.

1. Responsable de la sécurité des systèmes d'information.
2. Direction des systèmes d'information.

1.3 Convention de lecture

Pour quelques recommandations, il est proposé plusieurs solutions d'architecture qui se distinguent par leur niveau de sécurité. Le lecteur a ainsi la possibilité de choisir une solution en phase avec ses besoins de sécurité.

En outre, dans une démarche itérative de sécurisation d'un SI, ces différents niveaux de sécurité proposés peuvent permettre de fixer une cible d'architecture et d'identifier les étapes pour l'atteindre.

Ainsi, les recommandations sont présentées de la manière suivante :

- R*x* constitue une recommandation à l'état de l'art ;
- R*x*- constitue une recommandation alternative à R*x*, d'un niveau de sécurité moindre.

Par ailleurs, dans ce guide, l'utilisation du verbe « *devoir* » ou encore les formulations « *il faut* » ou « *il est important* » ou « *il est nécessaire* » sont volontairement plus prescriptives que les formulations « *il est recommandé* » ou « *il est conseillé* ».

2
Présentation du sujet

2.1 Définitions

Nomadisme numérique

Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.

Télétravail

Le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication (article L. 1222-9 du code du travail). Le télétravail est donc une forme de nomadisme numérique.

SI nomadisme

Le SI Nomadisme est l'ensemble des éléments du SI de l'entité, qui entrent en jeu dans la chaîne de connexion d'un utilisateur nomade. C'est donc un sous-ensemble du SI de l'entité.

Utilisateur nomade

Un utilisateur nomade est un utilisateur déclaré dans l'entité comme disposant de droits d'accès particuliers lui permettant de se connecter au SI de son entité depuis un lieu situé en dehors des locaux de celle-ci.

Administrateur

Un administrateur est un utilisateur de l'entité disposant de privilèges spécifiques, lui permettant d'administrer des ressources du SI. Il est donc une ressource critique investie de capacités techniques d'accès aux informations métier de l'entité. Un administrateur réalise des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système, susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.

Partenaire

Un partenaire est une entité tierce, ayant l'autorisation et les moyens techniques de se connecter à distance au SI de l'entité. Le partenaire est considéré ici comme disposant de ses moyens propres de connexion au SI de l'entité.

2.2 Périmètre

La figure 2.1 décrit le périmètre du guide en couleur bleue :

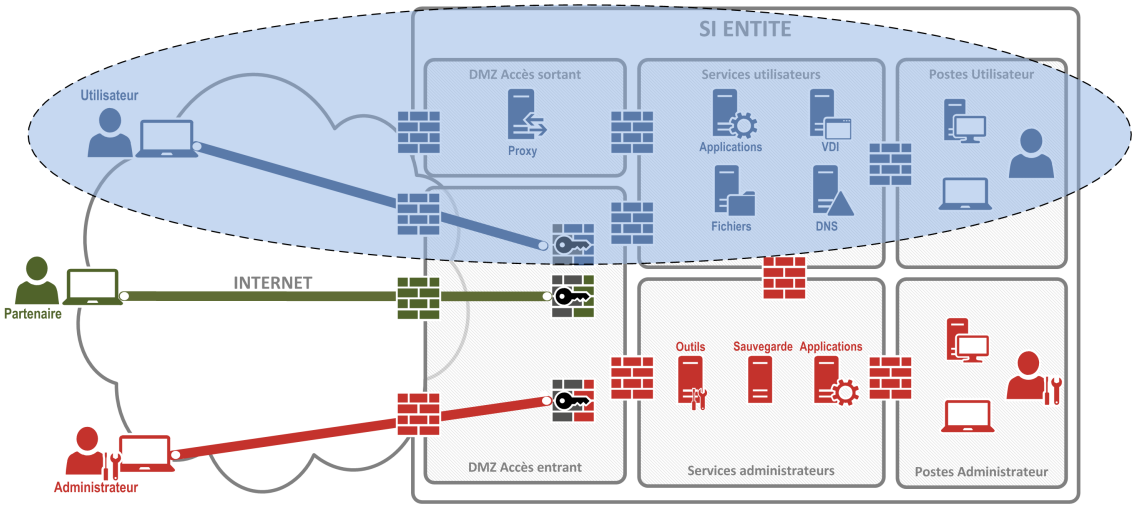

FIGURE 2.1 – Différents cas d'accès à distance et périmètre du guide

Afin de restreindre le périmètre de ce guide, et parce que d'autres guides de l'ANSSI traitent déjà de ces sujets, les cas de nomadisme concernant les utilisateurs suivants ne seront pas abordés spécifiquement :

- les administrateurs. Dans ce cas précis, il est recommandé de suivre les recommandations contenues dans le guide publié par l'ANSSI [15] ;
- les utilisateurs situés en dehors du territoire national. Dans ce cas précis, il est recommandé, en complément des préconisations de ce guide, de suivre les recommandations contenues dans le passeport de conseils aux voyageurs [9] ;
- les accès *partenaire* tels que définis dans le paragraphe 2.1 ;
- les accès des visiteurs extérieurs à l'entité.

2.3 Risques

Le lieu de connexion du travailleur nomade peut présenter des niveaux de sécurité variables selon l'environnement.

Cela dépend non seulement de la protection physique et logique du lieu (contrôle d'accès par badge, surveillance), mais également du fait que les locaux sont partagés ou non entre plusieurs entités. Un des cas les plus sensibles est celui où l'utilisateur travaille depuis un espace complètement ouvert au public (cafétéria, bibliothèque, etc.).

De même, le domicile à partir duquel un utilisateur fait du télétravail est à considérer comme un lieu non maîtrisé, car il est très difficile d'évaluer de façon pérenne l'environnement du point de vue de la sécurité.

Ainsi, la principale caractéristique du nomadisme est le degré d'exposition de l'information, en raison de la localisation de l'utilisateur dans des lieux n'ayant pas les moyens de protection physique habituellement mis en œuvre dans les locaux de l'entité. C'est le cas par exemple :

- lorsque l'on travaille à l'hôtel pendant un déplacement professionnel ;
- pendant le trajet domicile-travail, dans les transports en commun ;
- lorsque l'on travaille dans des salles d'attentes ou tout autre lieu public ;
- lorsque l'on se connecte depuis un espace de *co-working*.

Dans tous ces lieux de travail non maîtrisés par l'entité, les risques suivants sont exacerbés :

- la perte ou vol de matériel ;
- la compromission du matériel, par exemple pendant une absence temporaire de l'utilisateur ;
- la compromission des informations contenues dans le matériel volé, perdu ou emprunté ;
- l'accès illégitime au SI de l'entité (et donc la compromission de celui-ci) ;
- l'interception voire altération des informations (perte de confidentialité et/ou d'intégrité).

Ainsi, il est considéré que le lieu de travail d'un utilisateur nomade peut difficilement apporter des garanties de sécurité suffisantes par rapport au besoin de protection des informations auxquelles l'utilisateur a accès lors de son activité professionnelle nomade.

Objectif

L'objectif d'un SI nomadisme est de réussir à tendre vers un niveau de sécurité le plus proche possible de celui du SI interne de l'entité, en répondant aux risques d'exposition plus forts listés ci-dessus.

Des mesures spécifiques au nomadisme et au télétravail doivent être définies dans la PSSI de l'entité concernée.

R1

Intégrer le nomadisme dans la PSSI de l'entité

L'entité doit mettre à jour sa PSSI, c'est-à-dire redéfinir les objectifs de sécurité à atteindre, les acteurs concernés ainsi que les moyens mis en œuvre pour accomplir la cible de sécurité de son SI nomadisme.

Une fois les différents risques liés au nomadisme évoqués, le chapitre suivant aborde les différents éléments qui composent la chaîne de connexion nomade, et les mesures de sécurité permettant de réduire ou de couvrir ces risques.

3
Architecture

3.1 Architecture globale

La figure 3.1 présente de façon macroscopique les éléments qui composent un SI nomadisme :

- l'utilisateur nomade ;
- l'équipement d'accès (ou poste de travail) ;
- le canal d'interconnexion ;
- la passerelle d'interconnexion ;
- les ressources accessibles par les équipements nomades dans le SI interne de l'entité.

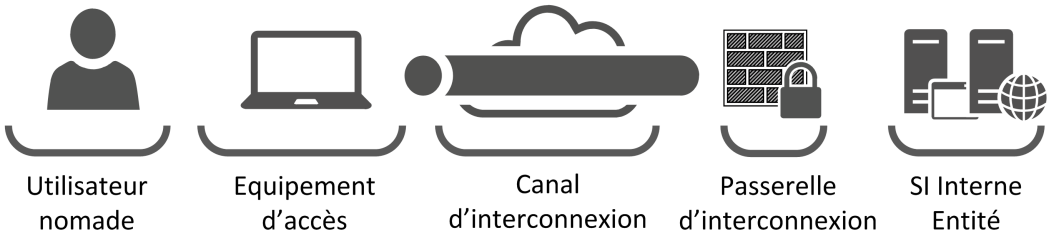

FIGURE 3.1 – Architecture globale du SI nomadisme

Dans une démarche de défense en profondeur, chaque élément doit mettre en œuvre des mécanismes de protection afin de réduire les risques d'attaques potentielles. Les sections suivantes présentent les mesures spécifiques à chaque élément, puis le chapitre suivant présente les mesures générales qui s'appliquent à l'ensemble.

3.2 Utilisateur nomade

3.2.1 Inventaire

Certaines catégories d'utilisateurs, ou bien certaines applications, du fait de leur sensibilité, doivent être exclues du périmètre du nomadisme.

R2

Réaliser l'inventaire des activités des utilisateurs compatibles avec le nomadisme

Il est important d'identifier quels sont les métiers qui sont éligibles au nomadisme et au télétravail. Le travail en dehors des locaux de l'entité peut être interdit par exemple pour les raisons suivantes :

- parce que le niveau de sensibilité des données ou de l'activité est trop élevé ;
- pour des contraintes réglementaires ;
- parce qu'il existe des restrictions liées au métier (utilisation de matériel spécifique par exemple).

Il est important de bien tenir à jour la liste des utilisateurs nomades, comme cela doit être fait pour la gestion en général des utilisateurs de l'entité. Il faut surveiller le statut des utilisateurs nomades, et notamment s'assurer que dans le cas d'un changement de fonction, ils n'exercent pas ensuite une activité incompatible avec le nomadisme numérique.

De même, il est possible de catégoriser les utilisateurs nomades en fonction du niveau de risque auquel ils sont exposés, et d'appliquer des règles spécifiques selon cette catégorisation (accès restreint, etc.). Par exemple, cela peut tenir compte de la localisation géographique de l'utilisateur nomade, lors de ses déplacements professionnels.

R3

Maîtriser la gestion des utilisateurs nomades

Il faut documenter et mettre en place des procédures pour gérer correctement les changements dans le groupe d'utilisateurs nomades. Il faut définir au minimum des procédures pour les arrivées, les mutations et les départs des utilisateurs. Celles-ci doivent être formalisées, validées et appliquées strictement. Elles concernent notamment :

- la gestion et la révocation des comptes et des droits d'accès au SI nomadisme ;
- le changement de catégorie de l'utilisateur nomade ;
- la gestion des équipements mobiles nomades.

3.2.2 Sensibilisation

Le comportement de l'utilisateur nomade est susceptible de provoquer des situations à risques, favorisant, par exemple :

- le vol ou la compromission de matériel et d'informations ;

- des indiscrétions et fuites d'informations.

Il est donc indispensable de mettre en place des campagnes de sensibilisation spécifiques pour tous les futurs utilisateurs nomades, afin que ceux-ci soient bien conscients des risques liés à ce mode de travail particulier.

R4

Sensibiliser et former les utilisateurs nomades

Les utilisateurs doivent suivre des formations à la sécurité numérique. Ils doivent maîtriser parfaitement les outils, connaître les risques et les comportements à adopter en fonction de leur lieu de travail et des circonstances. La charte informatique de l'entité doit également intégrer les règles d'usage liées au nomadisme.

3.2.3 Lien avec l'équipement d'accès

Dans un contexte d'utilisation nomade, il est fréquent que les équipements d'accès soient partagés entre plusieurs utilisateurs, si ces équipements ne sont utilisés que de façon ponctuelle par exemple. Cependant, chaque utilisateur nomade doit être identifié et authentifié lorsqu'il se connecte au SI de l'entité.

Le partage d'un poste de travail rend la tâche de supervision plus compliquée pour les administrateurs, et pose également un problème de confidentialité entre les utilisateurs qui partagent le poste, pour les données présentes localement sur celui-ci. Ainsi, il est fortement déconseillé de mettre en place des postes ou des comptes partagés pour la pratique du nomadisme.

R5

Dédier l'équipement d'accès à un utilisateur nomade identifié

Chaque équipement doit être lié à un utilisateur nomade. L'utilisateur doit être identifié et référencé dans le système de gestion d'équipements de l'entité.

Cependant si l'utilisation de postes partagés est nécessaire au bon fonctionnement de l'entité, alors il est important de mener une analyse de risques, et de prendre des mesures compensatoires, pour éviter principalement qu'un utilisateur ne puisse accéder aux données d'un autre utilisateur en partageant le même poste.

L'annexe B présente quelques-unes de ces mesures.

R5 -

Sécuriser la mise en place de postes nomades partagés

Si le partage des équipements d'accès nomades est une fonctionnalité retenue, il est important de mettre en œuvre des mesures de sécurité complémentaires pour s'assurer d'un cloisonnement entre les utilisateurs partageant le même poste de travail nomade.

3.3 Équipement d'accès

3.3.1 Maîtrise du poste

L'équipement d'accès de l'utilisateur nomade peut être entre autres :

- un poste de travail portable ;
- un mobile multifonction (ou *smartphone*) ;
- une tablette.

Toutes les recommandations suivantes s'appliquent pour tout type de matériel fourni à l'utilisateur, et quel que soit le système d'exploitation présent sur cet équipement d'accès.

Il est important de bien considérer que la connexion depuis l'extérieur au SI de l'entité ne se fait pas forcément depuis le même équipement que l'on utilise quand on travaille en interne dans les locaux de l'entité. Un utilisateur réalisant ses tâches sur un poste bureautique fixe à l'intérieur de l'entité peut utiliser une tablette lorsqu'il se déplace à l'extérieur, chez des clients par exemple.

Il est nécessaire de maîtriser complètement l'ensemble des équipements sur lesquels les utilisateurs nomades se connectent.

L'utilisation d'équipements personnels par l'utilisateur (AVEC [3] en français ou *BYOD* [4] en anglais) pour se connecter au SI de l'entité est donc à proscrire. Cela est justifié entre autres pour les raisons suivantes :

- l'impossibilité de garantir le niveau de sécurité de l'équipement personnel ;
- la multiplication des environnements utilisateur, qui rend la gestion du cycle de vie des applications difficile (navigateurs Web, interfaces homme-machine, etc.) ;
- la complexité de l'investigation en cas d'incidents.

Certains équipements permettent de mettre en œuvre un système de conteneur sécurisé et cloisonné, destiné à l'usage professionnel. À titre d'exemple, *Samsung Knox*, *Blackberry Dynamics*, ou bien les conteneurs configurables dans les solutions de *MDM* [5] tels *AirWatch* ou *MobileIron* proposent cette fonction de sécurité sur les appareils mobiles.

Cependant, même si le conteneur professionnel dispose de fonctions de cloisonnement logique ou physique, et de chiffrement du conteneur, son utilisation reste partagée avec un système d'exploitation qui n'est pas protégé.

Si l'entité fait le choix d'utiliser ce système, elle doit donc impérativement maîtriser l'ensemble de l'équipement, c'est-à-dire le conteneur dédié à l'usage professionnel, mais également la partie du système qui n'est pas protégée. En particulier, il est important que l'utilisateur ne puisse pas être en mesure d'installer n'importe quelle application présente dans les magasins (ou *store*) publics

3. Apportez votre équipement personnel de communication.
4. *Bring your own device.*
5. *Mobile device management.*

sur les systèmes protégé et non protégé. Des restrictions d'usage doivent donc être mises en place, avec un outil de MDM par exemple.

De manière non exhaustive, il est possible de citer les mesures de restrictions suivantes :

- mettre en place un *store* privé d'entreprise et interdire l'installation manuelle d'applications ;
- désactiver les services qui ne sont pas nécessaires d'un point de vue métier et qui sont potentiellement sources de menaces, comme la géolocalisation, le Bluetooth, le *NFC*[6], etc. ;
- filtrer la navigation sur Internet.

R6

Maîtriser l'équipement d'accès de l'utilisateur nomade

Seuls les équipements d'accès gérés et configurés par les équipes informatiques de l'entité, ou un prestataire mandaté, doivent pouvoir être utilisés par les utilisateurs nomades. L'utilisation d'équipements personnels est à proscrire.

De même, l'usage d'équipements professionnels fournis par l'entité pour des besoins personnels est à proscrire, ou bien a minima à encadrer strictement. Dans tous les cas, il faut toujours considérer l'usage d'un équipement professionnel pour des besoins personnels comme dangereux et source de compromission, et ceci est d'autant plus important dans le cadre du nomadisme, du fait du degré d'exposition des équipements.

3.3.2 Protection physique

Dans le cadre du nomadisme, un attaquant est susceptible de faire acte d'indiscrétion sur l'écran de l'équipement, de piéger ou de voler du matériel appartenant à l'entité.

Particulièrement dans les environnements publics (transports en commun, cafétérias, etc.), il est hautement probable que l'affichage de l'équipement d'accès soit visible par l'entourage proche de l'utilisateur nomade.

Il est donc nécessaire de protéger physiquement l'équipement d'accès lorsque le contexte d'utilisation l'exige.

R7

Mettre en œuvre des moyens de protection physique de l'équipement d'accès nomade

L'entité doit mettre à disposition les moyens suivants pour protéger les équipements d'accès :

- un filtre écran de confidentialité (pour les postes de travail, mais aussi pour les tablettes ou mobiles multifonction) ;
- des scellés pour identifier une éventuelle compromission matérielle ;
- des verrous de ports USB et RJ45 si nécessaire ;
- éventuellement un câble antivol.

6. *Near Field Communication*.

3.3.3 Contrôle d'intégrité au démarrage

Un attaquant peut introduire un code malveillant qui s'exécute avant le lancement du système d'exploitation de l'équipement d'accès, lorsque celui-ci démarre (par injection de code dans le firmware *UEFI*[7] par exemple).

De même, il est possible qu'un attaquant essaye d'amorcer l'équipement d'accès sur un autre système d'exploitation que celui prévu pour l'usage de l'utilisateur nomade. Il est donc important de désactiver, lorsque cela est possible, toute possibilité de démarrer le poste sur un autre système d'exploitation que celui installé et durci par l'entité.

En premier lieu, cela passe par l'ajout systématique d'un mot de passe pour l'accès à l'interface de configuration *UEFI* ou équivalent. Seuls les administrateurs des postes doivent avoir connaissance de ce secret d'authentification.

En complément, il est également recommandé de désactiver les fonctionnalités d'accès à distance présentes dans le BIOS. Parmi celles-ci, on peut citer par exemple *Intel AMT*[8] ou bien *Computrace*.

La vérification de l'intégrité de la séquence de démarrage est impérative, pour s'assurer qu'un attaquant n'a pas réussi à compromettre l'équipement d'accès.

Sur les systèmes d'exploitation Windows 10, il est recommandé de mettre en place le *Secure Boot UEFI*. Cette fonctionnalité permet de contrôler l'intégrité de chaque élément faisant partie de la séquence de démarrage (micrologiciels ou *firmwares UEFI*, pilotes et noyau du système d'exploitation, chargeurs de démarrage ou *bootloaders*).

Sur les systèmes d'exploitation Linux, il est possible de mettre en place un *Secure Boot* via l'utilisation combinée de *Shim* et d'un gestionnaire de boot comme *rEFInd* ou *Grub* par exemple. *Shim* est un outil de sécurité qui est utilisé pour vérifier l'intégrité des différents modules chargés au démarrage du poste. Il inclut un programme (*MokManager*) permettant également de signer des binaires liés au démarrage. Lors du processus de *Secure Boot*, *Shim* vérifie tout d'abord la signature du gestionnaire de boot (*rEFInd* ou *Grub*), puis il contrôle l'intégrité du noyau à amorcer. Plusieurs versions de *Shim* ont été elles-mêmes signées par la *Microsoft Secure Boot Key*, reconnue par les différents constructeurs.

Une base de données de signatures autorisées et révoquées (liste blanche et noire) est installée dans une mémoire sécurisée, initialisée par le constructeur et appelée en général *NVRAM*.

La plupart de ces bonnes pratiques sont détaillées dans les guides de l'ANSSI concernant Windows 10 [6] et Linux [2, 4].

7. *Unified extensible firmware interface.*
8. *Active management technology.*

R8

Maîtriser l'intégrité de la séquence de démarrage de l'équipement d'accès nomade

Il faut prendre des mesures sur chaque élément intervenant dans la séquence de démarrage de l'équipement et utiliser les méthodes de protection adéquates :

- désactiver les modules d'accès à distance du BIOS, et la possibilité de démarrer sur un autre système que celui prévu ;
- utiliser les fonctions de *Secure Boot UEFI* ou équivalents, pour les environnements Windows et Linux.

3.3.4 Chiffrement des disques

Un équipement d'accès peut être volé ou perdu en situation de nomadisme. Il est primordial que des personnes autres que l'utilisateur légitime ne puissent pas avoir accès à des données sensibles.

Même sans disposer d'identifiants de connexion sur le poste utilisateur, il est toutefois possible pour un attaquant de lire toutes les données contenues sur le disque dur de l'équipement. Afin de s'en prémunir, il est impératif de mettre en œuvre un mécanisme de chiffrement adéquat des disques durs sur le poste de travail nomade.

Il est recommandé de chiffrer, si l'outil le permet, l'intégralité du disque, ou au minimum, toutes les partitions pouvant contenir des informations sensibles, ainsi que la partition système car l'accès à celle-ci peut orienter un attaquant sur les possibles méthodes de compromission du poste.

Il est notamment possible de suivre le guide sur les recommandations pour une utilisation sécurisée de Cryhod [8].

R9

Mettre en œuvre une solution de chiffrement de disque sur les équipements d'accès nomade

Un chiffrement de disque doit être mis en place. Celui-ci doit être complet (*Full Disk Encryption*) et respecter l'état de l'art des mécanismes cryptographiques mis en œuvre.

Information

Le chiffrement concerne tous les disques durs mais il également recommandé de chiffrer les périphériques amovibles si l'utilisation de ceux-ci est requise.

3.3.5 Périphériques amovibles

Du fait de l'absence de sécurité physique sur le lieu d'utilisation, un attaquant est susceptible d'avoir plus facilement un accès direct au matériel de l'utilisateur nomade.

Par exemple, il est possible de compromettre l'équipement en y connectant temporairement une clé USB permettant l'écoute réseau passive, afin de récupérer des condensats (ou *hash*) de mots de passe d'authentification. Il existe également d'autres moyens de compromissions par support

USB, comme le mécanisme qui permet l'injection de commandes clavier au travers d'une clé se faisant passer pour un support de stockage. Il est aussi envisageable que le support amovible exploite des vulnérabilités liées au système d'exploitation de la machine pour y déployer des logiciels malveillants. Enfin, certaines clés s'attaquent physiquement au poste utilisateur en provoquant une surtension électrique, qui peut mettre hors d'état certains composants matériels comme le disque dur, les contrôleurs de la carte mère, etc.

Face à toutes ces menaces, il est important d'évaluer le risque d'ouvrir les périphériques d'accès sur le poste d'accès nomade, en fonction des besoins utilisateurs.

Une interdiction stricte des périphériques amovibles peut se faire par les moyens suivants :

- désactiver les périphériques dans le BIOS (en considérant néanmoins que certains composants internes au poste utilisent l'USB comme la caméra, la puce Bluetooth, etc.) ;
- désinstaller les modules de gestion de l'USB dans le système d'exploitation ;
- désactiver l'utilisation de ports USB par *GPO* dans l'*Active Directory* pour les environnements Windows.

Cependant, pour des raisons de confort d'utilisation ou par besoin métier, il est possible que les utilisateurs soient contraints de travailler en connectant régulièrement des clés USB de stockage, pour y récupérer ou y déposer des documents (échanges avec des clients par exemple).

De même, l'usage de clavier et de souris connectés en USB sur un poste portable est devenu de plus en plus fréquent au regard du gain de temps que l'utilisateur peut avoir, comparé au clavier intégré et au pavé tactile (ou *Touchpad*).

La mise en place d'une authentification forte de l'utilisateur par un système de carte à puce pourrait également nécessiter de connecter un lecteur USB sur le poste nomade.

Si l'un ou plusieurs de ces besoins sont identifiés, il faut alors prendre des mesures de sécurité pour réduire les risques associés :

- connecter uniquement du matériel fourni par l'entité ;
- bloquer techniquement l'utilisation d'autres matériels en filtrant les équipements autorisés et en vérifiant périodiquement l'inventaire des équipements amovibles autorisés ;
- lorsque cela est possible, mettre en œuvre une fonction de reconnaissance de signature cryptographique entre le support amovible et l'équipement d'accès ;
- inspecter systématiquement le contenu par des solutions antivirales lors de la connexion du support amovible et bloquer ce dernier ou le mettre en quarantaine en cas de fichier vérolé ;
- journaliser les actions réalisées depuis les périphériques USB (montage, copie, suppression, accès aux fichiers, etc.) ;
- désactiver les fonctions de démarrage et d'exécution automatique (*Autorun* et *Autoplay*) sur les équipements d'accès.

Attention

L'utilisation de filtrage par *Vendor ID*, *Product ID* ou *USB Serial Number* est une première mesure compensatoire, mais celle-ci peut facilement être contournée par des outils d'usurpation d'identité USB (*USB Spoofing*) et ne suffit pas pour sécuriser complètement la connexion de périphériques amovibles.

R10

Maîtriser la connexion de supports amovibles sur l'équipement d'accès nomade

Il est recommandé d'interdire la connexion de tout support amovible et de bloquer tous les périphériques d'accès (USB, lecteurs DVD, cartes SD, etc.) par le moyen le plus approprié. Si cette interdiction stricte n'est pas possible, il est important de mettre en œuvre des mesures de filtrage et de traçabilité pour l'utilisation d'équipements amovibles.

3.3.6 Restrictions des privilèges de l'utilisateur

L'utilisateur ne doit pas être en mesure de modifier la configuration, et notamment désactiver ou désinstaller les moyens de connexion logiciels installés sur son poste nomade. Cela implique qu'il n'est pas administrateur local de son poste.

Le lancement des moyens de connexion doit être automatique, sans possibilité pour l'utilisateur nomade de tuer les processus ou d'arrêter les services.

L'utilisateur ne doit à aucun moment être en mesure de modifier les barrières de protection mises en place sur son poste nomade.

R11

Interdire à l'utilisateur le débrayage ou la modification des moyens de connexion au SI nomadisme

Cette recommandation inclut tous les logiciels nécessaires à la connexion, installés sur l'équipement d'accès de l'utilisateur, comme le client de connexion *VPN* ou le pare-feu local.

3.3.7 Durcissement système

L'équipement d'accès nomade dispose en général de plusieurs applications ou logiciels installés par défaut lors de l'installation du système d'exploitation. De même, certains services réseaux sont activés lors de l'installation alors même qu'ils ne seront jamais utilisés pour un besoin métier. Il est donc important d'analyser l'intégralité des applications et des services installés sur le système, et de désinstaller ceux qui ne sont d'aucune utilité.

Les moyens de connexion possibles sur un poste de travail sont en général assez nombreux. Ainsi, si certains d'entre eux ne sont jamais utilisés dans le cadre du nomadisme, alors il est conseillé de supprimer les pilotes et les modules de gestion de ces composants.

De même, si jamais plusieurs moyens de connexion sont proposés aux utilisateurs nomades, il est recommandé de faire en sorte qu'un seul moyen de connexion soit utilisable à la fois. Par exemple, si l'utilisateur se connecte au moyen d'un câble RJ45 sur un réseau Ethernet, alors la désactivation de la carte réseau Wi-Fi du poste doit être automatique.

Ces recommandations s'appliquent ici au même titre que pour le SI interne de l'entité et les utilisateurs standards. Il s'agit principalement d'un rappel de bonnes pratiques.

R12

Réduire la surface d'attaque sur le système d'exploitation de l'équipement d'accès nomade

De manière générale, il est recommandé de respecter les bonnes pratiques suivantes :

- utiliser uniquement des équipements initialisés à partir d'un standard d'installation propre à l'entité, c'est-à-dire une image de référence ou *Master* ;
- n'installer que les logiciels et les modules strictement nécessaires ;
- réduire au strict besoin le nombre de comptes à privilèges ;
- désactiver les technologies non utilisées selon le contexte d'usage : Wi-Fi, 3G, Bluetooth, NFC, etc.

Des outils sont disponibles sur les systèmes d'exploitation Windows et Linux pour réaliser un durcissement du système d'exploitation.

En environnement Windows, *AppLocker* permet de définir des règles d'accès aux différentes applications déployées sur le poste, pour des utilisateurs donnés. Il est possible de filtrer en fonction des chemins d'accès, des signatures de binaires, des versions ou des éditeurs par exemple. L'outil permet également de mettre en œuvre une journalisation d'évènements liés au démarrage d'applications par les utilisateurs.

L'outil *EMET*[9] permet de renforcer la sécurité pour réduire la probabilité d'attaques liées à l'exploitation de vulnérabilités dans la gestion de la mémoire, lors de l'exécution d'applications. *EMET* met en œuvre différentes protections :

- marquage de pages mémoires pour interdire l'exécution de code sur celles-ci (*DEP*[10]) ;
- protection contre les vulnérabilités liées à la levée d'exceptions (*SEHOP*[11]) ;
- chargement de librairies dans des espaces mémoires alloués de manière aléatoire, pour éviter le rejeu d'attaques (*ASLR*[12]).

9. *Enhanced mitigation experience toolkit.*
10. *Data execution prevention.*
11. *Structured exception handling owerwrite protection.*
12. *Address space layout randomisation.*

Attention

Il est à noter qu'*EMET* n'est plus maintenu par Microsoft depuis le 31 juillet 2018, les fonctionnalités de cet outil étant désormais intégrées nativement dans les dernières versions de Windows 10 avec *Windows Defender Exploit Guard*. L'utilisation d'*EMET* n'a un intérêt que dans le cas de contraintes techniques fortes imposant le maintien de postes en version Windows 7 ou 8.

Enfin, les fonctions *Credential Guard* et *Device Guard* de Microsoft permettent respectivement de protéger les processus d'authentification (*LSASS* [13]) et le code du noyau système, dans des environnements virtuels cloisonnés, reposant sur la technologie *VBS* [14].

En environnement Linux, la solution *SELinux* permet de définir des politiques de sécurité très fines. L'outil ajoute des attributs étendus aux fichiers présents sur le système, pour définir un contexte d'utilisation. Les processus et utilisateurs devront respecter les règles de filtrage du contexte d'utilisation pour être en mesure d'accéder à chacun de ces fichiers (en lecture, en écriture, en exécution...). Un contexte est composé d'une identité spécifique *SELinux*, d'un rôle, d'un domaine d'utilisation, et également d'un niveau de sensibilité de la donnée.

Toujours sous Linux, *AppArmor* repose sur des règles et des autorisations liées à des exécutables. Des profils d'utilisation sont définis, permettant de restreindre les exécutables ciblés selon deux critères principaux : l'accès aux ressources (fichiers, périphériques, etc.) et le niveau de privilèges requis (*capabilities* Linux [15]).

La plupart de ces bonnes pratiques sont détaillées dans les guides de l'ANSSI concernant Windows 10 [3, 6, 7] et Linux [1, 2, 4].

R13

Mettre en œuvre un durcissement système de l'équipement d'accès nomade

Il est recommandé d'utiliser les outils suivants pour sécuriser l'équipement d'accès de l'utilisateur nomade :

- *Applocker, EMET, Device Guard, Credential Guard* sur des systèmes Windows ;
- *SELinux, AppArmor* sur des systèmes Linux.

3.3.8 Mise en quarantaine

Dans les prérequis de connexion d'un équipement d'accès nomade, il peut être utile de vérifier que toutes les fonctions de sécurité sont bien présentes, et à jour.

Par exemple, dans le cas où un utilisateur ne s'est pas connecté depuis plusieurs mois sur son poste nomade, celui-ci n'aura pas pu bénéficier des derniers correctifs de sécurité ainsi que des dernières signatures antivirales. Dans ce cas, connecter l'équipement d'accès directement sur le SI interne de l'entité peut présenter un risque. Lorsque cela est possible il est pertinent de connecter dans un premier temps cet équipement dans un environnement cloisonné de quarantaine.

13. *Local security authority subsystem service.*
14. *Virtualisation based security.*
15. Les *capabilities* sont des droits spécifiques intégrés au *Linux Security Modules* et associés à des opérations à privilèges.

Cet environnement ne donne accès qu'à des services de remédiation (mises à jour antivirus, applications de correctifs de sécurité, etc.). Une fois cette mise en conformité réalisée, l'équipement peut alors basculer sur l'environnement de production nomade.

Il n'y a pas, à la date de rédaction de ce document, de produit de mise en quarantaine et de remédiation disposant d'un visa de sécurité de l'ANSSI.

Attention

Dans certains cas, lorsque des vulnérabilités critiques pour le SI ont été détectées, et que la mise en quarantaine n'est pas réalisable (parce que les outils ne le permettent pas), alors il est recommandé de réinitialiser complètement l'équipement avant de le connecter de nouveau sur le SI nomadisme.

Pour compléter ce sujet, de nouvelles fonctionnalités de contrôle d'intégrité sont apparues avec les dernières versions des systèmes d'exploitation. Elles permettent d'exécuter une série de tests de sécurité au démarrage du poste de travail, comme contrôler l'intégrité de la fonction *secure boot UEFI*, la bonne éxecution des services de sécurité du noyau ou encore de l'outil de chiffrement du disque.

Cependant ces outils présentent souvent deux inconvénients :

- d'une part, ce contrôle d'intégrité concerne uniquement la phase d'amorçage du système d'exploitation et la vérification de bon fonctionnement de certains éléments du noyau. Il ne peut donc garantir complètement que le poste de travail n'a pas été compromis puisqu'une vulnérabilité liée à une application utilisateur (le navigateur Web par exemple) n'est généralement pas détectée par ce contrôle ;
- d'autre part, ces services de contrôle fonctionnent généralement en nuage, et nécessitent donc que le poste utilisateur soit en mesure de contacter directement un serveur distant sur Internet. Cette contrainte contredit l'exigence de sécurité sur les flux autorisés depuis les postes, à la section 3.4.3, où il est recommandé de limiter au maximum les flux vers l'extérieur en dehors du tunnel VPN.

À titre d'exemple, Microsoft a récemment implémenté ce service appelé *Remote Health Attestation* pour les environnements Windows.

R14

Activer des mécanismes de mise en quarantaine et de remédiation pour les équipements nomades non conformes aux mises à jour de sécurité

Il faut mettre en œuvre des mesures techniques permettant de bloquer temporairement toutes les connexions des équipements non conformes au SI nomadisme. Il faut alors procéder à la mise à jour des équipements non conformes au moyen d'un ou plusieurs serveurs de remédiation (correctifs de sécurité, anti-virus) situés dans une zone démilitarisée (*DMZ*).

3.3.9 Verrouillage du poste

Pour répondre au risque d'oubli de la part d'un utilisateur nomade de verrouiller logiciellement son équipement d'accès, il est recommandé de réduire la durée d'inactivité avant verrouillage automatique du poste. Il est de même possible de réduire la durée d'expiration (*timeout*) des sessions inactives dans les différentes applications utilisées par le travailleur nomade.

R15

Réduire la durée d'inactivité avant verrouillage automatique de la session utilisateur

La durée d'inactivité avant verrouillage du poste doit être un compromis entre la sécurité physique des situations de nomadisme et les besoins métiers des utilisateurs. Il est recommandé une valeur maximum de 5 minutes.

3.4 Canal d'interconnexion

3.4.1 Schéma général

L'utilisateur connecte un équipement d'accès professionnel depuis un réseau non maîtrisé (par exemple son réseau local à domicile ou un espace de *co-working*).

Le canal d'interconnexion doit être un lien sécurisé entre l'équipement d'accès et le SI de l'entité. Il est composé :

- d'un client logiciel situé sur l'équipement d'accès (client *VPN* [16]) ;
- d'un tunnel d'interconnexion VPN ;
- d'un équipement de terminaison VPN.

Tous les flux en provenance et à destination de l'équipement d'accès doivent être maîtrisés.

16. *Virtual private network* : désigne un réseau privé virtuel, c'est-à-dire une technologie permettant de créer un tunnel de communication entre deux éléments.

La figure 3.2 illustre une connexion à distance de l'équipement d'accès vers le SI de l'entité :

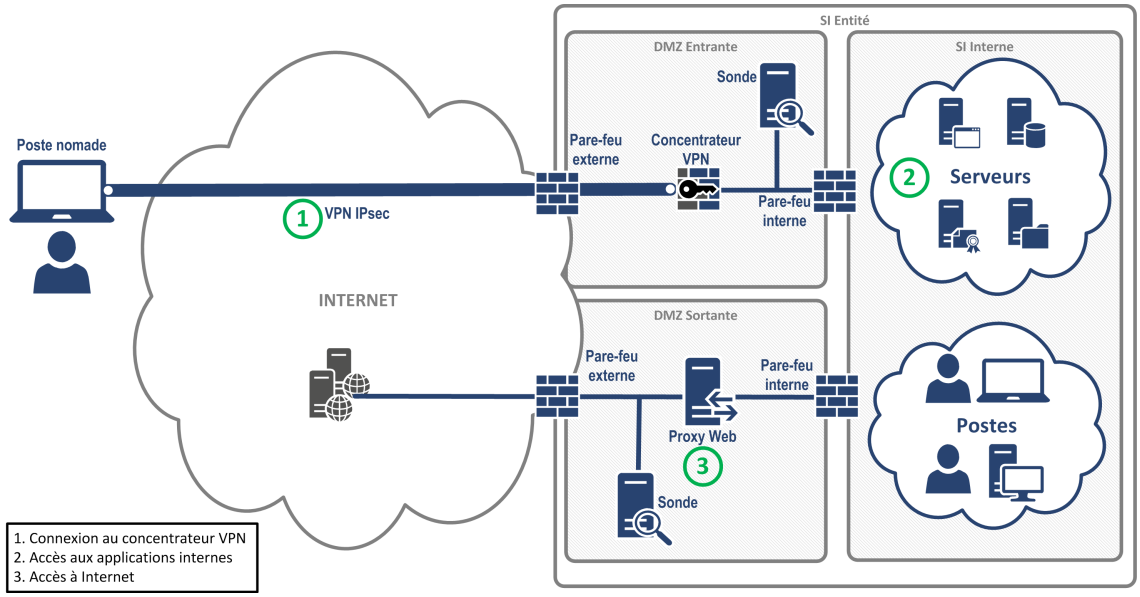

FIGURE 3.2 – Schéma général de connexion VPN nomade

Dans le schéma d'architecture présenté, l'entité met en place deux DMZ. La première est nommée DMZ entrante, et elle est composée des équipements de sécurité permettant la connexion de l'utilisateur nomade (concentrateur VPN, sonde, pare-feu...) au SI nomadisme. Une fois que le tunnel VPN est établi, l'utilisateur accède aux ressources internes de son entité (applications métiers), et peut également accéder à Internet au moyen d'une DMZ sortante, disposant d'équipements de sécurité prévus pour cet usage (sonde, *proxy*, pare-feu...).

3.4.2 Technologie VPN

Un attaquant peut tenter de se faire passer pour l'utilisateur ou usurper l'équipement d'accès, mais également essayer d'intercepter les communications entre l'équipement d'accès et l'équipement de terminaison VPN (en se faisant passer pour ce dernier, suivant l'attaque de l'homme du milieu ou *man-in-the-middle attack*).

Il est donc important d'utiliser des mécanismes robustes de chiffrement, d'authentification et d'intégrité pour la mise en place du canal d'interconnexion d'un équipement d'accès nomade. L'ANSSI recommande l'utilisation du protocole IPsec plutôt que TLS pour la mise en place du tunnel VPN entre l'équipement d'accès et l'équipement de terminaison VPN, notamment pour les raisons suivantes :

- la surface d'attaque d'IPsec est plus réduite comparativement à celle de TLS. Les opérations de sécurité critiques (comme les fonctions utilisant les clés) d'IPsec se font en environnement cloisonné, au sein du noyau du système d'exploitation, tandis que TLS s'exécute généralement dans l'espace utilisateur, depuis la couche applicative ;
- les mécanismes de choix initial des algorithmes entre le client et le serveur sont plus robustes en IPsec qu'en TLS. De manière générale, la conception et la séparation des différentes fonctions de

sécurité est plus aboutie dans IPsec (définition de *SPD* [17] et de *SA* [18], négociation des échanges de secrets partagés avec le protocole *IKE* [19], mécanisme de création et modification automatiques de SA avec *ISAKMP* [20], mécanisme de *Re-key* et de *Re-Auth* pour le renouvellement des clés de sessions et la réauthentification) ;

- la gestion par défaut des autorités de certification autorisées est plus permissive dans les différentes implémentations de TLS que dans celles d'IPsec ;
- la majorité des vulnérabilités récentes concerne les implémentations des protocoles SSL et TLS (*POODLE, BEAST, CRIME, FREAK, Heartbleed, etc.*). De manière générale, ce n'est pas tant le protocole TLS en lui même qui est source de vulnérabilités, mais plutôt des mauvaises implémentations développées dans des langages qui n'apportent pas toujours un niveau de sécurité satisfaisant.

R16

Mettre en œuvre un tunnel VPN IPsec à l'état de l'art pour le canal d'interconnexion nomade

La solution VPN IPsec doit être à l'état de l'art pour les mécanismes de chiffrement et d'authentification mutuelle (se référer au guide de l'ANSSI concernant les bonnes pratiques d'implémentation d'IPSec [13]).
En particulier, il est impératif d'utiliser le protocole IKEv2 de négociation des échanges de secrets partagés.

R16 -

Mettre en œuvre un tunnel VPN TLS à l'état de l'art pour le canal d'interconnexion nomade

Si une solution VPN TLS est utilisée, elle doit être à l'état de l'art pour les mécanismes de chiffrement et d'authentification mutuelle (se référer au guide TLS de l'ANSSI [14]).

Attention

En particulier, tel qu'indiqué dans les guides, il est nécessaire de limiter les suites cryptographiques utilisées pour la négociation entre le client VPN et le concentrateur VPN, afin de n'autoriser que les suites cryptographiques les plus robustes.

3.4.3 Maîtrise des flux réseaux sur le poste de travail

Il est possible que l'environnement interne de l'entité mette en œuvre des fonctions de filtrage réseau, sur les connexions entrantes et sortantes des postes utilisateurs se connectant en interne. De même, la configuration des commutateurs au sein de l'entité peut intégrer des fonctions tels que le *PVLAN* [21], ou une authentification des postes par protocole *802.1x*.

17. *Security policy database.*
18. *Security association.*
19. *Internet key exchange.*
20. *Internet security association and key management protocol.*
21. *Private VLAN* : technologie permettant notamment d'interdire les connexions directes entre les clients d'un même VLAN.

Dans l'environnement externe à l'entité, ces fonctions de sécurité n'existent généralement pas. Il faut donc impérativement protéger l'équipement d'accès en activant le pare-feu local directement sur celui-ci. Cette préconisation est une bonne pratique générale, présente dans le guide d'hygiène [10], mais elle revêt ici un caractère *obligatoire* en environnement nomade.

R17

Activer le pare-feu local sur l'équipement d'accès nomade

Il est indispensable d'activer le pare-feu local pour bloquer tous les flux entrants et sortants, autres que ceux nécessaires à l'établissement de la connexion VPN vers le SI de l'entité.
La liste des flux autorisés doit être revue régulièrement, notamment afin de supprimer les règles obsolètes.

Il est impératif que l'utilisateur nomade ne puisse pas utiliser sa connexion réseau locale pour d'autres flux que ceux nécessaires à l'établissement du tunnel VPN. Par exemple, un utilisateur nomade en télétravail ne doit pas, depuis son poste professionnel, naviguer directement sur Internet, utiliser son imprimante personnelle installée chez lui ou encore accéder à des équipements personnels.

La figure 3.3 distingue les différents flux qui doivent être autorisés et interdits lors de la configuration du pare-feu local de l'équipement d'accès :

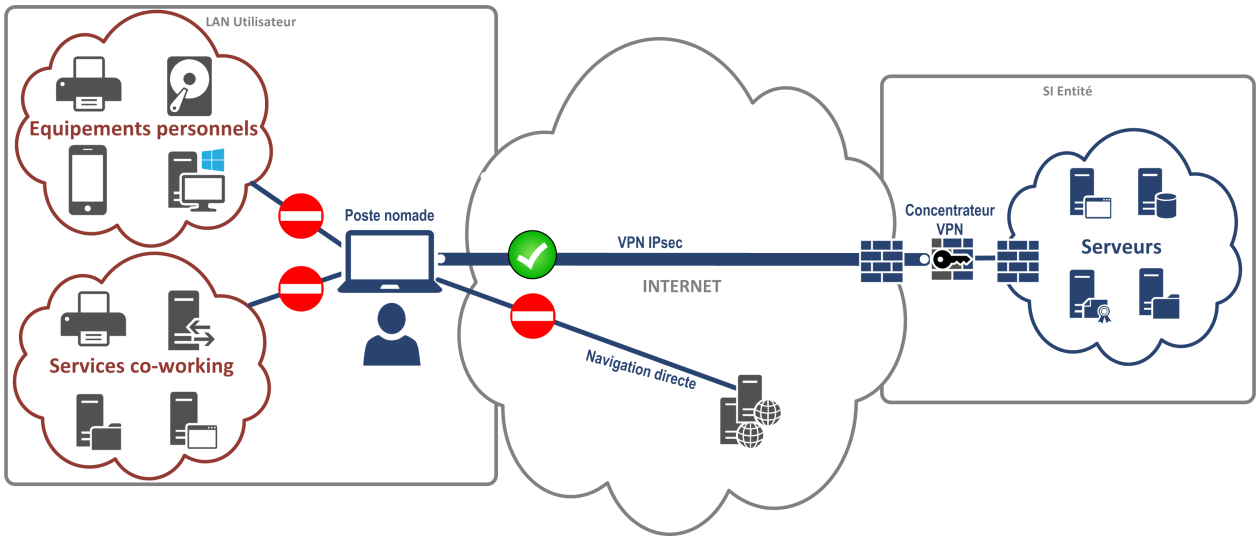

FIGURE 3.3 – Flux autorisés et interdits dans le cadre du nomadisme

Si le pare-feu local du poste de travail nomade n'est pas correctement configuré, l'équipement d'accès est en mesure de faire du *Split-Tunneling* [22], ce qui présente le risque qu'un attaquant le compromette depuis Internet et l'utilise comme rebond vers le SI de l'entité.

22. Situation d'un équipement qui dispose d'un accès simultané à deux réseaux d'un niveau de sensibilité différent. Cela signifie ici un accès au réseau de l'entité et également au réseau local de l'utilisateur nomade. L'expression *Split-Tunneling* indique que seuls les flux à destination du SI de l'entité sont routés vers le tunnel VPN. L'expression *Full-Tunneling* signifie au contraire que tous les flux sont routés vers le tunnel VPN.

De plus, cela accroît le risque d'exfiltration de données en provenance du SI de l'entité vers Internet, en passant par la connexion réseau locale de l'utilisateur, laquelle n'est pas sécurisée par des équipements de filtrage (pare-feu, *proxy*, etc.).

Ainsi, tel que décrit précédemment, il est recommandé de bloquer tous les flux sur le poste de travail, à l'exception des flux nécessaires à l'établissement du tunnel VPN.

Action	Sens	IP Source	Port Source	IP Destination	Port Destination	Type	Commentaire
Accepter	Entrant	Tous	67	Tous	68	UDP	DHCP
Accepter	Sortant	Tous	67	Tous	68	UDP	DHCP
Accepter	Sortant	IP_CLIENT_LAN	500, 4500	IP_VPN_IPSEC	500, 4500	UDP	Connexion VPN
Refuser	Tous	Tous	Tous	Tous	Tous	Tous	Règle par défaut

TABLE 3.1 – Exemple de configuration du pare-feu local

Dans cet exemple de configuration, les seuls flux autorisés sur l'interface réseau LAN du poste de travail nomade sont les flux DHCP permettant de recevoir la configuration réseau, ainsi que le flux permettant la connexion au concentrateur VPN IPsec sur Internet. Selon le contexte de l'entité, il peut être nécessaire de rajouter d'autres flux autorisés comme l'accès à un service DNS par exemple.

R18

Bloquer le split-tunneling sur l'équipement d'accès nomade et n'autoriser que les flux nécessaires pour monter le tunnel VPN

Une fois le tunnel monté entre l'équipement d'accès et le SI de l'entité, tous les flux doivent être acheminés uniquement vers le SI de l'entité.
Le *split-tunneling* doit être proscrit sur l'équipement d'accès de l'utilisateur nomade.

Dans la liste des flux autorisés hors VPN, se pose la question du protocole DNS, et en particulier la résolution du nom public lié au concentrateur VPN sur lequel le poste nomade se connecte.

Il est recommandé de ne pas ouvrir de flux DNS, pour la résolution de nom de l'équipement de terminaison VPN. En effet, l'autorisation de ce flux supplémentaire pourrait permettre à un attaquant de se faire passer pour le serveur cible (par une attaque de type empoisonnement du cache DNS [23]) ou bien d'exfiltrer des données du poste par une attaque dite *DNS Tunneling*, en les faisant transiter par ce protocole ouvert sur Internet.

Cependant, pour des raisons de maintenance et de flexibilité dans l'architecture nomade, il peut être compliqué de mettre à jour les adresses IP des concentrateurs VPN sur les clients VPN nomades, en cas de changement dans le SI interne de l'entité.

Plusieurs solutions sont possibles pour sécuriser le flux DNS si celui-ci est nécessaire à l'établissement du tunnel VPN. Un descriptif de ces solutions se trouve en annexe C.

23. Appelée aussi *DNS Cache Poisening*.

R19

Bloquer les flux DNS vers Internet et configurer directement les adresses IP publiques des concentrateurs VPN sur le client

Si la configuration le permet, il est recommandé de configurer plusieurs adresses IP pour les concentrateurs VPN, afin de gérer plus facilement un changement de configuration d'adressage public ou privé (dans le cas d'un concentrateur interne).

R19 -

Sécuriser et maîtriser les flux DNS pour la résolution du nom du concentrateur VPN

Si l'utilisation de DNS est nécessaire, il est conseillé de restreindre au maximum l'usage de la résolution DNS directement sur Internet, en installant un service DNS maîtrisé par l'entité. Les flux DNS peuvent être sécurisés par l'ajout d'une fonction d'authentification et de contrôle d'intégrité, entre le client et le serveur de l'entité.

3.4.4 Cas du portail captif

Le filtrage réalisé par le pare-feu local au poste peut poser des problèmes dans le cas particulier d'un utilisateur voulant s'authentifier sur un portail captif, par exemple dans un hôtel. Dans ce cas, la restriction d'accès aux services VPN de l'entité fait que le poste ne peut pas se connecter vers l'extérieur, puisque les requêtes *http* et *https* sur les ports 80 et 443 sont bloquées.

Cependant, il est très risqué d'ouvrir des ports dans ce cas particulier, puisqu'un filtrage strict ne peut être mis en œuvre sur les adresses cibles des portails captifs. Un accès direct (sans filtrage et sans *proxy*) à un portail captif suppose donc d'ouvrir un accès global vers Internet, ce qui, pour rappel, présente un risque fort de compromission du poste d'accès. La recommandation sur le filtrage strict des flux sur le poste nomade doit donc s'appliquer et tout accès à un portail captif doit être bloqué sur le pare-feu de l'équipement.

Une solution alternative est d'utiliser un équipement de routage non sensible (matériel professionnel dédié à cet usage), qui réalise la connexion au portail captif, et qui fait ensuite office de routeur pour l'équipement d'accès professionnel. Cet équipement de routage ne doit en aucun cas avoir la possibilité de se connecter au SI interne de l'entité. Son rôle doit se limiter à un rôle de routeur uniquement.

Toutefois cette solution est utile, uniquement dans le cas où l'utilisateur n'a d'autre choix que d'utiliser la connexion au portail captif pour se connecter à Internet. Dans le cas où l'utilisateur dispose, en plus de son équipement d'accès, d'un second équipement *routeur* avec son propre accès à Internet (via un réseau 3G / 4G) alors il est recommandé d'utiliser ce moyen de connexion, pour éviter d'avoir à passer par le portail captif non maîtrisé.

De manière générale, l'intérêt et le but de la mise en place d'un tunnel VPN IPsec (ou TLS) est d'assurer un niveau de sécurité bien défini, pour les communications vers le SI de l'entité, tout en faisant abstraction du niveau de sécurité déjà existant sur la couche de transport du réseau d'accès à Internet.

La figure 3.4 résume les flux autorisés et interdits dans le cas d'un accès via portail captif :

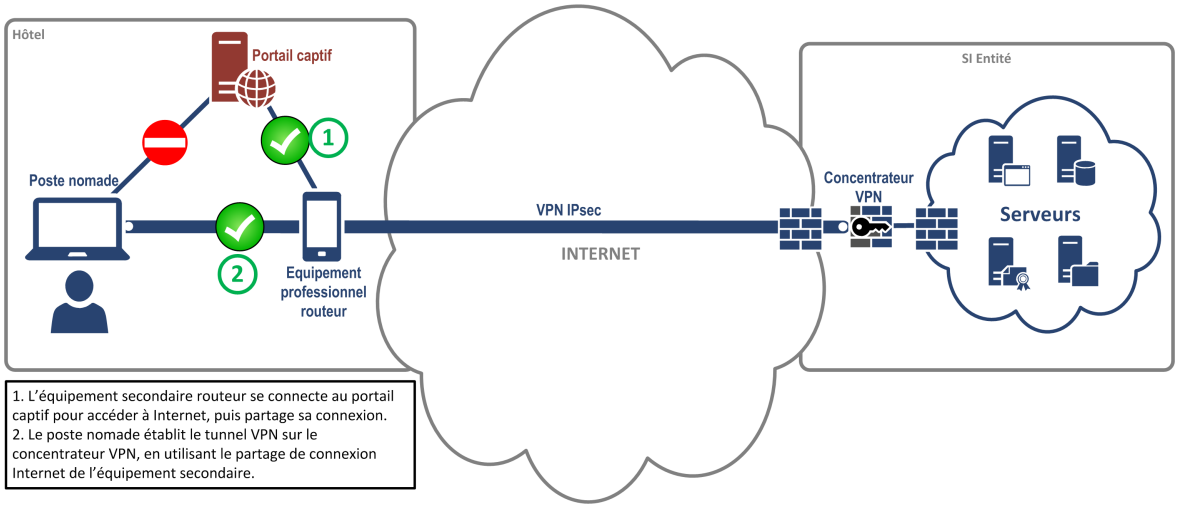

FIGURE 3.4 – Connexion VPN à travers un réseau disposant d'un portail captif

3.4.5 Détection de posture

Dans le cas où l'équipement d'accès est le même en interne et à l'extérieur de l'entité, il est indispensable de mettre en place un dispositif permettant d'apporter le même niveau de sécurité quel que soit l'environnement d'utilisation.

Les mécanismes de détection de posture ou de détection d'environnement, liés à la configuration du client VPN ne semblent pas, à la date de rédaction de ce guide, apporter un niveau de sécurité suffisant.

Ceux-ci reposent généralement sur des tests de requêtes de résolution de noms DNS internes, d'interrogations de services Web ou encore de requêtes *LDAP*, à destination du contrôleur de domaine *Active Directory* (AD) dans le cas des environnements Windows.

Certains tests peuvent être considérés comme fiables, dans le sens où ils font appel à des protocoles disposant d'une fonction d'authentification des services internes interrogés (par une vérification de certificat dans le cas d'utilisation du protocole *https* par exemple).

Ces contrôles reposent néanmoins sur la bonne configuration des outils par les administrateurs, et pourraient être contournés si les contrôles sont trop simples ou ne requièrent pas d'authentification (par exemple dans le cas d'une requête vers un serveur DNS interne). De plus, les requêtes de contrôle envoyées depuis l'équipement d'accès à l'extérieur peuvent permettre à un attaquant de recueillir des informations sur l'environnement interne de l'entité (noms de serveurs, cartographie réseau, etc.).

Enfin, le comportement des fonctions de détection d'environnement doit impérativement être testé et éprouvé dans le cas d'un changement de configuration réseau (déconnexion temporaire, perte de signal Wi-Fi, passage d'un mode filaire en Wi-Fi, etc.), pour s'assurer que l'outil répond correctement, et dans un délai le plus court possible.

Pour ne pas avoir à dépendre de la fiabilité d'un outil de détection de posture, la préconisation est de mettre en place un concentrateur VPN interne, pour le cas où l'utilisateur se connecte à partir du SI interne de l'entité, depuis son équipement d'accès nomade. Ainsi le client VPN sera configuré pour établir une connexion sur le premier des deux concentrateurs (externe ou interne), joignable depuis le réseau de l'utilisateur nomade.

La recommandation est d'avoir deux concentrateurs VPN distincts pour l'accès externe et interne, car la sensibilité et l'exposition de ces concentrateurs ne sont pas les mêmes dans les deux cas.

L'avantage de cette solution est qu'elle permet de ne pas avoir à gérer les risques liées à un SI interne qui serait trop ouvert par conception. En effet, le concentrateur VPN interne offre une fonction de filtrage et d'authentification supplémentaire avant l'accès au SI interne, ce qui n'est pas forcément le cas sur le réseau local des postes fixes de l'entité.

La solution apporte également une simplification de la configuration du poste d'accès et des règles de pare-feu sur celui-ci, puisque celles-ci seront sensiblement les mêmes quel que soit l'environnement de l'utilisateur. Si besoin, cette solution permet également de paramétrer un filtrage différent sur chacun des deux concentrateurs VPN de l'entité, s'il est nécessaire d'ouvrir plus de services en interne qu'en situation nomade.

L'inconvénient de cette solution peut être une baisse des performances réseau (en fonction du débit des différents liens traversés), et une latence plus élevée (en fonction du nombre de nœuds et d'équipements de filtrage traversés) dans le cas où le concentrateur VPN interne ne serait pas assez « *proche* » de l'utilisateur, puisque tous les flux réseaux doivent transiter par celui-ci.

Le coût d'investissement du matériel doit également être pris en compte dans cette solution, dans le cas où l'entité est répartie géographiquement sur un nombre important de sites.

La figure 3.5 illustre le concept de mise en place de deux concentrateurs VPN distincts :

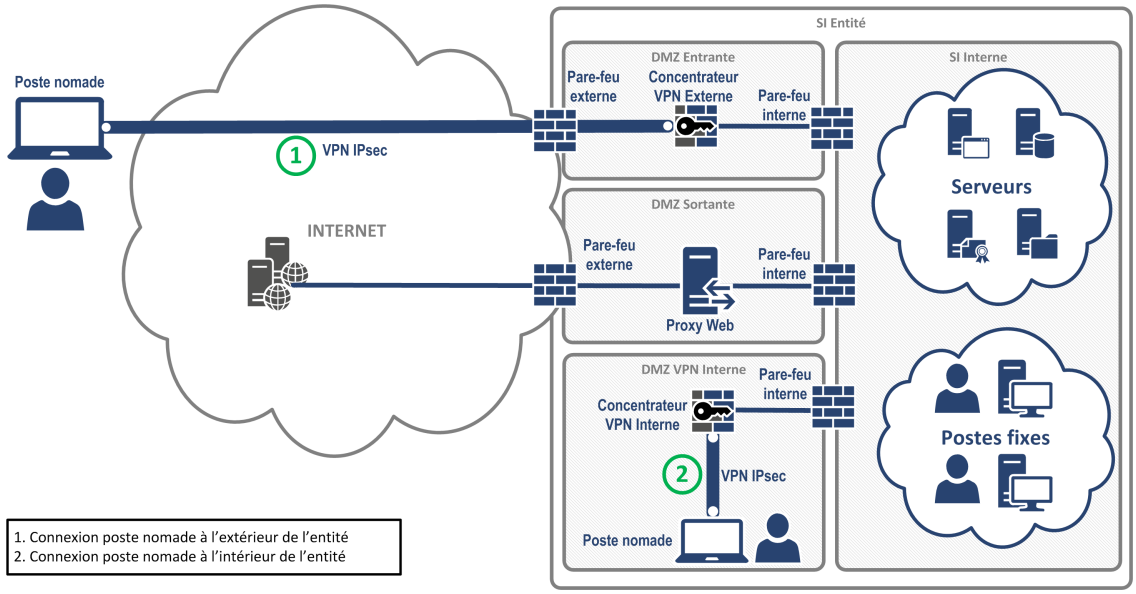

FIGURE 3.5 – Connexion VPN en interne et à l'extérieur du SI de l'entité à partir d'un équipement d'accès nomade

R20

Mettre en place un concentrateur VPN interne et forcer l'établissement du tunnel VPN quel que soit l'environnement de l'utilisateur

La mise en place de concentrateurs VPN internes permet de rationaliser et de simplifier la configuration réseau du SI nomadisme, et apporte une protection supplémentaire dans le cas des connexions des utilisateurs nomades en interne de l'entité.

Dans le cas d'une entité multi-sites, la justification de la mise en place d'un concentrateur VPN interne sur un site donné dépend de plusieurs facteurs :

- le nombre de postes nomades par rapport au nombre de postes fixes ;
- la présence ou non de serveurs applicatifs locaux pour les utilisateurs du site ;
- la performance du lien réseau entre un site secondaire et le site principal.

La figure 3.6 illustre le concept de mise en place de concentrateurs VPN internes dans le cas d'une entité multi-sites :

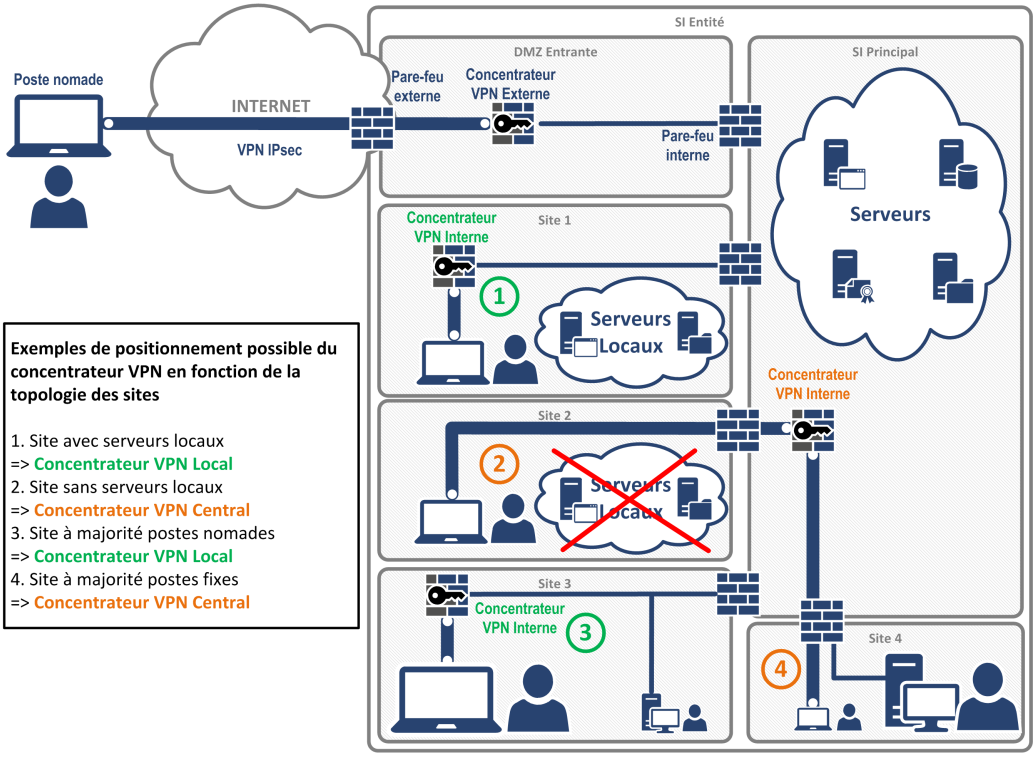

FIGURE 3.6 – Connexion VPN en interne et à l'extérieur du SI de l'entité dans le cas d'un multi-sites

Dans le cas où il n'est pas possible de mettre en place un concentrateur VPN interne, alors il est possible d'utiliser un mécanisme de détection de posture. Il faut faire attention à ne pas mettre en œuvre un mécanisme trop simple qui pourrait être facilement contourné par un attaquant.

Ce mécanisme doit dans tous les cas être documenté, et maintenu, que ce soit un produit développé en interne ou par un éditeur.

Ce mécanisme ne doit pas pouvoir être stoppé, débrayé ou modifié par l'utilisateur. S'il s'agit d'un service Windows ou d'un processus lancé au démarrage de la session, il faut s'assurer que celui-ci ne peut pas être stoppé par l'utilisateur nomade.

Le mécanisme doit être lancé le plus tôt possible dans la séquence de démarrage du poste, c'est-à-dire idéalement dès que la connexion de la carte réseau est établie. L'outil doit être capable de détecter un changement d'environnement réseau et d'adapter son comportement en fonction du nouvel environnement.

Il n'existe pas, à la date de rédaction de ce guide, de produit de détection de posture ou de client VPN intégrant cette fonctionnalité et disposant d'un visa de sécurité de l'ANSSI.

R20 -

Mettre en place un mécanisme de détection de l'environnement de l'utilisateur nomade

Si l'utilisation d'un mécanisme de détection de posture est nécessaire, l'outil retenu doit au minimum respecter les principes suivants :

- les contrôles de détection de posture doivent être fiables, et ces contrôles doivent intégrer une fonction d'authentification dans les requêtes effectuées ;
- l'outil ne doit pas être débrayable par l'utilisateur ;
- l'outil doit permettre une journalisation de son utilisation ;
- l'utilisation de l'outil doit être documentée.

3.5 Authentifications

3.5.1 Principes généraux

L'objectif des authentifications dans le cadre du nomadisme est de s'assurer d'une part que l'utilisateur nomade est bien connecté sur un poste maîtrisé par l'entité, et d'autre part de vérifier l'identité et les droits d'accès de l'utilisateur avant sa connexion au SI interne de l'entité.

Dans le cadre d'une connexion au SI de l'entité, plusieurs authentifications sont donc requises. En premier lieu l'utilisateur doit être authentifié sur son équipement d'accès au démarrage de celui-ci. Ensuite, l'équipement d'accès et l'utilisateur nomade doivent s'authentifier sur le SI de l'entité.

L'authentification de l'utilisateur sur l'équipement d'accès permet de s'assurer qu'en cas de vol ou de perte, une personne malveillante ne peut pas accéder facilement aux données présentes sur le poste. Cette authentification peut se faire de diverses manières, par exemple avec :

- le mot de passe de déchiffrement du disque dur au démarrage du poste ;
- le mot de passe d'un compte utilisateur local au poste ;
- le mot de passe du compte utilisateur lié à un annuaire central, et dont le contrôle est effectué par la présence d'un cache d'empreinte des mots de passe en local ;
- une carte à puce et un code *PIN* (authentification double facteur).

Dans tous les cas, les éléments secrets doivent être personnels, et seul l'utilisateur du poste de travail doit avoir la connaissance ou la possession de ceux-ci.

L'authentification de l'équipement d'accès sur le SI nomadisme permet de s'assurer que l'utilisateur se connecte bien depuis un poste maîtrisé par l'entité, et non pas depuis un poste personnel par exemple (*BYOD*). L'authentification du poste sur le SI nomadisme se fait généralement par l'installation d'un certificat machine sur le poste. Ce certificat n'est donc pas lié à l'utilisateur du poste, et les éléments secrets de ce certificat (clé privée) doivent être stockés de manière sécurisée et ne doivent pas être accessibles à l'utilisateur nomade. Si les éléments secrets sont stockés sur le disque, le disque doit être chiffré, pour se prémunir du risque de récupération à froid de ces éléments secrets par un attaquant.

L'authentification de l'utilisateur sur le SI de l'entité permet de contrôler l'identité de l'utilisateur et de vérifier ses droits d'accès. Cette authentification peut se faire de différentes façons ; le sujet est d'ailleurs détaillé avec des exemples concrets en annexe D.

R21

Authentifier l'utilisateur et l'équipement d'accès dans le processus de connexion au SI nomadisme

Le processus d'authentification au SI nomadisme doit inclure les trois étapes suivantes :

- authentification de l'utilisateur sur l'équipement d'accès ;
- authentification de l'équipement d'accès sur le SI nomadisme ;
- authentification de l'utilisateur sur le SI nomadisme.

Un attaquant est susceptible d'usurper l'identité d'un utilisateur nomade si le processus d'authentification de celui-ci n'est pas suffisament robuste, ou si les secrets d'authentification ne respectent pas l'état de l'art de la sécurité, conformément au référentiel général de sécurité [19].

Il est donc impératif, pour l'authentification de l'utilisateur nomade, de mettre en œuvre une authentification double facteur, reposant sur deux secrets parmi les suivants :

- ce que je sais (mot de passe) ;
- ce que je possède (carte à puce) ;
- ce que je suis (biométrie).

Attention

L'usage de la biométrie est à traiter avec précaution. À la différence des autres facteurs connus ou détenus par l'utilisateur, les facteurs biométriques ne peuvent pas être protégés en confidentialité. Il est ainsi très facile pour un attaquant d'obtenir les empreintes d'un individu et de chercher à forger une copie acceptable par le système authentifiant.
Si une telle attaque est détectée, il est impossible, à la différence d'un certificat ou d'un mot de passe, de révoquer l'accès en attendant une mise à jour corrigeant la vulnérabilité. En effet, cela reviendrait à révoquer également l'accès de l'utilisateur légitime car il n'est pas possible de changer ses facteurs biométriques.
Il est donc recommandé d'utiliser les deux facteurs *ce que je sais* et *ce que je possède* dans le cadre d'une authentification double facteur. L'utilisation de la biométrie seule est à proscrire.

Les moyens les plus répandus pour réaliser une authentification double facteur d'un utilisateur sont :

- l'usage d'une carte à puce (disposant d'un crypto-processeur) et d'un code *PIN* d'authentification ;
- l'usage d'un code temporaire *OTP*[24] envoyé à la demande sur un équipement professionnel différent de celui réalisant l'authentification (le mobile multifonction professionnel de l'utilisateur dans le cas d'une authentification sur ordinateur portable par exemple).

Cette authentification à double facteur peut avoir lieu lors de la première phase d'authentification au démarrage du poste ou lorsque l'utilisateur souhaite accéder au SI nomadisme, ou bien lors des deux phases.

R22

Mettre en place une authentification double facteur de l'utilisateur nomade

Il est primordial de mettre en place une authentification à double facteur pour l'utilisateur nomade. Ceci peut se faire par exemple avec une carte à puce et un code *PIN*, ou bien un mécanisme de type OTP.

3.5.2 Architecture d'authentification

Plusieurs architectures de SI nomadisme sont possibles pour gérer le processus d'authentification en situation de nomadisme. Il est envisageable de faire reposer la majorité des authentifications sur le concentrateur VPN, dans le cas où ces authentifications sont jugées suffisamment robustes, ou si l'on estime que les authentifications applicatives au sein du SI interne (applications métiers, serveurs, domaine *Active Directory*, etc.) apportent un niveau de sécurité suffisant au regard de l'analyse de risques.

Cependant, dans certains cas, il est pertinent de rajouter un élément de sécurité supplémentaire, par la mise en œuvre d'un serveur d'authentification dédié, positionné en coupure entre le concentrateur VPN et le SI interne. L'intérêt de ce serveur est d'apporter une défense en profondeur

24. *One time password* : mécanisme de mot de passe à usage unique pour un utilisateur, qui est désactivé une fois celui-ci utilisé.

sur le SI nomadisme, et de pallier une authentification qui ne serait pas jugée assez robuste sur le concentrateur VPN. En effet, dans le cas où un attaquant réussit à compromettre l'accès au concentrateur VPN, il lui faut également compromettre le serveur d'authentification avant de pouvoir accéder au SI interne de l'entité.

Ce serveur d'authentification peut être un portail Web d'authentification, comme le proposent les solutions *Windows Terminal Services* ou *Citrix XenApp / XenDesktop* par exemple. Il peut également être directement une machine de rebond accessible par les protocoles de déport d'affichage standard comme *RDP* [25].

Les deux possibilités d'architecture d'authentification sont à étudier en fonction de l'analyse de risques liée au SI nomadisme.

Comme cela a été vu précédemment, le processus d'authentification au SI nomadisme doit pouvoir authentifier :

- l'utilisateur sur l'équipement d'accès ;
- l'équipement d'accès sur le SI nomadisme ;
- l'utilisateur sur le SI nomadisme.

Il est donc primordial, d'une part que ces trois étapes soient présentes dans l'architecture d'authentification retenue, et d'autre part qu'il y ait au moins une des authentifications de l'utilisateur qui soit une authentification double facteur.

Des exemples concrets d'architectures d'authentification sont détaillés dans l'annexe D, afin de permettre une meilleure compréhension de ces principes.

3.5.3 Infrastructure de gestion de clés

Il est préférable dans la mise en œuvre des solutions IPsec ou TLS d'utiliser des certificats, et donc d'utiliser une IGC [26] pour la gestion de ceux-ci.

Ces certificats sont utilisés pour réaliser l'authentification mutuelle de l'équipement d'accès (certificat machine) et de l'équipement de terminaison VPN, ainsi que le chiffrement des flux au sein du tunnel VPN.

L'autorité de certification du SI nomadisme doit être dédiée à cet usage. Elle est ainsi isolée des autres autorités de certification en cas de compromission. Elle peut être indépendante des autres IGC de l'entité ou bien être liée à une IGC racine de l'entité. Dans ce dernier cas, l'autorité de certification du SI nomadisme doit être une autorité intermédiaire (ou subordonnée) dédiée.

La gestion des certificats est primordiale et doit faire l'objet de procédures et de règles de gestion strictes au sein du SI de l'entité (circuit de validation lors de la demande de certificats, gestion fine des droits d'administrateurs, durée de validité adéquate, définition et restrictions d'usage des certificats, utilisation d'extensions, etc.).

25. *Remote Desktop Protocol.*
26. Infrastructure de gestion de clés.

Les recommandations suivantes permettent de faire un rappel sur les bonnes pratiques liées à la gestion de certificats.

R23

Protéger les éléments secrets liés aux certificats nomades

Il faut vérifier que le stockage des clés privées est sécurisé.
Pour la partie cliente, cela peut se faire en stockant les éléments secrets sur une carte à puce sécurisée, équipée d'un crypto-processeur.
Pour l'équipement de terminaison VPN, il est recommandé d'utiliser des équipements de type *HSM* (*Hardware security module.*), dédiés à cet usage.

Les autorités de certification configurées et autorisées par défaut sur le poste d'accès, doivent être revues et adaptées au strict nécessaire pour la connexion au SI nomadisme.

Il faut être vigilant si la solution VPN utilise le magasin de certificats Windows pour gérer les autorités de certification de confiance. Dans ce cas, il faut étudier quels sont les impacts en cas de suppression définitive de certaines autorités sur le poste de travail nomade. Il est possible de configurer le magasin des équipements d'accès avec des *GPO* sur le domaine *AD* pour restreindre la liste des autorités de certification valides sur un poste Windows.

De manière générale, il est fortement recommandé de choisir des logiciels permettant une configuration stricte des autorités de certification autorisées, et qui ne reposent pas sur le magasin du système d'exploitation. Dans une situation standard, seule une autorité de certification doit être définie et configurée pour l'accès au SI nomadisme.

R24

Configurer strictement l'autorité de certification légitime sur les équipements de nomadisme

Il faut ne faire confiance qu'à l'autorité de certification légitime pour monter le tunnel VPN entre l'équipement d'accès et le SI de l'entité.

3.5.4 Vérification de la validité des certificats

Les certificats peuvent être révoqués parce que l'équipement a été compromis ou volé, ou bien leur durée de validité peut être dépassée.

Dans le cas d'une connexion VPN, la vérification de la validité des certificats, de la part du client comme du serveur doit impérativement être effectuée. Il convient de contrôler, outre la validité de la chaîne de certification, l'identité (*Subject Name*) et les restrictions d'usage (*Key usage extensions*) du certificat. Le fait que le certificat soit signé par une IGC valide est nécessaire mais n'est pas suffisant pour considérer celui-ci comme légitime pour l'établissement du tunnel VPN.

Il est important que la vérification ne soit pas juste à titre indicatif, lors de l'établissement de la connexion VPN, mais bien que celle-ci déclenche une interruption de la connexion si le certificat est invalide.

Le contrôle de la validité en cas de révocation, peut être réalisé par les moyens suivants :

- par le téléchargement périodique d'un fichier *CRL* [27] qui contient la liste des numéros de série des certificats révoqués et leur date de révocation. Ce fichier est signé par l'autorité de certification à chaque fois qu'il est mis à jour ;
- par un service Web *OCSP* [28] mis à disposition sur un élément de la plateforme de l'autorité de certification ;
- par un mécanisme dit d'agrafage *OCSP* (ou *OCSP Stapling*), permettant au concentrateur VPN de fournir directement une preuve horodatée et authentifiée de la validité de son certificat, sans que le client n'ait à requêter directement le service de l'autorité de certification. Cette vérification fait partie de la négociation qui a lieu pendant l'établissement de la connexion VPN.

La récupération de l'information de validité des certificats ne pose généralement pas de problème sur le concentrateur VPN, puisque celui-ci se situe généralement dans le même SI que les services de distribution *CRL* ou *OCSP*.

Cependant, concernant le poste d'accès, il est aussi important que celui-ci vérifie la validité du certificat du concentrateur VPN, et ce, même si l'on considère qu'un concentrateur VPN ayant été détecté comme compromis, devrait être en théorie coupé ou déconnecté du réseau de l'entité. En effet, le vol de la clé privée liée au concentrateur VPN pourrait permettre à un attaquant de la réutiliser et se faire passer pour un équipement de terminaison VPN légitime pour un utilisateur nomade. Cette attaque n'est pas triviale car elle nécessite également de pouvoir être en mesure d'usurper l'adresse IP publique ou le nom DNS du concentrateur VPN de l'entité.

Les deux premiers moyens de vérification de la validité d'un certificat de concentrateur VPN nécessitent d'ouvrir un flux supplémentaire sur le poste d'accès, avant que celui-ci ne se connecte au serveur VPN, pour requêter le serveur *OCSP*, ou pour télécharger le fichier *CRL* à jour. Cette règle supplémentaire d'accès sur le pare-feu augmente la surface d'attaque, car ce flux ne peut pas être considéré d'un même niveau de sécurité qu'un flux transitant au sein du tunnel VPN établi. Ainsi, il est recommandé d'utiliser préférentiellement le mécanisme d'agrafage *OCSP*, si les logiciels client et concentrateurs VPN supportent cette fonctionnalité.

R25

Vérifier la validité des certificats client et concentrateur VPN par le mécanisme d'agrafage OCSP

Cette vérification doit se faire avant que l'établissement de la connexion VPN ne soit complète. Cette fonction doit faire partie de l'analyse de risques à mener sur le SI nomadisme.

27. *Certificate revocation list.*
28. *Online certificate status protocol.*

La figure 3.7 présente les recommandations d'usage pour le contrôle de la validité des certificats des concentrateurs VPN :

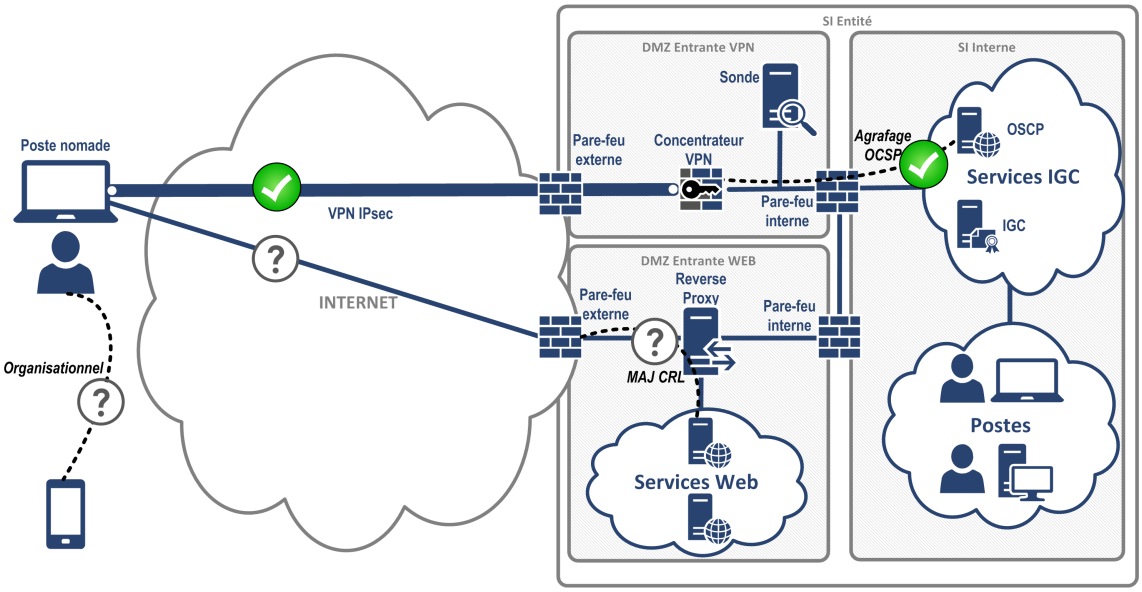

FIGURE 3.7 – Vérification de la validité des certificats des concentrateurs VPN

Dans le cas où la fonctionnalité d'agrafage OCSP n'est pas supportée, il faut mener une analyse de risques pour décider quelle mesure compensatoire est la meilleure afin de répondre au risque de compromission du concentrateur VPN :

1. mettre en place une mesure organisationnelle pour prévenir les utilisateurs nomades de ne pas se connecter au concentrateur VPN qui serait compromis ;
2. ouvrir un flux spécifique sur le pare-feu local pour vérifier et télécharger la dernière version du fichier CRL (connexion Web directe sur Internet) ;
3. déployer des certificats à durée de vie très courte pour le concentrateur VPN, et les renouveler régulièrement.

R25 - **Vérifier la validité des certificats concentrateurs VPN par l'ouverture d'un flux direct sur le poste client ou par une mesure organisationnelle**

Si l'agrafage OCSP n'est pas la solution retenue, il est recommandé de mener une analyse de risques pour choisir la meilleure alternative dans ce cas précis.

3.6 Passerelle d'interconnexion

3.6.1 DMZ entrante du SI nomadisme

La DMZ entrante est composée généralement :

- d'un pare-feu externe connecté en frontal sur Internet ;
- d'un équipement de terminaison VPN ;

- d'un annuaire répliqué pour l'authentification des utilisateurs ;
- d'un pare-feu interne protégeant le SI de l'entité.

Cette DMZ peut également être composée d'un serveur d'authentification dédié aux utilisateurs nomades, comme cela est détaillé dans la section D.

La DMZ entrante peut éventuellement contenir d'autres services d'infrastructure comme un collecteur de journaux ou bien un serveur DNS si nécessaire. Le choix de cette architecture est à définir en fonction du contexte de l'entité, et de l'analyse de risques liée à la mise en place du SI nomadisme. Cette analyse de risques repose sur la confiance que l'on accorde aux postes utilisateurs nomades et sur le niveau de sécurité mis en place sur ceux-ci.

Dans le cas où la confiance sur les équipements d'accès nomades est limitée, il est alors recommandé de positionner certains services d'infrastructure (DNS...) dans une DMZ cloisonnée, afin de limiter l'impact d'une compromission de l'un de ces services vers le SI interne de l'entité.

La figure 3.8 présente un schéma global de la DMZ entrante VPN :

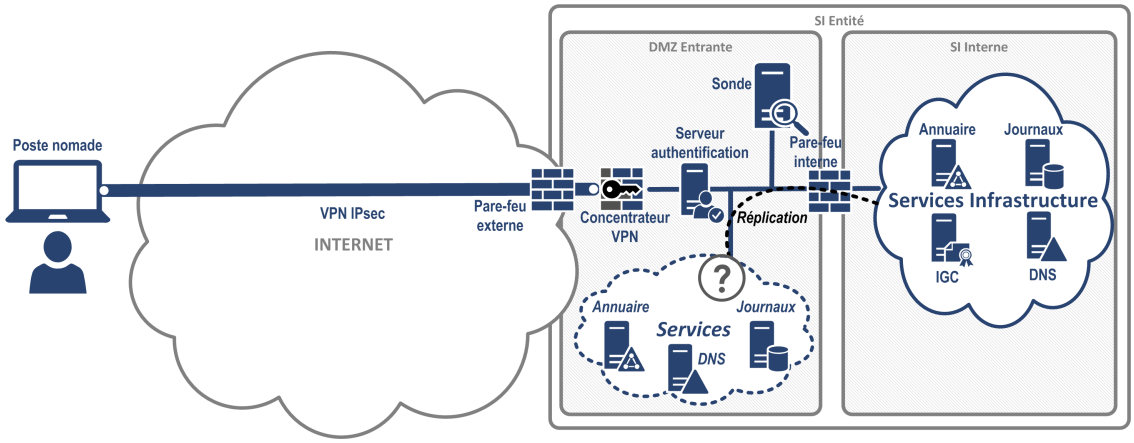

FIGURE 3.8 – Schéma global de la DMZ entrante VPN

Il est possible de consulter à ce sujet les recommandations pour mettre en œuvre des passerelles Internet sécurisées [18].

Il est recommandé que les équipements de cette DMZ entrante soient physiquement dédiés à la connexion des utilisateurs nomades. Le fait de mutualiser cette infrastructure avec d'autres services de connexion à distance (liens vers les partenaires, télémaintenance, etc.) présente un risque de débordement latéral en cas de compromission d'une des parties.

R26

Mettre en place des équipements physiquement dédiés au SI nomadisme dans la DMZ entrante

Il est recommandé de dédier le matériel nécessaire à la connexion des utilisateurs nomades, au sein de la DMZ entrante.

Cependant, s'il n'est pas possible de dédier physiquement les équipements de la DMZ entrante au SI nomadisme, alors il est obligatoire de mettre en place un cloisonnement logique, par exemple au moyen :

- de *VLAN*[29] et *VRF*[30] pour la partie réseau ;
- d'instances virtuelles de pare-feu (à titre d'exemple appelés *contexte* pour les équipements Cisco ou *VDOM* pour Fortinet) ;
- de virtualisation de serveurs (voir le guide de l'ANSSI relatif à *VMWare ESXi* [5] par exemple).

Dans le cas où il n'est pas possible de dédier physiquement les équipements de la DMZ entrante pour le SI nomadisme, alors il peut être acceptable, en fonction de l'analyse de risques, de mutualiser certains éléments présents dans cette DMZ entrante, comme par exemple :

- la mutualisation du pare-feu externe avec d'autres fonctions que celle liée au SI nomadisme ;
- la mutualisation du pare-feu interne avec d'autres fonctions que celle liée au SI nomadisme.

Il est toutefois très fortement recommandé de ne pas mutualiser la fonction de concentrateur VPN avec d'autres SI de l'entité (comme par exemple, les accès VPN site-à-site). La recommandation est également identique dans le cas de l'utilisation d'un serveur d'authentification pour les utilisateurs nomades. Celui-ci ne doit en aucun cas être mutualisé avec d'autres accès distants (par exemple l'authentification des administrateurs ou des opérateurs de télémaintenance).

R26 -

Mettre en place un cloisonnement logique pour le SI nomadisme dans la DMZ entrante

A défaut d'une infrastructure physique dédiée, il est primordial de cloisonner logiquement l'infrastructure de nomadisme du reste du SI de l'entité, par des fonctions de virtualisation , mais également par du chiffrement et du contrôle d'intégrité des flux.

3.6.2 Flux réseau entre postes nomades

Un attaquant ayant pris le contrôle d'un des équipements d'accès est susceptible de propager son attaque vers d'autres équipements nomades (propagation latérale), le but étant généralement de réussir à acquérir des privilèges supplémentaires sur le SI de l'entité.

R27

Interdire tous les flux de communication directs entre les équipements d'accès nomades

Il est fortement recommandé de configurer l'équipement de terminaison VPN de façon à ce que la communication entre les équipements au sein du même sous-réseau soit interdite. Toute connexion depuis l'équipement d'accès doit passer impérativement par la DMZ entrante.

29. *Virtual LAN* : réseau local virtuel, également appelé réseau de commutation logique.
30. *Virtual routing and forwarding* : ce mécanisme permet de créer plusieurs instances de table de routage sur un même routeur physique.

3.7 Ressources du SI de l'entité

3.7.1 Accès aux applications métiers internes

Toutes les applications métiers dédiées aux utilisateurs nomades et faisant partie du SI interne de l'entité ne doivent être accessibles qu'au sein du tunnel VPN établi entre le poste nomade et le concentrateur exposé sur Internet.

Il est très fortement recommandé de ne pas publier d'applications métiers à destination d'une population d'utilisateurs nomades, directement sur Internet.

Une application métier directement joignable depuis Internet représente un point d'entrée sur le SI interne avec une surface d'attaque importante. En effet, la fonction principale d'un service applicatif est d'accepter des requêtes. Cela ne permet généralement pas un filtrage et une protection renforcée, contrairement à la mise en place d'un concentrateur VPN en frontal, qui présente une surface d'attaque réduite et permet un rejet des requêtes correspondant à des connexions non légitimes.

Parmi les ressources métiers accédées depuis l'extérieur de l'entité, il n'est pas rare de voir la messagerie professionnelle joignable directement sur Internet, par le biais d'un portail de messagerie ou service *webmail*. Même si ce type de service répond à une demande importante des utilisateurs dans les différentes entités, il est fortement recommandé de ne pas mettre en place de messagerie professionnelle accessible directement depuis Internet. En effet, un accès d'utilisateur nomade à un service métier joignable directement sur Internet revient à autoriser la connexion d'équipements personnels au SI de l'entité (*BYOD*). Il suffit que l'équipement soit compromis (par exemple en exploitant une vulnérabilité du navigateur Web) pour qu'un attaquant puisse accéder facilement à des informations confidentielles de l'entité.

De même, en utilisant un *Keylogger*[31], un attaquant peut également récupérer facilement un compte utilisateur ainsi que son mot de passe et essayer de s'en servir pour accéder au SI interne.

Les flux de messagerie professionnelle (ou *webmail*) doivent donc transiter, au même titre que toutes les applications métiers des utilisateurs nomades, par le tunnel VPN sécurisé et la DMZ entrante de l'entité.

31. Logiciel espion d'enregistrement des frappes au clavier.

La figure 3.9 illustre les recommandations d'usage pour l'accès aux services applicatifs en situation de nomadisme :

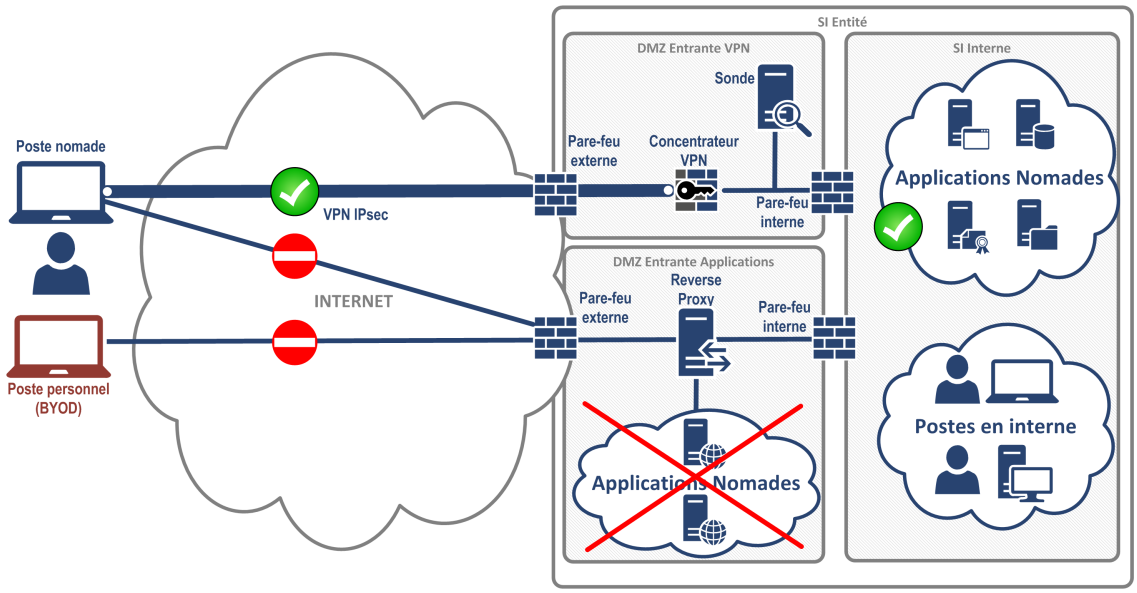

FIGURE 3.9 – Accès aux services applicatifs en situation de nomadisme

R28

Ne pas exposer d'applications métiers du SI nomadisme directement sur Internet

Il est important de conserver la maîtrise de l'information et le besoin de confidentialité en n'autorisant la connexion aux différentes applications métiers que depuis le tunnel VPN.

3.7.2 Accès aux applications métiers dans le Cloud

Dans le cas où l'entité décide de déployer des applications métiers sur une infrastructure dans le nuage (*Cloud*) public, alors la question de l'accès à ces applications métiers doit également être posée pour les utilisateurs nomades.

La recommandation est de ne pas autoriser un accès direct depuis les équipements d'accès aux ressources *Cloud* pour les utilisateurs en situation de nomadisme. Les utilisateurs nomades doivent se connecter aux services *Cloud* public en transitant par le SI de l'entité, c'est-à-dire par leur tunnel VPN.

Le SI nomadisme doit pouvoir centraliser toutes les connexions nomades, particulièrement à des fins de maîtrise des flux et de filtrage, mais également pour des besoins de traçabilité et d'analyse de journaux en cas d'incidents.

La figure 3.10 présente la recommandation d'usage pour un accès à un service *Cloud* en situation de nomadisme.

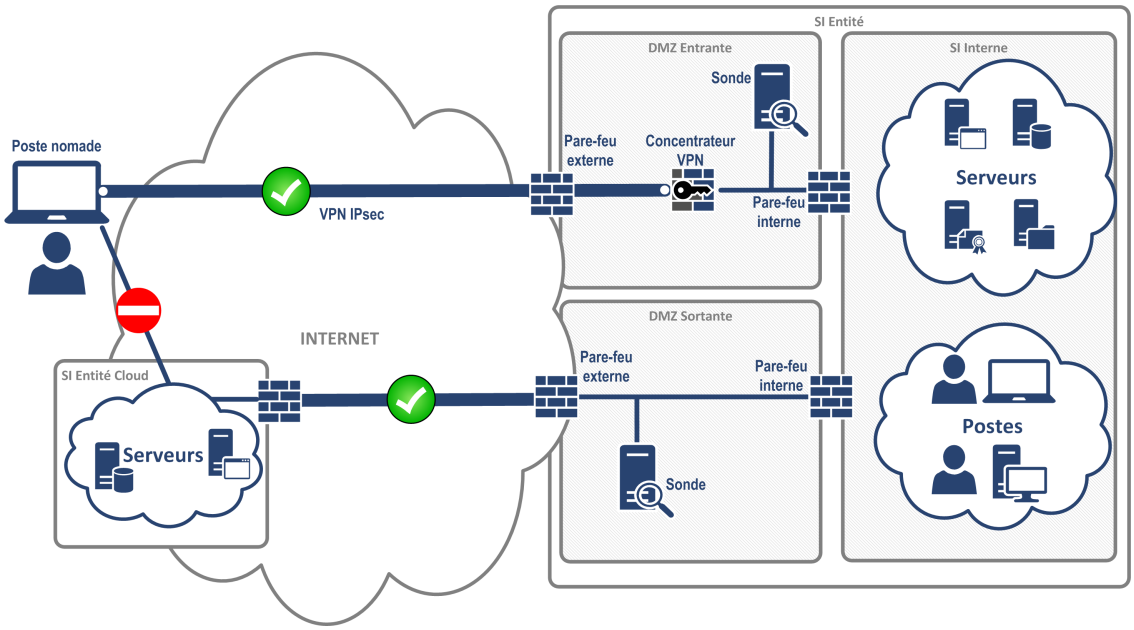

FIGURE 3.10 – Accès aux services applicatifs dans le Cloud

R29

Interdire un accès direct aux ressources présentes dans le Cloud pour les utilisateurs nomades

De même que pour les applications internes, toutes les connexions des utilisateurs nomades aux applications Cloud doivent transiter par le tunnel VPN, et uniquement par celui-ci.

3.7.3 Filtrage des applications autorisées

L'utilisateur nomade accède à des ressources situées dans le SI interne de l'entité. Un utilisateur ne doit pas pouvoir accéder à des applications internes à l'entité dont il n'a pas usage en situation de nomadisme.

R30

Réaliser un filtrage au sein du canal d'interconnexion VPN sur les applications autorisées pour un utilisateur nomade

Ce filtrage peut s'opérer sur les pare-feux liés au concentrateur VPN du SI nomadisme, mais également sur le pare-feu local du poste nomade si nécessaire.

Cette recommandation rejoint celle faite dans la partie 3.2, où il est précisé l'exigence de cartographier finement les besoins métiers d'un utilisateur nomade, au même titre que pour un utilisateur standard.

3.7.4 Protocoles utilisés

Une fois le tunnel VPN établi entre l'équipement d'accès nomade et le concentrateur VPN dans la DMZ entrante de l'entité, tous les flux de connexion nomade sont chiffrés et authentifiés par les protocoles IPsec ou TLS assurant la sécurisation du tunnel.

Cependant, dans une volonté de défense en profondeur, il est recommandé que les différentes applications métiers implémentent elles aussi des protocoles de communications sécurisées entre les postes d'accès nomades et les serveurs métiers.

Il faut ainsi veiller à ce que les flux transitant par le tunnel VPN soient également chiffrés et authentifiés. Ainsi en cas de compromission des équipements ou du canal d'interconnexion VPN, les données applicatives ne sont pas lisibles facilement par l'attaquant.

R31

Privilégier l'utilisation de protocoles chiffrés et authentifiés pour l'accès aux applications nomades au travers du tunnel VPN

Pour tous les flux transitant au travers du tunnel VPN, il est recommandé de ne pas utiliser de protocoles sans chiffrement ni authentification comme *http, ftp, telnet*, mais plutôt des protocoles sécurisés standards (*sftp, https, ssh*, etc.).
Pour le transfert de fichiers, il est conseillé d'imposer les versions sécurisées de *SMB* ou *NFS* et de désactiver les versions obsolètes présentant des vulnérabilités connues.

3.7.5 Synchronisation hors ligne

Certains outils et systèmes d'exploitation permettent de synchroniser des répertoires distants sur un serveur de fichiers, avec des répertoires locaux sur le poste de travail. Par exemple, sur un serveur Windows, il est possible d'activer la mise en cache hors ligne et la synchronisation automatique sur les répertoires partagés d'un serveur de fichiers.

Sur des environnements Linux, il est également possible d'utiliser des outils de synchronisation tels que ceux qui reposent sur *rsync* par exemple, ou bien de configurer des systèmes de cache *NFS* [32], ou bien encore de mettre en place des outils complets de partage documentaire, dédiés à la consultation hors-ligne de documents (par exemple *owncloud* ou *nextcloud*).

Ces mécanismes ne doivent être utilisés que s'ils répondent strictement à un besoin métier, car ils impliquent que l'on stocke localement sur le poste la totalité des répertoires synchronisés.

Dans le cas où l'équipement d'accès ne dispose pas d'un chiffrement de disque dur à l'état de l'art (cf. section 3.3.4), le risque d'exfiltration d'information sensible est accru, par exemple en cas de vol du matériel.

32. *Network file system.*

R32

Restreindre au strict nécessaire l'utilisation de synchronisation de documents hors ligne pour les utilisateurs nomades

Le risque de synchronisation de données entre le SI de l'entité et l'équipement d'accès est à étudier avec soin. Il faut éviter au maximum de stocker localement des informations sensibles sur le poste de travail nomade, si cela n'est pas nécessaire.

4
Recommandations d'ordre général

4.1 Produits et solutions

L'ANSSI met à disposition une liste de produits disposant d'un visa de sécurité [12], dans plusieurs domaines de la sécurité informatique. La certification ou la qualification de produits, pour une version donnée et pour une cible de sécurité donnée (ce qui ne correspond pas à la totalité des fonctionnalités de l'équipement), permet de s'assurer d'un certain niveau d'exigences du point de vue de la sécurité.

Il est recommandé de s'appuyer sur cette liste de produits certifiés ou qualifiés pendant la phase de conception du SI nomadisme. Dans le cas où certaines fonctionnalités ne seraient pas présentes sur ces produits, il faut alors mener une analyse de risques pour déterminer quel est le choix le plus pertinent entre l'usage d'un produit disposant d'un visa de sécurité mais ne répondant pas à tous les besoins, ou l'usage d'un produit standard qui répond à des besoins spécifiques.

R33

Mettre en œuvre des matériels et des logiciels disposant d'un visa de sécurité de l'ANSSI

À chaque fois que cela est possible, il est recommandé de mettre en œuvre des matériels et des logiciels disposant d'un visa de sécurité de l'ANSSI au niveau adéquat.

4.2 Administration

L'administration d'un SI est une fonction critique, pour laquelle une attention particulière est nécessaire, pendant la durée complète du cycle de vie de l'infrastructure. Dans le cadre du SI nomadisme, il est important de mettre en œuvre un SI dédié à l'administration de l'entité incluant l'administration du SI nomadisme, conformément au guide d'administration sécurisée publié par l'ANSSI [15].

R34

Respecter les recommandations du guide d'administration sécurisée de l'ANSSI pour le SI de l'entité incluant le SI nomadisme

L'administration du SI nomadisme doit avoir au moins le même niveau de sécurité que l'administration du SI de l'entité, en suivant les recommandations formulées dans le guide de l'ANSSI.

Il faut également veiller à maintenir en conditions opérationnelles et de sécurité (MCO/MCS [33]) le SI nomadisme suivant un processus formalisé, documenté et validé.

33. Maintien en condition opérationnelle / Maintien en condition de sécurité.

Pour cela, il faut réaliser régulièrement les tâches suivantes :

- faire une revue des droits et privilèges de tous les comptes utilisateurs nomades ;
- faire une revue des droits et privilèges de tous les comptes d'administration liés au nomadisme ;
- auditer régulièrement tous les équipements intervenant dans la mise en œuvre du service de nomadisme ;
- industrialiser les moyens d'administration et d'exploitation du SI nomadisme, et mettre à jour le *master* des postes nomades régulièrement ;
- se tenir informé des vulnérabilités et attaques potentielles sur les équipements composant le SI nomadisme ;
- mettre en place des procédures de résolution d'incidents pour tous les niveaux de support des utilisateurs nomades.

R35

Intégrer une politique de MCO et MCS pour le SI nomadisme

Veiller à garantir et à mettre en place au minimum un même niveau de MCO/MCS pour le SI nomadisme que celui déjà existant pour le SI interne de l'entité.

4.3 Supervision

La supervision des équipements d'accès nomade est plus difficile que la supervision des équipements en interne de l'entité, entre autres parce que :

- la localisation de ceux-ci est par nature changeante ;
- la fréquence de connexion est très variable selon les cas ;
- leur affectation aux utilisateurs peut évoluer dans le temps.

Il est donc nécessaire de disposer, au même titre que pour le SI interne, d'un outil de supervision, comme par exemple un outil *MDM* ou *EMM* [34]. Cet outil doit notamment permettre de produire des indicateurs sur les équipements d'accès nomade, comme par exemple :

- les informations techniques de l'équipement d'accès (nom de machine ou *hostname*, modèle, système d'exploitation, etc.) ;
- l'horodatage de la dernière connexion au SI ;
- les dernières applications démarrées par l'utilisateur ;
- le dernier rapport d'antivirus ;
- la version des mises à jour de sécurité critiques installées.

L'outil doit être en mesure de remonter des alertes en cas de problème sur un équipement d'accès nomade.

34. *Entreprise Mobility Management.*

R36

Prévoir une supervision de l'état du parc des équipements d'accès nomade

La supervision des équipements d'accès nomade doit permettre de réaliser un suivi régulier de la sécurité de ceux-ci. Il est très utile de disposer d'une fonction de visualisation des principaux indicateurs et alertes sur les équipements nomades.

4.4 Journalisation et analyse

La journalisation des évènements liés au SI nomadisme est une composante importante pour la détection, le suivi et la réponse aux incidents de sécurité. Il est recommandé de s'appuyer sur le guide de bonnes pratiques de la journalisation de l'ANSSI [11].

Une analyse doit être faite pour déterminer les évènements les plus pertinents à journaliser, dans le cadre de la connexion d'un utilisateur nomade.

Une protection de l'intégrité des journaux d'évènements doit être mise en œuvre, pour se prémunir du risque de modification de ces journaux par une personne non légitime.

R37

Mettre en place une journalisation des différents éléments du SI nomadisme en suivant les recommandations du guide de l'ANSSI

La journalisation doit se faire sur tous les éléments du SI nomadisme (équipement d'accès, concentrateur VPN...). Il est impératif que les journaux soient protégés en intégrité, et ne puissent pas être modifiés par l'utilisateur nomade.

Un système d'analyse et de corrélation des journaux doit être mis en place, afin de pouvoir réagir rapidement en cas d'incident de sécurité. Ce système ne peut être efficace que si tous les éléments du SI nomadisme sont horodatés sur une source de temps unique et sécurisée. Il est également nécessaire de configurer une centralisation des journaux d'évènements du SI nomadisme, dans le cadre de la mise en place de ce système. Il est important d'étudier quelle est l'architecture adéquate, pour réaliser de manière sécurisée la collecte des journaux, depuis les éléments du SI nomadisme vers les serveurs centralisés.

R38

Mettre en place un système d'analyse et de corrélation d'évènements du SI nomadisme

Un système d'analyse et de corrélation d'évènements doit être mis en place pour être en mesure de répondre aux incidents sur le SI nomadisme.

Ces différents points concernant la journalisation et l'analyse des journaux du SI nomadisme sont détaillés dans l'annexe E.

4.5 Détection

L'entité doit détecter au plus tôt une attaque en provenance de son SI nomadisme. Afin de compléter les mesures de défense en profondeur mises en place pour la connexion distante au SI de l'entité, il est recommandé de mettre en place une sonde de détection d'intrusion.

Cet équipement doit permettre de détecter un comportement anormal sur l'équipement d'accès (par exemple des requêtes réseaux malveillantes, une modification de modules systèmes, etc.) et d'alerter rapidement les administrateurs du SI nomadisme de l'entité.

R39

Mettre en œuvre une sonde de détection dans le SI nomadisme

Cette sonde doit être positionnée au sein du SI nomadisme. Il est possible de l'installer dans la zone DMZ entrante, entre le pare-feu interne et le concentrateur VPN (comme représenté sur la figure 3.2).
Le positionnement exact doit être étudié en fonction de l'architecture du SI de l'entité.

Information

De manière plus générale, le lecteur peut approfondir ce sujet en s'appuyant sur le référentiel PDIS [20].

Annexe A
Cas particulier « Diffusion Restreinte »

Une entité qui met en œuvre un SI traitant des informations « Diffusion Restreinte » (DR) doit se conformer à la réglementation applicable, c'est-à-dire à la date de rédaction de ce guide, à l'instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles (II 901) [17]. Si un service de nomadisme est mis en oeuvre sur un SI DR, ce SI DR doit satisfaire les exigences propres au service de nomadisme décrites dans l'II 901.

Cette réglementation rend notamment obligatoire l'utilisation de moyens de chiffrement agréés au niveau « Diffusion restreinte » pour protéger les informations stockées sur des supports de données (Ex. chiffrement du disque dur du poste nomade et des médias amovibles autorisés à être connectés au poste nomade). Le client logiciel VPN IPsec permettant l'établissement du lien entre le client nomade DR et le concentrateur VPN DR doit lui aussi être agréé DR.

Par ailleurs, en complément des exigences de l'II 901 portant sur le service de nomadisme, il est recommandé de considérer les bonnes pratiques décrites dans le présent guide comme des exigences complémentaires à la réglementation applicable aux SI DR [35].

R40

SI « Diffusion Restreinte » : Appliquer les bonnes pratiques du guide Nomadisme sur les SI DR

Afin d'assurer une protection à l'état de l'art d'un service de nomadisme mis en œuvre sur un SI traitant des informations de niveau DR, il est recommandé d'appliquer les bonnes pratiques du présent guide, voire de les considérer comme des exigences complémentaires à l'II 901.

35. A noter que ces bonnes pratiques pourront être amenées à être complétées par d'autres recommandations issues d'autres publications de l'ANSSI (Ex. Guide à venir de recommandations pour les architectures DR).

Annexe B
Sécurisation d'un poste partagé entre plusieurs utilisateurs nomades

Dans le cas où un poste de travail doit être partagé entre plusieurs utilisateurs nomades, plusieurs actions sont possibles pour sécuriser le poste, et réduire le risque d'accès illégitime entre les utilisateurs.

Dans un premier temps, il est recommandé de mettre en place une procédure de réinitialisation de poste (ou *remasterisation*) à chaque fois que l'attribution change. Cependant, cette mesure peut être coûteuse en temps et en ressources informatiques pour l'entité, selon la fréquence des changements d'utilisateurs.

Il est également possible d'attribuer à l'utilisateur un disque dur sécurisé, qu'il connecte au poste partagé, afin d'y déposer des documents de travail pendant son utilisation. Dans ce cas, le poste partagé ne servirait que de système d'exploitation pour l'utilisateur, et il ne doit pas être possible pour lui d'y installer des applications ou bien d'y copier des données. Une restriction des droits et privilèges est donc à faire pour la mise en œuvre de cette solution, et l'utilisateur ne doit en aucun cas disposer de droits d'administration sur son poste de travail. À titre d'exemple, cette restriction des droits peut se faire par l'application de *GPO* dans le cas d'un poste Windows.

L'utilisation de profils utilisateurs prédéfinis, avec une remise à l'état initial à chaque fois que l'utilisateur se déconnecte de son poste est également une piste de travail dans le cas de postes nomades partagés (par exemple avec les *Mandatory user profiles* sous Windows). Cette dernière solution doit cependant tenir compte de certaines contraintes pour les utilisateurs :

- un client lourd de messagerie (par exemple *Microsoft Outlook*, *Mozilla Thunderbird*) doit télécharger l'intégralité de la boîte mail à chaque nouvelle session ; aussi il est préférable d'opter pour l'utilisation d'un *Webmail* interne à travers un navigateur Web installé sur le poste dans ce cas précis ;
- l'utilisateur ne peut pas rajouter de favoris dans son navigateur si ceux-ci sont stockés dans son profil utilisateur. Il est donc nécessaire de déplacer ceux-ci dans un répertoire du disque externe attribué à l'utilisateur, ou bien de les prédéfinir pour tous les utilisateurs nomades.

Annexe C
Sécurisation des flux DNS sur l'équipement d'accès nomade

La sécurisation des flux DNS est importante dans le cas précis où l'équipement d'accès doit résoudre le nom public lié au concentrateur VPN, avant l'établissement du tunnel VPN.

L'objectif premier, si l'on choisit d'autoriser les flux DNS pour résoudre le nom du concentrateur VPN, est de pouvoir maîtriser ces flux. Il s'agit donc dans un premier temps que les clients nomades requêtent un serveur DNS maîtrisé par l'entité. Une bonne pratique consiste donc à configurer une vue DNS ou équivalent dans le SI de l'entité, et à la rendre accessible depuis Internet, pour que les clients nomades puissent exécuter des requêtes de résolution de noms sur la vue DNS.

L'adresse IP publique de la vue DNS de l'entité doit donc être configurée statiquement sur le poste de travail nomade, et la configuration ne doit pas être écrasée par les éventuels serveurs DNS qui sont renvoyés par le service DHCP local.

Une règle spécifique est donc rajoutée sur le pare-feu local de l'équipement d'accès, pour autoriser le flux sortant, sur le port DNS et à destination de l'adresse IP publique correspondant au service DNS de l'entité.

Par ailleurs, dans le cas où l'entité a la maîtrise de son serveur DNS, alors il est recommandé de sécuriser les requêtes DNS en utilisant des mécanismes comme *DNSSEC*, *DNSCrypt* ou *DNS over TLS*.

DNSSEC est une évolution du protocole DNS, normalisée par l'IETF dans différentes RFC, la plus récente étant la 4035. Il permet de garantir l'authenticité des échanges entre le serveur DNS faisant autorité, et le *resolver* ou serveur de cache local. Il ne garantit cependant aucune authenticité entre le client qui émet la requête et le *resolver* DNS.

Dans le contexte d'utilisation décrit plus haut, cela signifie que ce protocole ne présenterait un intérêt que si l'on configure localement sur chaque poste de travail, un *resolver* DNS. Cette opération peut être compliquée à mettre en œuvre et à administrer sur les postes. Si cette option est retenue, elle consiste donc à installer un service DNS sur le poste d'accès (par exemple sur Linux ou Windows avec l'outil *unbound*), de le configurer pour qu'il s'exécute sur l'interface *loopback 127.0.0.1* et enfin d'activer la fonction *DNSSEC* en paramétrant une clé de signature. Toutes les requêtes DNS du poste sont envoyées à destination de ce service local, qui ensuite les transmet au serveur DNS public de l'entité.

DNSCrypt est un protocole de sécurisation du protocole DNS, permettant d'authentifier mutuellement le client qui émet la requête DNS et le serveur qui lui répond. Un chiffrement est également

réalisé sur les paquets échangés. Le protocole utilise un système de cryptographie asymétrique, pour gérer l'authentification et le chiffrement. Le protocole est conçu pour fonctionner en UDP ou TCP (port 443). L'objectif est de se prémunir d'attaques de type « homme du milieu » (ou *man-in-the-middle attack*), et également de *Spoofing DNS*. *DNSCrypt* est supporté notamment par le logiciel *OpenDNS*.

Une autre méthode consiste à utiliser le protocole *DNS over TLS*, qui permet d'ajouter une surcouche TLS sur le paquet DNS initial. Ce protocole permet donc, de même que pour *DNSCrypt*, de réduire les risques d'attaques de type « homme du milieu » ou de *spoofing DNS*. Il assure la confidentialité des échanges, le contrôle d'intégrité et l'authentification par certificats. *DNS over TLS* n'est pas encore supporté par beaucoup d'outils, à la date de rédaction de ce document, mais il est normalisé dans la RFC 7858 (IETF), contrairement à *DNSCrypt*.

Annexe D
Architectures d'authentification possibles

Pour rappel, le processus d'authentification au SI nomadisme doit pouvoir authentifier :

- l'utilisateur sur l'équipement d'accès ;
- l'équipement d'accès sur le SI nomadisme ;
- l'utilisateur sur le SI nomadisme.

Les exemples suivants traitent de deux modèles d'architecture : avec ou sans serveur d'authentification en coupure entre le concentrateur VPN et le SI interne de l'entité. La solution de mise en œuvre d'un serveur d'authentification dédié ajoute un composant d'authentification complémentaire au concentrateur VPN : cela procure une défense en profondeur, si toutefois la sécurité de ce serveur est à l'état de l'art et n'est pas source de vulnérabilités facilement exploitables par un attaquant. Dans les architectures sans serveur d'authentification en coupure, des points d'attention sont signalés.

Les trois figures suivantes D.1, D.2 et D.3 présentent différents modèles d'authentification, avec un serveur d'authentification en coupure et une authentification double facteur de l'utilisateur.

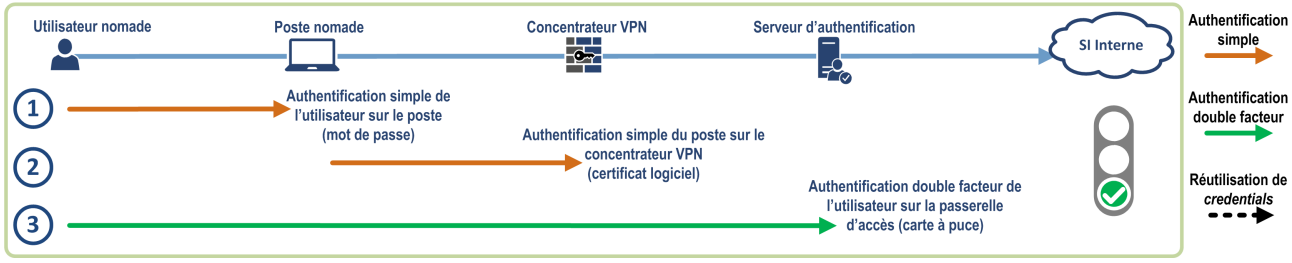

FIGURE D.1 – Exemple d'architecture

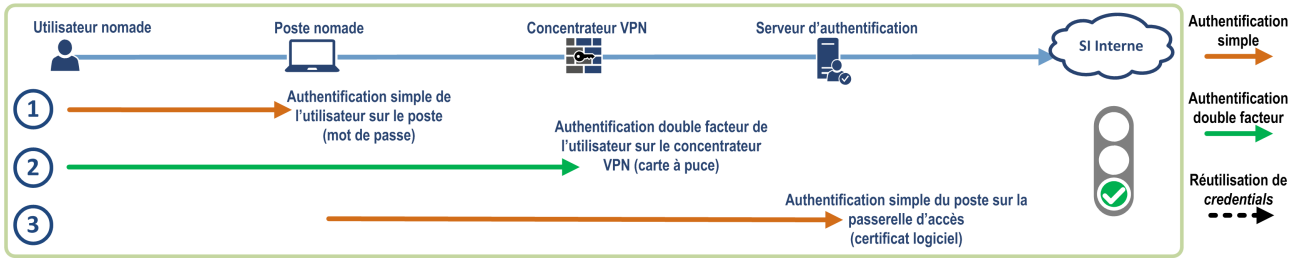

FIGURE D.2 – Exemple d'architecture

Les deux exemples d'architecture D.1 et D.2 présentent un bon niveau de sécurité au regard des risques liés au nomadisme. Une authentification double facteur de l'utilisateur est systématiquement faite (sur le concentrateur VPN ou bien sur le serveur d'authentification), ainsi qu'une authentification du poste de travail nomade.

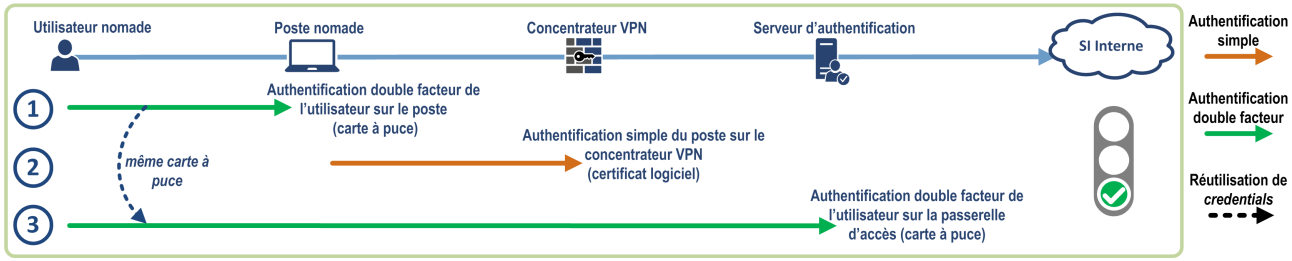

FIGURE D.3 – Exemple d'architecture

Dans l'exemple D.3, l'authentification double facteur est réalisée à la fois lors de l'authentification sur le poste et également sur le serveur d'authentification. L'intérêt est de pouvoir réutiliser la même carte à puce, mais avec des *AID* [36] différents, et des éléments secrets distincts.

Les figures D.4 et D.5 présentent des modèles sans serveur d'authentification en coupure, mais avec une authentification double facteur de l'utilisateur ainsi qu'une authentification du poste.

FIGURE D.4 – Exemple d'architecture

L'exemple D.4 met en œuvre deux authentifications successives sur le concentrateur VPN.

Dans le cas de l'utilisation d'un VPN IPsec, des spécifications ont été définies dans la RFC 4739 (*experimental*) pour ajouter une authentification supplémentaire lors de l'établissement du tunnel en IKEv2. Toutefois, celles-ci ont été très peu implémentées par les solutions du marché, à la date de rédaction de ce document.

Dans le cas d'un VPN TLS, plusieurs éditeurs supportent l'ajout d'une deuxième authentification par mot de passe utilisateur, pendant la phase d'établissement du tunnel VPN.

Ainsi, il est possible de faire une double authentification du poste et de l'utilisateur sur le concentrateur VPN, par le biais d'un certificat machine installé sur le poste et ensuite par une authentification double facteur de l'utilisateur (carte à puce et code PIN).

36. *Application Identifier* : Cet identifiant permet d'adresser un espace particulier sur la carte à puce, dédiée à une application spécifique. Selon les modèles de carte à puce il est possible de spécifier plusieurs *AID*, avec des éléments secrets différents pour chacun d'entre eux.

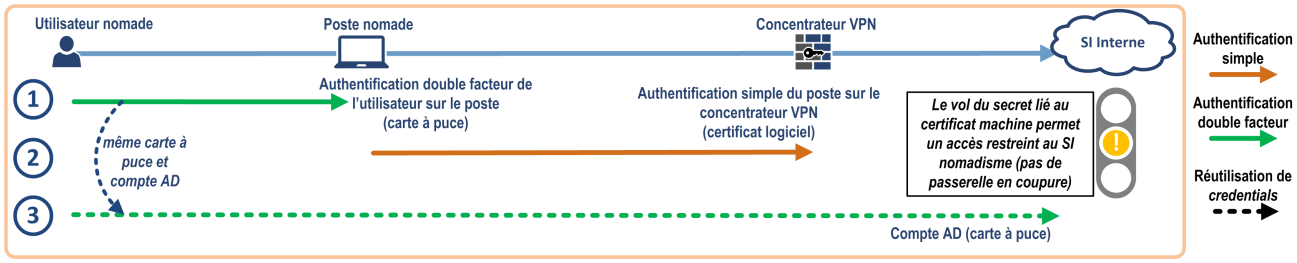

FIGURE D.5 – Exemple d'architecture

L'exemple D.5 d'utilisation de carte à puce pour une connexion vers un domaine *Active Directory* présente une faiblesse sur les contrôles opérés sur le concentrateur VPN. En effet, seule la validité du certificat machine y est vérifiée. Il est donc possible pour un attaquant, s'il parvient à récupérer les éléments secrets liés au certificat, de les utiliser pour se connecter au concentrateur VPN. L'attaquant a ainsi un accès restreint sur le SI interne de l'entité, et notamment la possibilité d'accéder au contrôleur de domaine, qui est un élément critique dans la sécurité d'un SI.

Sans la présence d'un serveur d'authentification supplémentaire avant l'accès au SI interne, la sécurité repose alors uniquement sur le filtrage réseau qui pourrait être réalisé sur des pare-feux internes, et également sur le filtrage applicatif des différents serveurs. Le cloisonnement de l'environnement du concentrateur VPN est donc à prendre en compte lors de l'analyse de cette solution.

La figure D.6 présente un modèle d'authentification similaire à l'exemple D.4 mais sans l'authentification double facteur de l'utilisateur.

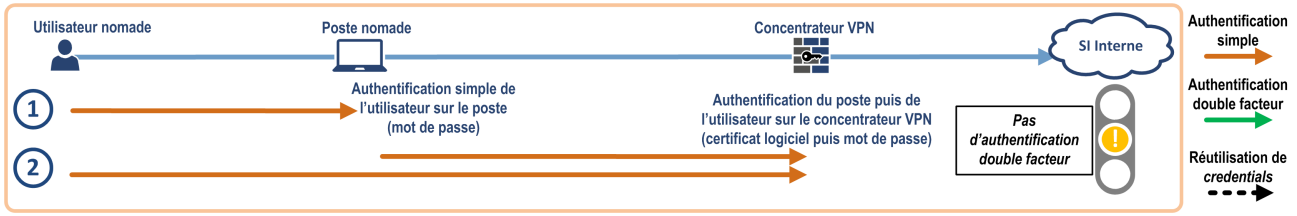

FIGURE D.6 – Exemple d'architecture

L'exemple D.6 est acceptable dans le sens où la tâche d'un attaquant pour accéder au SI interne est rendue plus complexe (il doit récupérer deux éléments secrets), mais elle ne respecte pas l'exigence d'avoir une authentification double facteur pour l'utilisateur nomade.

La figure D.7 présente un modèle d'authentification sans serveur d'authentification en coupure, mais avec une authentification double facteur de l'utilisateur.

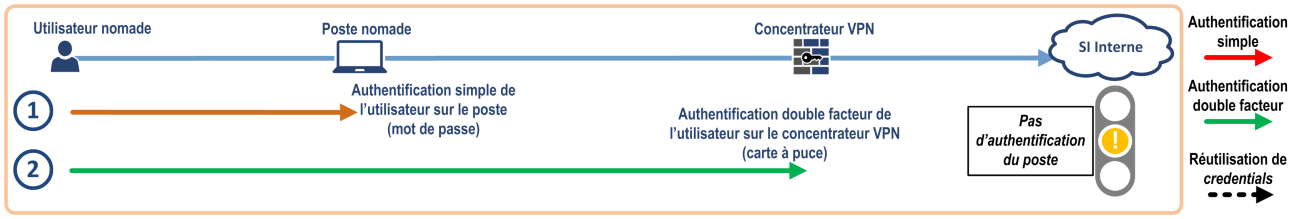

FIGURE D.7 – Exemple d'architecture

Dans l'exemple D.7, il n'y a pas de contrôle de la validité du poste utilisateur (certificat machine). Il est donc en théorie possible de se connecter sur le concentrateur VPN depuis n'importe quel poste, pour peu que l'utilisateur soit en mesure d'y brancher un lecteur de carte à puce et d'y installer le client VPN. Le risque de connexion vers le concentrateur VPN depuis un poste non maîtrisé est donc réel.

La figure D.8 présente un modèle d'authentification ne disposant ni de serveur d'authentification en coupure ni d'authentification double facteur de l'utilisateur.

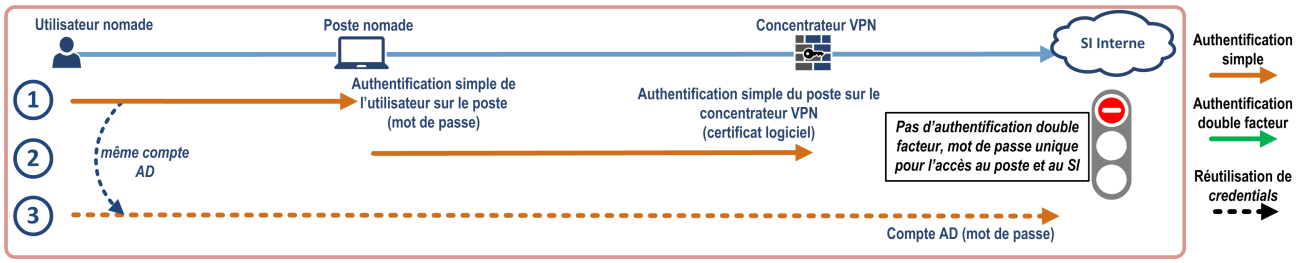

FIGURE D.8 – Exemple d'architecture

Cette dernière solution D.8 est à proscrire dans le sens où il n'y a aucune authentification double facteur et où les demandes d'authentification utilisateur sont limitées au strict minimum. L'utilisation des mêmes informations d'authentification (*credentials*) pour se connecter à la fois sur le poste et sur le SI de l'entité présente un risque de compromission important si l'élément secret en question est dérobé par un attaquant.

Annexe E
Journalisation du SI nomadisme

E.1 Évènements

Le SI nomadisme doit journaliser les évènements les plus pertinents des éléments de l'infrastructure vus précédement. Voici quelques exemples d'évènements, qui ne sont pas exhaustifs :

- ouvertures de sessions utilisateur (réussites, échecs, certificats expirés, etc.) ;
- fermetures de sessions utilisateur ;
- applications métier accédées par l'utilisateur ;
- connexions de supports amovibles ;
- erreurs système ;
- résultat de l'analyse anti-virus ;
- modifications de configurations (changement de mot de passe, etc.).

La journalisation de toutes les actions réalisées sur l'équipement d'accès utilisateur, pour se connecter sur le concentrateur VPN, puis au SI interne de l'entité, doit être mise en place.

E.2 Intégrité des journaux

Les journaux ne doivent être accessibles que par des personnes ayant le besoin d'en connaître (équipes de supervision, etc.). Quel que soit l'équipement concerné, personne ne doit être en mesure de modifier ces journaux et donc d'en compromettre l'intégrité. Pour rendre plus simple la résolution d'incidents lors d'un support technique, l'utilisateur peut être en mesure de consulter en lecture seule les journaux de son poste de travail.

Il faut donc prendre des mesures techniques de protection des journaux pour empêcher la modification par un tiers.

Sur les environnements Linux, il faut restreindre les droits en lecture et écriture sur le répertoire où sont stockés les journaux (généralement */var/log*).

Il est également recommandé de vérifier les droits d'écriture du démon *rsyslog* ou *syslog-ng* et de restreindre les droits de lecture aux seuls utilisateurs ayant le besoin d'en connaître.

Sur les environnements Windows, il est possible de mettre en œuvre des règles de sécurité par GPO avec les *Event Log Policy Settings*, par exemple en restreignant l'accès en lecture à certains groupes d'utilisateurs du domaine.

E.3 Analyse et corrélation des journaux

L'entité doit être capable de mener une analyse de corrélation sur l'ensemble des journaux composant le SI nomadisme, en cas d'incident suspecté ou avéré.

Ceci ne peut se faire correctement que si l'ensemble des journaux sont horodatés depuis une même source de temps, et si l'ensemble des systèmes de journalisation sont centralisés en un service unique.

Il est recommandé de faire la synchronisation via un serveur de temps *NTP* interne à l'entité. Il est conseillé que ce serveur *NTP* dispose de deux sources de temps distinctes, de technologies différentes (GPS, radio, Internet).

Pour mener correctement une analyse en cas d'incident, il est beaucoup plus facile de pouvoir visualiser dans une source unique l'ensemble des journaux correspondant au SI nomadisme. Pour mettre en œuvre cette fonctionnalité, il est nécessaire de configurer les différents serveurs pour envoyer une copie des journaux locaux sur un serveur centralisé.

De plus, cela permet une protection supplémentaire contre le risque d'altération des journaux par un attaquant, dans le cas où celui-ci aurait pris le contrôle d'un équipement avec des privilèges avancés. En effet, même s'il lui est possible de modifier et de supprimer des entrées de journal localement sur la machine corrompue pour effacer ses traces, il lui sera plus compliqué de devoir prendre également le contrôle sur le serveur qui centralise les journaux.

Les flux de journaux peuvent transporter des informations sensibles (comme des identifiants, des noms de serveurs, des adresses IP par exemple), et il est recommandé d'utiliser une surcouche TLS pour le chiffrement et le contrôle d'intégrité des flux, ainsi que l'authentification mutuelle entre le fournisseur et le collecteur de journaux.

Les flux de transfert des journaux d'évènements doivent se faire par le réseau d'administration du SI nomadisme.

Pour centraliser les journaux, il est possible d'utiliser deux modes : *push* ou *pull*, l'envoi se faisant respectivement à l'initiative du fournisseur ou du collecteur. Dans un environnement nomade, il est plus intuitif que l'envoi des journaux soit à l'initiative du fournisseur vers le collecteur, car les postes nomades sont, par définition, peu souvent connectés au SI de l'entreprise.

Il est donc recommandé d'utiliser le mode *push*.

Attention

L'utilisation du mode *push* pour l'envoi des journaux implique l'ouverture d'un flux réseau depuis un environnement supposé de moindre confiance (poste nomade) vers un environnement de confiance plus élevée (la DMZ entrante). Ce flux doit donc être sécurisé, filtré et contrôlé car il représente pour un attaquant une porte d'entrée vers le SI interne de l'entité.

La centralisation journaux peut se faire au moyen de l'implémentation d'un *SIEM* [37].

37. *Security information and event management.*

Liste des recommandations

Bibliographie

[1] *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.

[2] *Recommandations de configuration matérielle de postes clients et serveurs x86*.
Note technique DAT-NT-024/ANSSI/SDE/NP v1.0, ANSSI, mars 2015.
https://www.ssi.gouv.fr/nt-x86.

[3] *Déploiement et configuration centralisés d'EMET pour le durcissement des postes de travail et des serveurs Microsoft Windows*.
Note technique DAT-NT-027/ANSSI/SDE/NP v2.1, ANSSI, octobre 2016.
https://www.ssi.gouv.fr/emet.

[4] *Recommandations de configuration d'un système GNU/Linux*.
Note technique DAT-NT-028/ANSSI/SDE/NP v1.1, ANSSI, janvier 2016.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[5] *Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi*.
Note technique DAT-NT-034/ANSSI/SDE/NP v1.0, ANSSI, mai 2016.
https://www.ssi.gouv.fr/nt-vmware/.

[6] *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/.

[7] *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.

[8] *Recommandations pour une utilisation sécurisée de Cryhod*.
Guide ANSSI-BP-037 v1.0, ANSSI, mai 2017.
https://www.ssi.gouv.fr/recos-cryhod/.

[9] *Passeport de conseils aux voyageurs*.
Guide Version 2.0, ANSSI, août 2014.
https://www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs/.

[10] *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/guide/guide-dhygiene-informatique/.

[11] *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.

[12] *Achat de produits de sécurité et de services de confiance qualifiés*.
Guide Version 1.0, ANSSI, septembre 2014.
https://www.ssi.gouv.fr/achat-rgs/.

[13] *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.

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

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

[16] *Instruction générale interministérielle n° 1300*.
Référentiel Version 1.0, ANSSI, décembre 2006.
https://www.ssi.gouv.fr/igi1300/.

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

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

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

[20] *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.

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

ANSSI-PA-054
Version 1.0 - 17/10/2018

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