

RECOMMANDATIONS SUR LE NOMADISME NUMÉRIQUE

GUIDE ANSSI

PUBLIC VISÉ :

Développeur

Administrateur

RSSI

DSI

Utilisateur

Informations



Attention

Ce document rédigé par l'ANSSI s'intitule « **Recommandations sur le nomadisme numérique** ». Il est téléchargeable sur le site cyber.gouv.fr.

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

Conformément à la Licence Ouverte v2.0, le document peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales. Sauf disposition réglementaire contraire, les 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
2.0	13/11/2023	Mise à jour de la doctrine (Voir détails en Annexe B) Mise en cohérence avec d'autres guides Nouvelle charte graphique des schémas

Table des matières

1	Préambule	5
1.1	Pourquoi ce guide?	5
1.2	À qui s'adresse ce guide?	6
1.3	Convention de lecture	7
2	Présentation du sujet	8
2.1	Définitions	8
2.2	Périmètre	10
2.3	Risques	10
3	Sécurisation d'une infrastructure de nomadisme	12
3.1	Architecture globale	12
3.2	Utilisateur nomade	13
3.2.1	Inventaire	13
3.2.2	Sensibilisation	14
3.2.3	Lien avec les postes nomades	14
3.3	Poste nomade	15
3.3.1	Maîtrise du poste nomade	15
3.3.2	Protection physique	17
3.3.3	Contrôle d'intégrité au démarrage	18
3.3.4	Chiffrement des disques	20
3.3.5	Périphériques amovibles	22
3.3.6	Restrictions des priviléges de l'utilisateur	23
3.3.7	Durcissement système	25
3.3.7.1	Réduction de la surface d'attaque	25
3.3.7.2	Activation de fonctions de sécurité natives	26
3.3.8	Mise en quarantaine	27
3.3.9	Verrouillage du poste nomade	28
3.4	Canal d'interconnexion	29
3.4.1	Schéma général	29
3.4.2	Technologie VPN	30
3.4.3	Maîtrise des flux réseaux sur le poste nomade	31
3.4.3.1	Cas d'usage du <i>full-tunneling</i>	32
3.4.3.2	Cas d'usage du <i>split-tunneling</i>	33
3.4.3.3	Cas des flux DNS	35
3.4.3.4	Cas des flux DHCP	37
3.4.4	Portail captif	39
3.4.5	Connexion des postes nomades en interne de l'entité	40
3.4.5.1	Risques liés au mode de connexion	40
3.4.5.2	Risques liés à la détection de posture	41
3.4.5.3	Concentrateurs VPN internes	41
3.4.5.4	Mutualisation des concentrateurs VPN	44
3.4.5.5	Cas particulier d'une architecture VPN multi-sites	47

3.5 Authentifications	48
3.5.1 Principes généraux	48
3.5.1.1 Authentification de l'utilisateur sur le poste nomade	48
3.5.1.2 Authentification du poste nomade sur le SI	49
3.5.1.3 Authentification de l'utilisateur sur le SI	49
3.5.2 Authentification multifacteur	50
3.5.2.1 Présentation	50
3.5.2.2 Cas particulier de la biométrie	51
3.5.2.3 Technologies d'authentification multifacteur dans le cas du nomadisme	51
3.5.2.4 Cas d'usage de l'authentification multifacteur	51
3.5.3 Modèles d'authentification en nomadisme	53
3.5.3.1 Modèle d'authentification A	54
3.5.3.2 Modèle d'authentification B	56
3.5.3.3 Modèle d'authentification C	57
3.5.3.4 Modèle d'authentification D	58
3.5.3.5 Modèle d'authentification E	59
3.5.3.6 Modèle d'authentification F	60
3.5.4 Infrastructure de gestion de clés	61
3.5.5 Vérification de la validité des certificats	62
3.6 Passerelle d'interconnexion	65
3.6.1 Zones d'accès du SI interne	65
3.6.2 Flux réseau entre postes nomades	69
3.7 Ressources du SI de l'entité	69
3.7.1 Accès aux applications métiers internes	69
3.7.2 Accès aux applications métiers dans le Cloud	71
3.7.3 Filtrage des applications autorisées	72
3.7.4 Protocoles utilisés	73
3.7.5 Synchronisation hors ligne	73
4 Recommandations d'ordre général	75
4.1 Produits et solutions	75
4.2 Administration	75
4.3 Supervision	76
4.4 Journalisation	77
4.4.1 Liste d'événements à journaliser	77
4.4.2 Centralisation des journaux	78
4.5 Détection	79
4.5.1 Analyse et corrélation d'événements	79
4.5.2 Sonde de détection d'intrusion	79
Annexe A Sécurisation d'un poste nomade partagé entre plusieurs utilisateurs	81
Annexe B Évolutions du guide	82
B.1 Nouvelles recommandations	82
B.2 Mises à jour entre les versions 1.0 et 2.0	82
B.3 Matrice de rétrocompatibilité depuis la version 1.0 vers les versions ultérieures	83
Liste des recommandations	86

1

Préambule

1.1 Pourquoi ce guide ?

Le développement du nomadisme et du télétravail ne cesse de prendre de l'ampleur ces dernières années. Il est aujourd'hui au centre des priorités 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 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 responsables de la sécurité des systèmes d'information (RSSI), directeurs des systèmes d'information (DSI), administrateurs et équipes d'exploitation des systèmes d'information 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 ou non-sensibles.



Attention

Le cas du nomadisme pour des SI « Diffusion Restreinte » n'est pas traité dans ce guide mais dans une section spécifique du guide de l'ANSSI relatif à ces SI [35]. De même, ce guide n'est pas applicable aux SI contenant ou susceptibles de contenir des informations relevant du secret de la défense nationale au sens de l'IGI 1300 (Instruction générale interministérielle N°1300 sur la protection du secret de la défense nationale) [34].

1.3 Convention de lecture

Pour certaines recommandations de ce guide, il est proposé, compte-tenu de l'état de la menace constaté lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

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* ».

Ainsi, les recommandations sont présentées de la manière suivante :

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

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information¹, la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

Quelles que soient les recommandations finalement retenues, l'application de ces mesures ne peut en aucun cas remplacer une évaluation du niveau de sécurité du SI par un audit, ni dispenser d'évaluer le niveau de risque résiduel sur les actifs métier.

La liste récapitulative des recommandations est disponible en page 88.

1. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [23].

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 de l'entité

Le SI de l'entité désigne l'ensemble des éléments qui composent le système d'information de l'entité : serveurs en *datacenter* interne, services externalisés dans un *cloud*, postes de travail, ressources publiques, etc.



SI interne

Le SI interne est une sous-partie du SI de l'entité, qui inclut l'ensemble des ressources accessibles par les utilisateurs lorsqu'ils ne sont pas en situation de nomadisme.



Passerelle d'interconnexion

Une passerelle d'interconnexion est constituée d'une ou plusieurs « DMZ »² qui doivent être des zones neutres, perdables, protégées par des pare-feux périphériques et servant dans le cas de ce guide à sécuriser les connexions des utilisateurs depuis un réseau public vers le SI interne.

2. *Delimitarized zone* : terme anglais désignant une zone démilitarisée, qui est régulièrement réutilisé pour désigner un sous-réseau (concrètement, quelques équipements) séparant deux zones de confiance hétérogène.



Poste nomade

Le poste nomade désigne le terminal physique mis à disposition de l'utilisateur nomade pour accéder aux ressources de l'entité. Il s'agit généralement d'un PC portable (*laptop*), d'un téléphone mobile (*smartphone*) ou encore d'une tablette professionnelle.



Canal d'interconnexion

Le canal d'interconnexion désigne le lien réseau sécurisé entre le poste nomade en situation de nomadisme et l'équipement de sécurité de la passerelle d'interconnexion permettant de donner accès aux ressources du SI interne.



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 priviléges 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 1 décrit le périmètre du guide en couleur bleue :

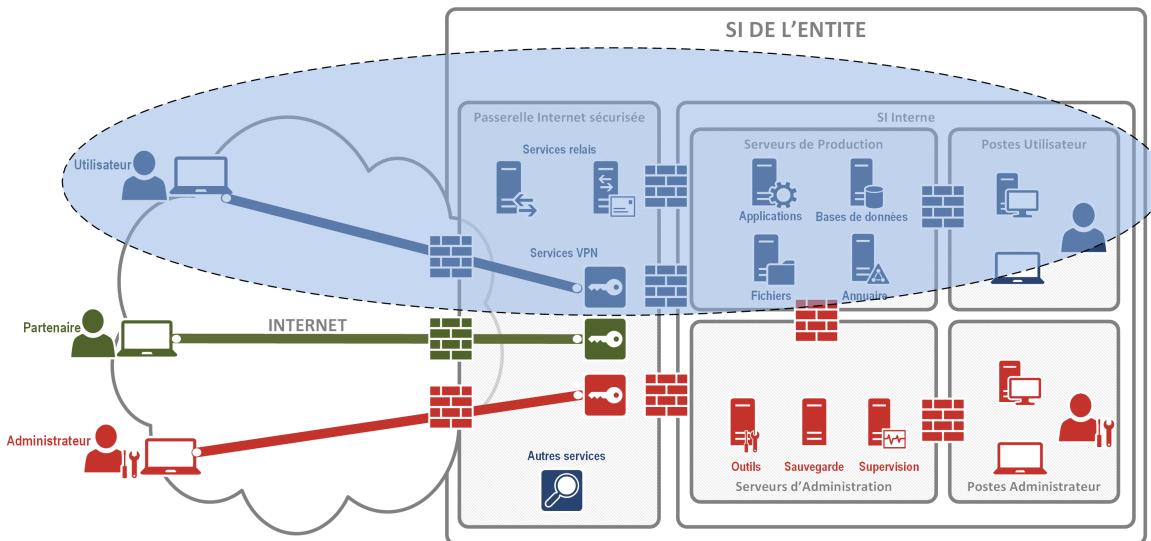


FIGURE 1 – Différents cas d'accès à distance et périmètre du guide

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 conseillé de suivre les recommandations contenues dans les guides [13, 27] publiés par l'ANSSI ;
- les utilisateurs situés en dehors du territoire national. Dans ce cas précis, il est conseillé, en complément des préconisations de ce guide, de suivre les recommandations contenues dans le guide de bonnes pratiques à l'usage des professionnels en déplacement [15] ;
- les accès des partenaires 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 du lieu (contrôle d'accès par badge, surveillance), mais également du fait que les locaux soient 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 télétravaille 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 :

- lorsqu'il travaille à l'hôtel pendant un déplacement professionnel;
- lorsqu'il travaille dans les transports en commun;
- lorsqu'il travaille dans des salles d'attente ou tout autre lieu public;
- lorsqu'il 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 le 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 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

Dans le cadre du nomadisme, l'objectif est de réussir à s'aligner avec le niveau de sécurité 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, les acteurs concernés ainsi que les moyens mis en œuvre pour atteindre la cible de sécurité de son SI en situation de 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

Sécurisation d'une infrastructure de nomadisme

3.1 Architecture globale

La figure 2 présente de façon macroscopique les éléments qui composent le nomadisme :

- l'utilisateur nomade ;
- le poste nomade ;
- le canal d'interconnexion ;
- la passerelle d'interconnexion ;
- les ressources accessibles par les postes nomades dans le SI interne de l'entité.

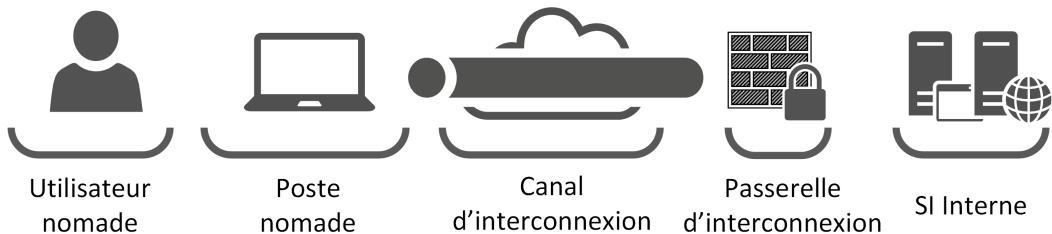


FIGURE 2 – Composants du nomadisme

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 et les conséquences d'une attaque réussie. Les mesures spécifiques qui s'appliquent à chacun de ces éléments sont présentées dans ce chapitre, celles s'appliquant à l'ensemble de ces éléments étant présentées dans le chapitre suivant.

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. De même, certaines applications métier peuvent imposer des restrictions d'accès à des modules ou des interfaces métier dans le cas où les utilisateurs sont en situation de nomadisme. Cette problématique peut être pertinente pour traiter le cas des administrateurs fonctionnels des applications sensibles de l'entité. Elle peut néanmoins nécessiter certains développements logiciels afin de prendre en compte la situation d'un utilisateur donné avant de lui affecter des droits d'accès dans l'application.

R2

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

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

- le niveau de sensibilité des données ou de l'activité est trop élevé ;
- des contraintes réglementaires ;
- des restrictions liées au métier (p. ex. utilisation de matériel spécifique).

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 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.

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 création et la révocation des comptes et la gestion des droits d'accès au SI ;
- le changement de catégorie de l'utilisateur nomade ;
- la gestion des postes 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 indiscretions et fuites d'informations.

Il est donc indispensable de mettre en place des campagnes de sensibilisation spécifiques pour tous les 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 (p. ex. verrouiller sa session lorsque l'on laisse le poste sans surveillance, ne pas exposer la saisie de secrets à la vue d'autres personnes, etc.).

3.2.3 Lien avec les postes nomades

Dans un contexte d'utilisation nomade, il est fréquent que les postes nomades 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 avec un compte personnel permettant l'imputabilité 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

Dévier le poste nomade à un utilisateur nomade identifié

Chaque poste nomade doit être lié à un utilisateur nomade. L'utilisateur et le poste nomade doivent être identifiés dans le système de gestion d'équipements de l'entité³.

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

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

³. Ce système de gestion d'équipements est une suite logicielle que l'on retrouve généralement sous l'appellation *ITSM - Information Technology Service Management* ou bien *CMDB - Configuration Management Database*.

Dans le cas où les postes nomades sont partagés, il est important de mettre en œuvre des mesures de sécurité complémentaires pour s'assurer d'un cloisonnement strict entre les utilisateurs partageant ces postes.

3.3 Poste nomade

3.3.1 Maîtrise du poste nomade

Pour rappel, le poste nomade de l'utilisateur nomade peut être entre autres :

- un poste de travail portable (*laptop*);
- un mobile multifonction ou téléphone mobile (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 ce poste nomade.

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 postes nomades sur lesquels les utilisateurs nomades se connectent.

L'utilisation d'équipements personnels par l'utilisateur (AVEC⁴ en français ou BYOD⁵ 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 suffisant de l'équipement personnel;
- la multiplication des environnements utilisateur, qui rend la gestion du parc et du cycle de vie des applications difficile (navigateurs Web, interfaces homme-machine, etc.);
- la complexité de l'investigation en cas d'incidents.

Certains équipements de téléphonie mobile permettent de mettre en œuvre un système de conteneur sécurisé et cloisonné, destiné à l'usage professionnel.

Cependant, même si le conteneur professionnel dispose de fonctions de cloisonnement logique vis-à-vis du système d'exploitation hôte et que l'image disque de ce conteneur est chiffrée, son utilisation reste néanmoins partagée avec un système d'exploitation qui n'est pas protégé.

4. Apportez Votre Équipement personnel de Communication.

5. Bring your own device.

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 *stores*) publics sur les systèmes protégé et non protégé. Des restrictions d'usage doivent donc être mises en place, avec un outil de MDM⁶ 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 depuis des sources non maîtrisées ;
- 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 NFC⁷, etc. ;
- filtrer la navigation Web sur Internet.

R6

Maîtriser le poste nomade de l'utilisateur nomade

Seuls les postes nomades 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 (BYOD).

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

6. *Mobile device management*.

7. *Near Field Communication*.

3.3.2 Protection physique

Dans le cadre du nomadisme, un attaquant est susceptible de faire acte d'indiscrétion sur l'écran du poste nomade, 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 du poste nomade soit visible par l'entourage proche de l'utilisateur nomade.

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

R7

Mettre à disposition des moyens de protection physique du poste nomade

L'entité doit mettre à disposition les moyens suivants pour protéger les postes nomades :

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

3.3.3 Contrôle d'intégrité au démarrage

En modifiant un ou plusieurs éléments de la chaîne de démarrage, un attaquant peut compromettre l'intégrité du système d'exploitation du poste nomade. Lors de chaque démarrage du poste nomade, l'attaquant aura ainsi un accès privilégié sur le système d'exploitation. Le fait de déployer une porte dérobée au sein de la chaîne de démarrage est un moyen furtif et efficace de conserver une persistance sur le système.

De même, il est possible qu'un attaquant essaye d'amorcer le poste nomade 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 nomade sur un autre système d'exploitation que celui installé et durci par l'entité. En particulier, il est recommandé que le démarrage du poste nomade depuis un périphérique amovible (USB) et depuis le réseau local (*boot PXE*) soit interdit.

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

De manière générale, il est important de configurer le BIOS ou l'*UEFI* de manière à ce que les fonctionnalités non utilisées soient désactivées (p. ex. les fonctionnalités d'accès à distance comme *Intel AMT*⁸ ou bien *Computrace*).

Il est impératif d'assurer l'intégrité de la chaîne de démarrage du système via des mécanismes cryptographiques. En effet, l'intégrité, et donc la confiance que l'on peut avoir dans le système d'exploitation, dépend de l'intégrité et de la confiance que l'on a dans chaque maillon de la chaîne de démarrage. Il est donc recommandé de mettre en place le *Secure Boot UEFI*.

Cette fonctionnalité permet de contrôler l'intégrité de certains éléments faisant partie de la chaîne de démarrage, par exemple les chargeurs de démarrage (*bootloader*), le noyau du système d'exploitation, etc. Le *Secure Boot UEFI* ne permet que le contrôle d'images exécutables, soit par une signature à l'aide d'une clé de signature et accompagnée d'un certificat, soit par une somme de contrôle inscrite dans une base de données.

La majorité des équipements du marché sont configurés par défaut avec des clés publiques de Microsoft chargées dans le système *UEFI*. Ces clés signent plusieurs composants de la chaîne de démarrage de Windows, tels que le *Windows Boot Manager* (*bootmgr.exe*) mais également des utilitaires comme *shim*. Cet utilitaire *shim* est utilisé par les distributions Linux majeures pour bénéficier de la fonction *Secure Boot UEFI* sans avoir à refaire signer toute nouvelle version de leur noyau et de leur *bootloader* par Microsoft. Les clés préchargées sur ces équipements autorisent donc le démarrage d'une multitude de systèmes d'exploitation et de *bootloader*.

Dans le cas d'un système d'exploitation autre que Windows, il est donc conseillé de remplacer l'architecture de clés de Microsoft par une architecture de clés interne maîtrisée, puis de signer les binaires *UEFI* nécessaires (*bootloader*, *UKI*, etc.). Une *UKI* (*Unified Kernel Image*) regroupe généralement plusieurs composants : le noyau, l'*initramfs* et la ligne de commande du noyau. Il est

8. Active management technology.

important que ces trois éléments au minimum fassent partie de l'UKI, afin que leur intégrité soit vérifiée par le *Secure Boot UEFI* lors du démarrage.

Le *Secure Boot UEFI* ne permet cependant pas de maîtriser tous les éléments de la chaîne de démarrage (p. ex. les fichiers de configuration des *bootloader*). Le *Measured Boot* est une technique complémentaire du *Secure Boot UEFI*. En effet, ce dernier assure que les binaires UEFI de la chaîne de démarrage sont tous signés, mais permet donc de démarrer plusieurs versions du système (ancienne version, version parallèle signée...). Par contraste, le *Measured Boot* s'appuie sur plus de paramètres et permet de s'assurer que le système actuellement démarré est dans un état précis attendu. Pour cela, le *Measured Boot* s'appuie sur le TPM⁹ et ses PCR¹⁰.

Lors du démarrage, les différents éléments constituant la chaîne de démarrage (*firmware*, binaires UEFI, état du *Secure Boot UEFI*, etc.) sont mesurés, et leurs empreintes sont stockées dans les PCR du TPM. Cet ensemble de valeurs représente donc de façon unique l'état du système actuellement démarré. La fiabilité du *Measured Boot* provient du fait que chaque élément de la chaîne de démarrage mesure le prochain maillon à exécuter ou à consommer, avant de démarrer l'action associée à cette ressource.

Un secret peut ensuite être scellé dans le TPM avec une politique de descellement reposant sur un ensemble de PCR et leurs valeurs. Au prochain redémarrage, le secret sera descellé par le TPM à la seule condition que les valeurs des PCR du système démarré correspondent aux valeurs décrites dans la politique associée à ce secret. Autrement dit, il faut que l'état du système soit le même que celui choisi lors du scellement, assurant que le démarrage n'a pas été compromis.

Ce secret peut être utilisé, par exemple, comme clé de chiffrement d'un disque. En cas de démarrage compromis, le *Measured Boot* n'interrompra pas le démarrage, mais le TPM ne descellera pas le secret, empêchant le déchiffrement du disque (voir à ce sujet la section 3.3.4).

La plupart de ces bonnes pratiques sont détaillées dans les guides de l'ANSSI concernant Windows [7] et Linux [4, 11].

R8

Maîtriser l'intégrité de la séquence de démarrage du poste nomade

Il faut prendre des mesures de protection sur les éléments intervenant dans la séquence de démarrage du poste nomade :

- durcir la configuration de l'UEFI, notamment la possibilité de démarrer sur un autre système que celui prévu (USB, PXE, etc.);
- protéger l'accès à la configuration UEFI par un mot de passe robuste;
- utiliser les fonctions de *Secure Boot UEFI*;
- mettre en place la fonctionnalité de *Measured Boot* avec un maximum de PCR.

9. *Trusted Platform Module* : composant physique généralement intégré sur la carte mère des équipements, et permettant l'exécution d'opérations cryptographiques et le stockage de secrets, dans un environnement sécurisé résistant à certaines attaques, par canaux auxiliaires par exemple.

10. *Platform Configuration Register* : emplacement mémoire au sein du TPM permettant le stockage de valeurs de contrôle lors du processus de démarrage du poste.

3.3.4 Chiffrement des disques

En situation de nomadisme, un poste nomade peut être perdu ou volé. Il est primordial que personne, autre que l'utilisateur légitime, ne puisse avoir accès à des données sensibles.

Sans mesure de sécurité particulière, un attaquant est en capacité d'accéder aux informations stockées sur les disques du poste nomade quand bien même il ne dispose pas d'identifiants et d'authentifiants valides du système d'exploitation. Afin de réduire ce risque d'accès illégitime aux informations, il est impératif de mettre en œuvre un mécanisme de chiffrement adéquat des disques sur le poste nomade.

Il est recommandé de chiffrer l'intégralité du disque, ou au minimum, toutes les partitions pouvant contenir des informations sensibles. Le chiffrement de la partition système est également important car l'accès à cette partition peut donner à un attaquant des indications sur de potentielles vulnérabilités du poste, et donc d'orienter sa méthodologie pour le compromettre. En l'absence de protection de cette partition système, un attaquant pourrait également être en mesure de modifier directement le système d'exploitation, pour y ajouter des fonctions malveillantes (p. ex. remplacer des fichiers ou des utilitaires d'administration sur le disque pour se créer un compte à privilège).

Dans l'idéal, si la solution logicielle le permet, le chiffrement du disque doit également être protégé en intégrité et en authenticité¹¹.

Pour être efficace, l'outil doit être configuré de manière à ce que la fonction de déchiffrement du disque au démarrage du poste ne soit pas automatique mais nécessite la saisie préalable d'un mot de passe par l'utilisateur.

En outre, il est recommandé que les clés utilisées pour le chiffrement du disque du poste nomade soient protégées au moyen d'un composant de sécurité physique. Ce composant est généralement un TPM.

Il est indispensable de maintenir dans tous les cas la nécessité de saisie d'un mot de passe utilisateur au démarrage du poste nomade, même lorsque qu'un TPM est utilisé pour protéger le secret de déchiffrement du disque.

Lorsque la solution logicielle le permet, il est recommandé de lier le descellement de ce secret de déchiffrement au mot de passe renseigné par l'utilisateur. En effet, comme expliqué dans la section 3.3.3, l'utilisation du mécanisme de *Measured Boot* reposant sur le TPM permet de sceller un secret à ce TPM et d'être en mesure de le récupérer seulement à la condition que le système soit dans un état connu et de confiance.

Il faut donc associer une politique de descellement par PCR (mesures indiquant un système dans un état légitime) à une politique de descellement par mot de passe, afin de permettre la récupération du secret de déchiffrement auprès du TPM seulement en cas de succès combiné sur ces deux contrôles.

L'association de ces deux mécanismes permet ainsi de complexifier plusieurs techniques de compromission pour un attaquant : tentative de déchiffrement du disque sur un matériel différent, sur

11. par exemple, à l'aide de l'option *-integrity* de l'outil *cryptsetup* sur les environnements Linux.

un clone du disque, avec une option de démarrage différente (p. ex. démarrage sur une clé USB au lieu du disque), tentative de lecture illégitime du secret de déchiffrement scellé dans le TPM (p. ex. attaques physiques sur le matériel), etc.

Il est recommandé que cette politique de scellement du secret de déchiffrement prenne en compte un maximum de PCR afin de contrôler le plus d'éléments de la chaîne possibles.

R9

Mettre en œuvre une solution de chiffrement de disque avec un TPM

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

Un mot de passe permettant de lancer le déchiffrement du disque doit être demandé à l'utilisateur au démarrage du poste nomade.

Un composant de sécurité physique TPM doit être utilisé pour protéger les clés de chiffrement et l'intégrité de la chaîne de démarrage (*Measured Boot*). Il est recommandé, si possible, d'associer le descellement du mot de passe utilisateur à la politique de descellement par PCR lors de la récupération du secret de déchiffrement du disque.

Enfin, si la solution logicielle le permet, le chiffrement du disque doit également être protégé en intégrité et en authenticité.

La politique de scellement d'un secret de chiffrement au TPM peut nécessiter un mot de passe, mais également d'autres facteurs tels qu'une carte à puce (permettant une authentification multi-facteur).

Il est recommandé, si la solution de chiffrement supporte cette fonctionnalité, d'utiliser conjointement les protections offertes par le TPM et celles offertes par une carte à puce, afin d'une part d'améliorer le niveau de contrôle de l'intégrité du processus de démarrage (TPM) et d'autre part de protéger l'opération de descellement par l'utilisation d'un composant physique externe (carte à puce) avec un code PIN.

R9 +

Renforcé Mettre en œuvre une solution de chiffrement de disque avec un TPM et une carte à puce

Si la solution de chiffrement et le poste nomade le permettent, il est recommandé de mettre en place le *Measured Boot* via le TPM, et de lier les opérations de descellement à une carte à puce. Un mot de passe ou code PIN lié à cette carte à puce doit être demandé à l'utilisateur au démarrage du poste nomade, afin de lancer le processus de déchiffrement du disque.

Dans le cas où le poste nomade ne dispose pas de composant de sécurité TPM ni de carte à puce, ou bien si la solution logicielle de chiffrement n'est pas compatible avec ces deux fonctionnalités, il reste néanmoins primordial de chiffrer le disque.

Dégradé À défaut - Mettre en œuvre une solution de chiffrement de disque sans composant de sécurité physique

Si la solution de chiffrement ou le poste nomade ne permet pas l'utilisation d'un TPM et d'une carte à puce, un chiffrement du disque sans cette fonctionnalité doit être mis en place.

Un mot de passe permettant de lancer le déchiffrement du disque doit impérativement être demandé à l'utilisateur au démarrage du poste nomade.

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 le poste nomade 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 du poste nomade pour y déployer des logiciels malveillants. Enfin, certaines clés s'attaquent physiquement au poste nomade 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 l'accès aux périphériques amovibles sur le poste 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 ou UEFI (en considérant néanmoins que certains composants internes au poste nomade 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 nomade 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 multifacteur 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 :

- imposer la connexion exclusive 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 ;
- inspecter systématiquement le contenu par des solutions antivirales lors de la connexion du périphérique amovible et bloquer ce dernier ou le mettre en quarantaine en cas de détection d'un fichier vérifié ;
- 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 postes nomades.

À titre d'exemple, cette fonction de filtrage des périphériques USB peut être mise en œuvre au moyen de GPO sur les systèmes Windows et par l'usage d'outils comme *USBGuard* ou plus directement du module *udev* sur les systèmes Linux.



Attention

L'utilisation de filtrage par *Vendor ID*, *Product ID* ou *USB Serial Number* est une mesure possible pour réduire les risques, mais celle-ci peut facilement être contournée par des outils d'usurpation d'identité USB (*USB Spoofing*). En l'absence de moyen d'authentification du matériel plus robuste, ce risque résiduel doit donc être assumé.

R10

Maîtriser la connexion de périphériques amovibles sur le poste nomade

Il est recommandé d'interdire la connexion de tout périphérique amovible et de bloquer tous les accès de ces périphériques (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, de traçabilité et d'inspection antivirale pour l'utilisation de périphériques amovibles.

3.3.6 Restrictions des priviléges de l'utilisateur

L'utilisateur ne doit pas être en mesure de modifier le paramétrage des logiciels assurant la connexion du poste nomade au SI de l'entité. Il ne doit pas avoir les droits de désinstaller les moyens de connexion logiciels installés sur son poste nomade (client VPN, logiciel de gestion de carte à puce, etc.) ni de désactiver les fonctions de protection configurées sur son poste nomade (pare-feu, antivirus, etc.).

L'utilisateur ne doit donc pas être administrateur local de son poste.

R11

Interdire à l'utilisateur la modification de la configuration des moyens de protection et de connexion au SI de l'entité

Cette recommandation concerne tous les logiciels nécessaires à la connexion vers le SI de l'entité (p. ex. le client VPN) et les fonctions de protections associées (p. ex. le pare-feu local) installés sur le poste nomade de l'utilisateur.

Les moyens de connexion au SI de l’entité, comme le client logiciel permettant l’établissement du tunnel VPN (le client VPN), peuvent être lancés selon différents modes :

- automatiquement au démarrage du poste nomade avant l’ouverture de session utilisateur (mode appelé parfois *device tunnel*) ;
- automatiquement au démarrage du poste nomade après l’ouverture de session utilisateur (mode appelé parfois *user tunnel*) ;
- manuellement par une action de l’utilisateur lui-même, après qu’il a ouvert une session.

Ces différents modes ne sont pas équivalents du point de vue de la sécurité ; il convient d’adapter le mode de connexion aux besoins fonctionnels et de sécurité de l’entité.



Information

La possibilité pour un utilisateur de démarrer, stopper ou redémarrer le tunnel VPN n’est pas considéré ici comme une modification de configuration, dès lors que cette fonctionnalité est légitime, qu’elle répond à un besoin métier et qu’elle est prévue dans la politique de sécurité de l’entité.

Dans le cas où les besoins de sécurité sont importants, il est recommandé que le tunnel VPN soit lancé automatiquement au démarrage du poste nomade et sans possibilité d’être arrêté par l’utilisateur.

Cette configuration s’inscrit dans une démarche de défense en profondeur : deux dispositifs de filtrage sont mis en œuvre, le filtrage IP induit par l’établissement d’un tunnel VPN et l’interdiction du *split-tunneling* (cf. recommandation R19 de la section 3.4.3.1) ainsi que le filtrage IP par le pare-feu local.

Cette configuration permet que la défaillance de l’un soit compensée par le bon fonctionnement de l’autre.

En outre, ce mode de fonctionnement permet d’assurer une continuité de service pour certaines actions automatisées sur le poste nomade :

- l’envoi des journaux d’événements depuis le poste nomade vers un serveur de collecte centralisé. Cela peut ainsi faciliter la détection d’une compromission du poste nomade ;
- la réception des correctifs de sécurité sur le poste nomade depuis un serveur de mises à jour centralisé. Cela peut ainsi réduire la surface d’attaque du poste nomade dans le cas de correctifs de sécurité critiques.

Dans le cas où le réseau de transport subit une indisponibilité (p. ex. connexion Internet défaillante), le client VPN doit prévoir de nouvelles tentatives de connexion automatique vers le SI de l’entité à une fréquence régulière suffisamment courte (délai inférieur à 5 minutes).

R11 +

Renforcé Établir le tunnel VPN automatiquement au démarrage du poste nomade et interdire toute action manuelle de l'utilisateur

L'établissement du tunnel VPN doit être réalisé automatiquement le plus tôt possible lors de la séquence de démarrage du poste nomade. Il est donc recommandé de préférer le mode automatique de type *device tunnel* au mode *user tunnel*. Ce processus est exécuté sans qu'il n'y ait possibilité pour l'utilisateur d'interagir et de modifier le comportement de celui-ci, ni au démarrage du poste nomade, ni ultérieurement pendant sa durée d'utilisation.



Attention

Dans une démarche de défense en profondeur, il est recommandé que la fonction de filtrage réseau et la fonction de chiffrement VPN ne soient pas portées par le même logiciel sur le poste nomade. Par ailleurs, les logiciels utilisés pour ces deux fonctions doivent si possible être indépendants, c'est-à-dire interdire toute interaction de l'un sur l'autre (p. ex. un client VPN qui active ou désactive certaines règles du pare-feu local de manière automatique).

Cette recherche de deux barrières de protection indépendantes améliore la robustesse globale sur le poste nomade, en cas de vulnérabilité affectant l'un des deux composants.

3.3.7 Durcissement système

Le renforcement du niveau de sécurité du système d'exploitation du poste nomade peut se résumer par ces deux mesures génériques :

1. la réduction de la surface d'attaque ;
2. l'activation et la configuration stricte des fonctions de sécurité natives ;

3.3.7.1 Réduction de la surface d'attaque

La réduction de la surface d'attaque du poste nomade regroupe un ensemble de mesures destinées à désactiver ou désinstaller des services ou fonctions inutilisés, ou bien notoirement connus pour embarquer des vulnérabilités. Les mesures suivantes peuvent être mises en œuvre :

- désinstaller toutes les applications non nécessaires et notamment les applications pré-installées par défaut ;
- désactiver les fonctionnalités non nécessaires (Bluetooth, biométrie, Thunderbolt, etc.) ;
- désactiver les services réseaux et système non nécessaires (service de messagerie locale, service de *spooler* d'impression, etc.) ;
- désactiver les protocoles vulnérables (SMBv1, NTLMv1, FTP, etc.) ;
- désactiver ou supprimer des comptes locaux non utilisés, notamment les comptes disposant de priviléges ;
- restreindre les possibilités de paramétrage pour les utilisateurs (options visibles des panneaux de configuration) ;

- restreindre la possibilité pour l'utilisateur d'exécuter des commandes interactives (*Powershell* pour Windows, accès aux consoles pour Linux, etc.);
- désactiver les fonctions de télémétrie et d'envoi de statistiques aux éditeurs;
- etc.

Les moyens de connexion possibles sur un poste nomade 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 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 doit être automatique.

R12

Réduire la surface d'attaque sur le système d'exploitation du poste 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 opérationnel le nombre de comptes locaux à privilèges;
- désactiver les technologies non utilisées selon le contexte d'usage : Wi-Fi, réseau mobile (4G, 5G), Bluetooth, NFC, Thunderbolt, etc.

Dans une démarche de réduction de la surface d'attaque, il est pertinent de désactiver en particulier le protocole IPv6 sur les postes nomades si ces derniers ne nécessitent que le protocole IPv4 pour se connecter au réseau local. Cette mesure permet de se prémunir d'attaques connues sur IPv6, par exemple la possibilité de réaliser un *man-in-the-middle* avec le protocole DHCPv6.

R13

Désactiver IPv6 sur le poste nomade si celui-ci n'est pas nécessaire

Il est recommandé de ne pas laisser le protocole IPv6 activé sur le poste nomade si celui-ci ne nécessite qu'une connectivité réseau locale avec le protocole IPv4.

3.3.7.2 Activation de fonctions de sécurité natives

L'application de fonctions de sécurité supplémentaires dépend des possibilités offertes par l'OS du poste nomade.

En environnement Windows, la fonctionnalité *AppLocker* permet de définir des règles d'accès aux différentes applications déployées sur le poste nomade, pour des utilisateurs donnés. Il est possible de définir des autorisations d'exécution en fonction des répertoires d'accès, des signatures ou empreintes de binaires, etc. L'outil permet également de mettre en œuvre une journalisation d'événements liés aux tentatives de démarrage d'applications par les utilisateurs.

L'outil *Windows Defender Exploit Guard* permet de renforcer la sécurité pour réduire la probabilité d'attaques liées à l'exploitation de vulnérabilités dans la gestion de la mémoire des processus.

Les fonctions *Credential Guard*, *Device Guard* et *Windows Defender Application Guard* de Microsoft permettent respectivement de protéger les processus d'authentification (*LSASS*¹²), le code du noyau de Windows et la navigation web dans des environnements virtuels cloisonnés.

Enfin l'outil LAPS de Microsoft permet de durcir la politique de sécurité des mots de passe des comptes d'administrateur local sur les postes nomades : rotation régulière des secrets d'authentification, diversification entre chaque poste (éviter la latéralisation), etc.

La plupart de ces bonnes pratiques sont détaillées dans les guides de l'ANSSI concernant Windows [5, 7, 8, 9].

En environnement Linux, il est également possible de mettre en place un durcissement du poste nomade en suivant les guides de l'ANSSI à ce sujet [4, 11]. Par exemple, la sécurisation du poste nomade peut se faire par une configuration spécifique des paramètres *sysctl* réseau et système, par des mesures de cloisonnement système (*chroot*, conteneurisation [12], etc.) ou encore par une gestion stricte des comptes à priviléges avec l'outil *sudo*.

R14

Mettre en œuvre les fonctions de sécurité du système d'exploitation sur le poste nomade

Il est recommandé d'utiliser les fonctions de sécurité des systèmes d'exploitation des postes nomades :

- Configuration des fonctions natives *AppLocker*, *Windows Defender Exploit Guard*, *Device Guard*, *Credential Guard*, *Windows Defender Application Guard*, *LAPS* sur des systèmes Windows ;
- Application des recommandations du guide de l'ANSSI sur des systèmes Linux [4, 11].

3.3.8 Mise en quarantaine

Dans les prérequis de connexion d'un poste 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 antivirus. Dans ce cas, connecter le poste nomade 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 ce poste nomade dans un environnement cloisonné de quarantaine.

Cet environnement de quarantaine 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, le poste nomade peut alors basculer sur l'environnement de production nomade.

12. Local Security Authority Subsystem Service.



Attention

Dans certains cas, lorsque des vulnérabilités critiques ont été identifiées pour certains postes nomades, 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 ces postes avant de les connecter de nouveau sur le SI interne.

Pour réaliser ce contrôle de conformité, il est possible de s'appuyer sur des fonctionnalités nativement implémentées dans les systèmes d'exploitation quand elles existent, ou bien sur des produits tiers nécessitant l'installation d'un agent sur le poste nomade.

Dans tous les cas, il convient d'être vigilant sur les points suivants :

- un contrôle de conformité présente des limites et ne peut garantir complètement que le poste nomade n'a pas été compromis, puisqu'un attaquant ayant des droits d'administrateur local pourrait modifier le comportement de l'agent de vérification de manière à ne pas être détecté par le serveur de contrôle ;
- les services de contrôle de conformité fonctionnent généralement en mode SaaS (*software as a service*) et nécessitent donc que le poste nomade soit en mesure de contacter directement un serveur distant sur Internet. Cette contrainte contredit l'exigence de sécurité sur les flux sortants autorisés depuis les postes nomades, à la section 3.4.3 où il est recommandé de limiter au maximum les flux en dehors du tunnel VPN.

R15

Activer des mécanismes de mise en quarantaine et de remédiation pour les postes nomades non à jour des correctifs de sécurité

Il faut mettre en œuvre des mesures techniques permettant de bloquer temporairement toutes les connexions au SI interne de postes nomades non conformes à la politique de sécurité de l'entité. Il faut alors procéder à la mise à jour des postes nomades non conformes au moyen d'un ou plusieurs serveurs de remédiation (correctifs de sécurité, anti-virus, etc.) situés dans une zone isolée, au sein de la passerelle d'interconnexion par exemple.

3.3.9 Verrouillage du poste nomade

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

R16

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

La durée d'inactivité avant verrouillage automatique du poste nomade doit être un compromis entre la sécurité physique des situations de nomadisme et les besoins métier des utilisateurs. Il est recommandé que cette durée soit inférieure ou égale à 5 minutes.

3.4 Canal d'interconnexion

3.4.1 Schéma général

L'utilisateur connecte un poste nomade 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 le poste nomade et le SI interne de l'entité. Il est composé :

- d'un client logiciel situé sur le poste nomade (client *VPN*¹³);
- d'un tunnel d'interconnexion *VPN*;
- d'un équipement de terminaison *VPN* (nommé *concentrateur VPN* dans les schémas).

Tous les flux en provenance et à destination du poste nomade doivent être maîtrisés.

La figure 3 illustre une connexion à distance du poste nomade vers le SI de l'entité :

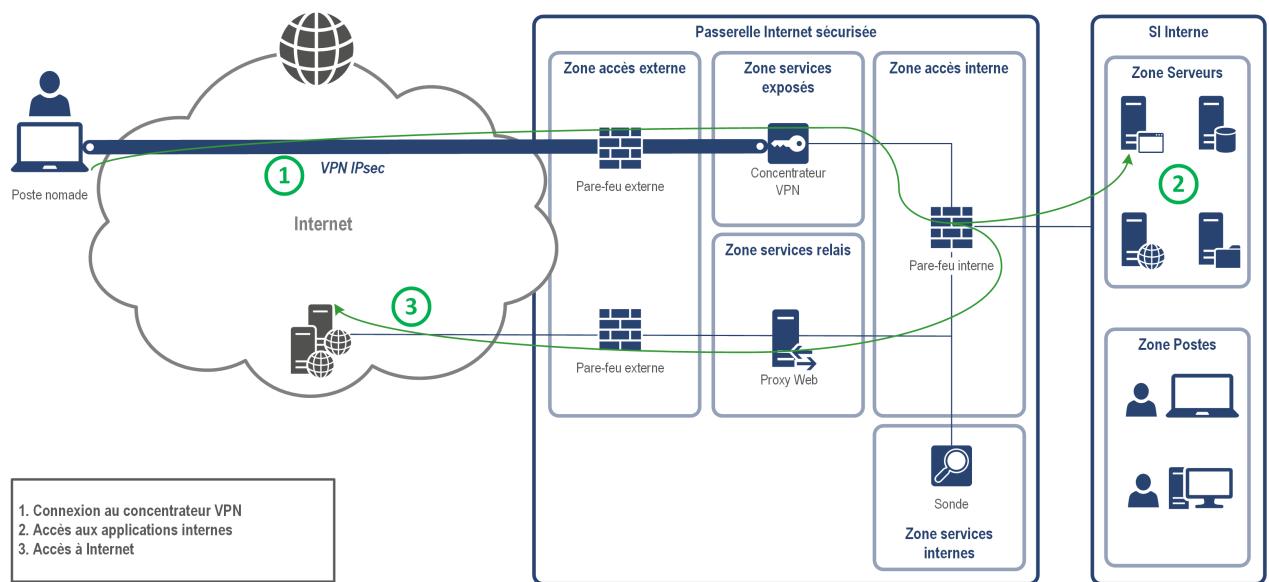


FIGURE 3 – Schéma général de connexion VPN nomade

Dans le schéma d'architecture présenté, l'entité met en place une passerelle Internet sécurisée comprenant plusieurs fonctions.

La première est une fonction dite « entrante » et elle est composée d'équipements de sécurité permettant la connexion de l'utilisateur nomade (concentrateur *VPN*, pare-feux externe et interne, etc.) au SI Interne. L'objectif de cette fonction est de sécuriser l'accès aux ressources internes de l'entité depuis des postes en situation de nomadisme.

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

Une fois que le tunnel VPN est établi, l'utilisateur nomade accède aux ressources internes de son entité (applications métiers dans la zone serveurs) mais il peut également accéder à Internet au moyen d'une fonction dite « sortante », disposant d'équipements de sécurité prévus pour cet usage (*proxy Web*, pare-feux externe et interne, etc.). L'objectif de cette fonction est de sécuriser l'accès à des ressources externes non maîtrisées par l'entité depuis les postes nomades (ressources Internet par exemple).

Enfin, des fonctions strictement internes à la passerelle, qui peuvent être des services d'infrastructure (annuaire, etc.) ou des services de sécurité (sonde de détection réseau, etc.), peuvent être mises en place dans la zone des services internes.

3.4.2 Technologie VPN

En fonction des moyens d'authentification mis en œuvre sur le poste nomade (cf. section 3.5), un attaquant peut tenter d'usurper l'identité de l'utilisateur ou celle du poste nomade. Mais l'attaquant peut également chercher à intercepter les communications entre le poste nomade 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 poste nomade.

Il est recommandé d'utiliser un VPN reposant sur le protocole IPsec configuré à l'état de l'art ou le protocole TLS configuré à l'état de l'art, pour la mise en place du lien sécurisé entre le poste nomade et l'équipement de terminaison centralisé.

Dans le cas où les besoins de sécurité sont importants, il est recommandé de privilégier le protocole IPsec plutôt que le protocole TLS. Il est possible de se référer au guide IPsec de l'ANSSI[19] pour avoir plus de détails sur le comparatif de ces deux protocoles.

R17

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

La solution VPN IPsec ou VPN TLS retenue doit être configurée à l'état de l'art, notamment les mécanismes de chiffrement et d'authentification mutuelle (se référer aux guides de l'ANSSI concernant les bonnes pratiques d'implémentation d'IPsec [19] et TLS [24]).

R17 +

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

Dans le cas où les besoins de sécurité sont importants, il est préférable de s'appuyer sur une technologie de VPN IPsec, ce dernier étant par nature plus résistant aux méthodes d'attaque les plus sophistiquées. Il est recommandé de se référer aux deux guides IPsec [19] et IPsec DR [2] de l'agence pour le choix ou l'implémentation de cette technologie.



Attention

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, et n'autoriser que les suites cryptographiques les plus robustes. L'utilisation de TLS 1.3 est un moyen de s'assurer que des suites cryptographiques obsolètes ne sont pas utilisées.

3.4.3 Maîtrise des flux réseaux sur le poste nomade

Il est possible que le SI interne de l'entité mette en œuvre des fonctions de filtrage réseau, sur les connexions entrantes et sortantes des postes nomades raccordés sur le réseau interne. De même, la configuration des commutateurs au sein de l'entité peut intégrer des fonctions tels que le *PVLAN*¹⁴ ainsi qu'une authentification des équipements grâce au protocole *802.1x*[10].

En situation de nomadisme, ces fonctions de sécurité n'existent généralement pas. Il faut donc impérativement protéger le poste nomade au moyen d'un pare-feu local. Cette préconisation est une bonne pratique générale, précisée dans le guide d'hygiène informatique [14], mais elle revêt ici un caractère *obligatoire* en environnement nomade.

L'objectif de sécurité doit permettre de s'assurer que l'ensemble des mesures de sécurité mises en place sur le poste nomade bloque toute connexion réseau :

- non-légitime, c'est-à-dire non prévue dans la définition des besoins métier de l'utilisateur ;
- non-nécessaire, c'est-à-dire non utile à l'établissement de la connexion au SI de l'entité ;
- non-sécurisée, c'est-à-dire ne mettant pas en œuvre des fonctions de chiffrement et d'authentification à l'état de l'art pour des informations transitant sur un réseau public (Internet) ou un réseau tiers non maîtrisé.

R18

Activer le pare-feu local sur le poste nomade

Il est indispensable d'activer le pare-feu local sur le poste nomade pour bloquer tous les flux entrants et sortants, autres que ceux strictement nécessaires à l'établissement de la connexion VPN vers le SI de l'entité et répondant à des besoins métier spécifiques.

La liste des flux autorisés doit être revue régulièrement, notamment pour supprimer les règles obsolètes.

L'utilisateur ne doit pas avoir la possibilité de désactiver ou de modifier la configuration du pare-feu local sur le poste nomade.

Cette recommandation doit être mise en lien avec les recommandations de la section 3.3.6 relative aux restrictions des droits utilisateurs sur les fonctions de connexion du poste nomade.

14. *Private VLAN* : technologie permettant notamment d'interdire les connexions directes entre les clients d'un même VLAN.

3.4.3.1 Cas d'usage du full-tunneling



Split-tunneling et Full-tunneling

Un équipement dit en *split-tunneling* est un équipement qui dispose d'un accès simultané à deux réseaux différents : un accès au réseau de l'entité (VPN) et un accès au réseau local de l'utilisateur nomade (et généralement par extension à Internet). L'expression *split-tunneling* indique que seuls les flux à destination du SI de l'entité sont routés vers le tunnel VPN, les autres flux sont routés au travers du réseau local du poste (par exemple des flux vers Internet).

L'expression *full-tunneling* signifie au contraire que tous les flux sont routés vers le tunnel VPN et qu'aucun flux ne peut être aiguillé vers une autre destination que la passerelle VPN.

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 en télétravail ne doit pas, depuis son poste nomade, naviguer directement sur le Web, utiliser une imprimante personnelle ou encore accéder à d'autres équipements informatiques personnels.

La figure 4 distingue les différents flux qui doivent être autorisés et interdits lors de la configuration du pare-feu local du poste nomade :

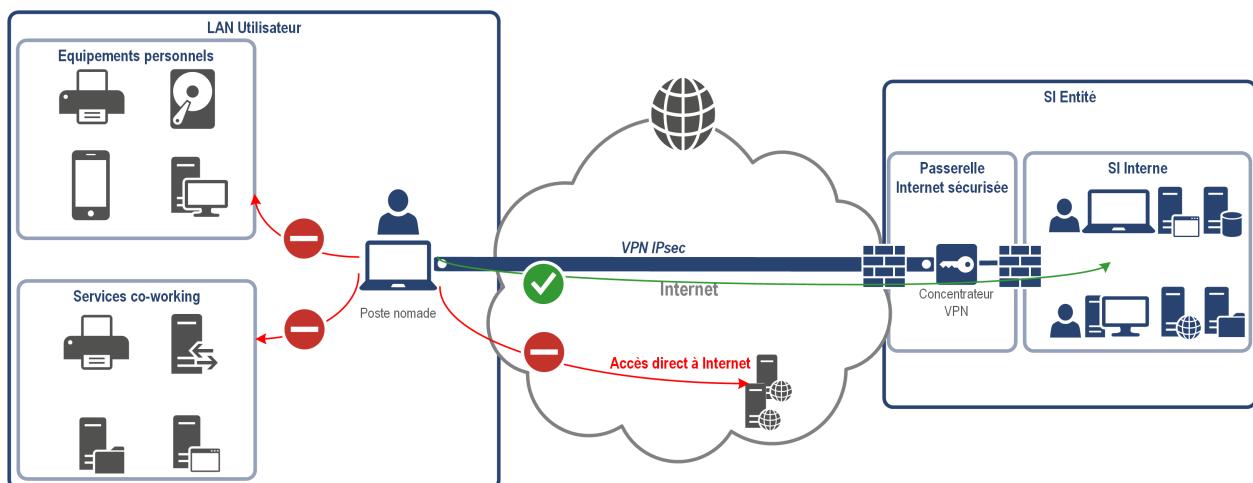


FIGURE 4 – Flux autorisés et interdits dans le cadre du nomadisme

Si le client VPN et le pare-feu local du poste nomade ne sont pas correctement configurés, ce poste est en mesure de faire du *split-tunneling* ce qui présente le risque d'une attaque directe depuis Internet, utilisant le poste nomade comme rebond vers le SI de l'entité.

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 généralement pas sécurisée par des équipements de filtrage (pare-feu, proxy, etc.).

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

Action	Sens	IP Source	Port Source	IP Dest	Port Dest	Type	Commentaire
Accepter	Sortant	Tous	68	Tous	67	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 1 – Exemple de configuration du pare-feu local d'un poste nomade avec VPN IPsec

Dans l'exemple de configuration présenté en table 1, les seuls flux autorisés sur l'interface réseau LAN du poste 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 (voir section 3.4.3.3).

R19

Interdire le split-tunneling sur le poste nomade et autoriser les seuls flux nécessaires pour monter le tunnel VPN

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

3.4.3.2 Cas d'usage du *split-tunneling*

Depuis plusieurs années, de plus en plus de fournisseurs d'applications métier et de services d'infrastructure proposent un hébergement en mode *SaaS*¹⁵, dans des environnements en nuage (*Cloud*). C'est le cas de suites bureautiques ou collaboratives (messagerie instantanée, visio-conférence, etc.) mais également de services techniques d'un SI comme par exemple des services de *proxy Web*.

De même, certains industriels et éditeurs s'appuyant sur une architecture *Zero Trust Network*[1] remettent en question le modèle de sécurité reposant sur la mise en œuvre de tunnels VPN en mode *full-tunneling*.

Si ces nouvelles offres peuvent paraître intéressantes sous certains aspects (financier, facilité de déploiement et de configuration), il convient d'analyser les risques et les impacts sous l'angle de la sécurité globale du SI, en n'omettant pas d'inclure dans l'analyse l'architecture de détection retenue, qui peut être centralisée (sondes réseaux), locale (EDR¹⁶) ou hybride.

L'intérêt de ces configurations repose notamment sur un accès plus *direct*¹⁷ aux applications métier depuis le poste nomade, afin de bénéficier de meilleures performances et d'une moindre latence. Ce besoin de performance en matière de latence peut se justifier notamment dans le cas d'applications « temps réel » comme les services d'audio-conférence et de visio-conférence, l'écriture collaborative de documents ou, dans une moindre mesure, les messageries instantanées.

Cependant, la mise en œuvre de cet accès direct implique l'activation du *split-tunneling* sur les postes nomades, ce qui entraîne les risques suivants :

15. *Software as a Service*

16. *Endpoint Detection and Response*

17. Un accès plus direct signifie ici que les paquets IP transitent par un nombre moins important d'équipements réseaux et de sécurité, ce qui peut avoir un impact sur la latence et le débit réseau.

- l'augmentation d'erreurs de configuration et l'hétérogénéité des configurations dans la gestion des autorisations de flux réseaux entrants et sortants du poste nomade, et une traçabilité des connexions plus compliquée à mettre en œuvre ;
- une exposition plus forte aux menaces en provenance d'Internet¹⁸ et des réseaux locaux (canal de contrôle commande, exfiltration de données, etc.) et un contournement des fonctions de détection et de protection centralisées dans le SI.

Dans le cas où la stratégie de détection est très centralisée, le *split-tunneling* peut abaisser la capacité de protection du poste nomade¹⁹. Il peut engendrer des dérives dans les autorisations de flux directs sur le pare-feu local des postes nomades et un manque de contrôle du niveau de sécurité de ces flux directs (suites cryptographiques dégradées par exemple). En outre, la mise en place du *split-tunneling* implique de s'assurer du bon fonctionnement et de la robustesse de son implémentation au sein du client logiciel VPN.



Attention

Dans le cas où les besoins de sécurité en confidentialité ou en intégrité d'un SI sont importants (p. ex. pour un SI DR au sens de l'II 901 [31]), la mise en place du *split-tunneling* est proscrite.

Le tableau 2 liste les prérequis à la mise en place du *split-tunneling*, en tentant de limiter les risques. Dans ce tableau, les services accessibles directement sur Internet qui ne transitent pas au travers du tunnel VPN sont appelés *services hors-tunnel* et les flux réseaux correspondants *flux hors-tunnel*.

ID	Règle
1	Les services hors-tunnel sont identifiés formellement et validés par les responsables de la sécurité de l'entité.
2	Les flux hors-tunnel sont protégés en confidentialité et sont authentifiés par des protocoles configurés à l'état de l'art (p. ex. en suivant le guide TLS [24] pour des flux HTTPS).
3	Les flux hors-tunnel doivent être filtrés en sortie sur le pare-feu local avec une liste d'adresses IP publiques restreinte au strict besoin opérationnel.
4	Le filtrage des flux hors-tunnel doit être fait par adresses IP (ou éventuellement par noms de domaine DNS) plutôt que par plages d'adresses IP (en fonction des préconisations de l'éditeur).
5	Le suivi des règles de filtrage local sur le poste nomade doit être le plus régulier possible et tenir compte des modifications des adresses IP publiques et des ports réseaux des services hors-tunnel.
6	Si le fournisseur d'un service hors-tunnel permet la configuration d'un proxy, cette fonction doit être activée afin de restreindre les adresses IP publiques de destination autorisées en sortie à ce seul proxy.
7	Si le fournisseur le propose, la phase d'authentification des utilisateurs aux services hors-tunnel doit transiter au travers du tunnel VPN et seuls les flux de données applicatives doivent transiter hors-tunnel une fois l'utilisateur authentifié ²⁰ .
8	Les fournisseurs des services hors-tunnel doivent proposer un niveau de journalisation aligné avec celui requis par la politique de sécurité de l'entité.
9	Toute modification non prévue de la configuration du <i>split-tunneling</i> (règles de filtrage, table de routage, client VPN) sur un poste nomade doit systématiquement déclencher la remontée d'une alerte aux administrateurs de sécurité de l'entité.
10	La route par défaut de la table de routage du poste nomade est l'adresse IP du concentrateur VPN. Les routes spécifiques des services hors-tunnel sont déclarées explicitement dans la table de routage.

TABLE 2 – Conditions d'application du *split-tunneling* sur un poste nomade

18. Cette menace est d'autant plus exacerbée que les attaquants utilisent parfois les mêmes services d'infrastructure de Cloud public que les entités pour y héberger temporairement leurs outils malveillants. Ainsi, autoriser le *split-tunneling* sur ces services peut faciliter le scénario de compromission de l'attaquant.

19. Cela ne signifie pas qu'une capacité de détection centralisée n'est pas pertinente, au contraire elle est nécessaire dans la majorité des contextes mais elle peut ne pas être suffisante dans le cas du *split-tunneling*

R19 -

Degradé À défaut - En cas d'usage du split-tunneling mettre en œuvre une configuration stricte visant à limiter les risques de compromission

Après analyse des risques, et à l'exclusion des SI d'administration, si la mise en place du *split-tunneling* sur le poste nomade est jugée acceptable, alors l'ensemble des conditions listées dans le tableau 2 doit être respectée.

Le respect des règles indiquées dans le tableau 2 implique que la navigation Internet depuis le poste nomade doit impérativement transiter par une fonction relais ou *proxy* de confiance, maîtrisée par l'entité ou un prestataire de l'entité, et à l'état de l'art au niveau de l'implémentation des protocoles de sécurisation (TLS). Un poste nomade ne doit donc jamais pouvoir accéder directement à des ressources web sur Internet.

R20 -

Degradé À défaut - N'autoriser la navigation Internet en split-tunneling sur le poste nomade que via un proxy de confiance

Dans le cas particulier de la navigation sur Internet, si l'entité fait le choix d'autoriser ces flux en *split-tunneling*, alors ces flux doivent impérativement transiter via une fonction *proxy*, qui peut être hébergée dans le SI interne de l'entité ou chez un prestataire. La configuration de ce proxy doit être sous la maîtrise de l'entité.



Attention

La mise en place du *split-tunneling* pour des administrateurs en situation de nomadisme est à proscrire, et ce, quel que soit le niveau de sensibilité du SI. En effet, les administrateurs disposent d'un niveau de privilège élevé sur le SI : l'accès à Internet est donc formellement proscrit sur leur poste d'administration, *a fortiori* à travers un mécanisme de *split-tunneling*.

3.4.3.3 Cas des flux DNS

Dans la liste des flux autorisés hors tunnel VPN, se pose la question de la résolution des noms de domaine publics liés aux concentrateurs VPN sur lesquels le poste nomade va établir une session sécurisée.

Il est fortement recommandé de ne pas autoriser de flux DNS pour la résolution de nom des concentrateurs VPN. En effet, l'autorisation de ce flux supplémentaire pourrait permettre à un attaquant de se faire passer pour le serveur cible²¹ (par une attaque de type empoisonnement du cache DNS²²) ou bien d'exfiltrer des données du poste nomade par une attaque dite *DNS tunneling*, en les faisant transiter par ce protocole ouvert sur Internet.

20. Cette mesure, si elle ne protège pas d'une compromission des données métier de l'entité, permet néanmoins de réduire le risque d'interception des secrets d'authentification des utilisateurs lors de l'accès aux services hors-tunnel. En outre, il est important d'avoir à l'esprit que cette mesure n'apporte pas non plus de protection supplémentaire contre la compromission des jetons d'authentification (*cookie* de session) utilisés une fois l'authentification établie.

21. Précisons néanmoins que pour usurper le concentrateur VPN cible, une usurpation DNS ne serait pas suffisante. Il faudrait en effet que l'attaquant compromette également les clés privées du concentrateur VPN utilisées pour réaliser l'authentification lors de l'établissement du tunnel en IPsec ou TLS.

22. Appelée aussi *DNS Cache Poisoning*.

Il faut donc privilégier l'utilisation de l'adresse IP du (ou des) concentrateur(s) VPN dans les paramètres du client VPN ou bien recourir à une résolution locale des noms des concentrateurs VPN (utilisation du fichier *hosts* sur le poste nomade).

R21

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

Il est recommandé de configurer le client VPN avec les adresses IP publiques des concentrateurs VPN de l'entité. Dans le cas où ce n'est pas possible, une résolution locale des noms des concentrateurs VPN peut être configurée sur le poste nomade (fichier *hosts*).

Toutefois, des raisons opérationnelles peuvent contraindre l'entité à recourir au protocole DNS pour résoudre publiquement les noms des concentrateurs VPN.

Plusieurs solutions sont possibles pour sécuriser le flux DNS si celui-ci est requis pour l'établissement du tunnel VPN. Parmi ces solutions, celle qui apporte le plus de garanties dans la maîtrise des risques consiste à implémenter son propre serveur DNS public. Ainsi, les postes nomades sont configurés pour n'envoyer des requêtes DNS uniquement à destination de ce serveur DNS maîtrisé. Ce service DNS peut être un service sous-traité à un prestataire, l'objectif étant de limiter au maximum les adresses IP de destination pour les requêtes DNS en provenance des postes nomades.

R21 -

Degradé À défaut - Sécuriser et maîtriser les flux DNS pour la résolution du nom du concentrateur VPN

Si l'utilisation de DNS est requise, il est conseillé de restreindre au maximum l'usage de la résolution DNS directement sur Internet, en utilisant un service DNS maîtrisé par l'entité ou par un prestataire de 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.



Attention

Dans un mode extrêmement dégradé, s'il n'est pas possible d'implémenter un service DNS propre à l'entité, l'entité peut faire le choix d'autoriser tous les flux DNS hors-tunnel, afin de résoudre le nom des concentrateurs VPN par n'importe quel serveur DNS public. Il faut bien prendre conscience que ce choix revient à autoriser tout flux réseau à destination du port 53 sur Internet, ce qui représente un risque conséquent, qui doit être assumé par les responsables de sécurité de l'entité.

Une fois le tunnel VPN établi, la configuration locale du poste nomade doit être modifiée automatiquement pour que toutes les résolutions DNS (publiques comme privées) soient réalisées en interne de l'entité, au travers du tunnel VPN.

3.4.3.4 Cas des flux DHCP

Tel que présenté dans la section précédente relative aux règles du pare-feu local 3.4.3.1, les flux DHCP font partie des flux à autoriser en sortie depuis le poste nomade. Si ces flux sont nécessaires afin que le poste nomade puisse obtenir une connectivité au réseau local IP, il est important de prendre en compte les risques inhérents à ce protocole.

En situation de nomadisme, l’entité n’a aucune maîtrise du service DHCP qui répond aux requêtes émises depuis le poste nomade. Ce service peut être un routeur d’un fournisseur Internet dans le cas du télétravail ou bien encore un équipement réseau commutateur dans le cas du *co-working* par exemple. Le protocole DHCP permet à un équipement de récupérer un nombre important d’informations de configuration de la part du serveur DHCP. La sécurité du poste nomade pourrait être impactée dans le cas où certaines de ces informations de configuration viendraient à être appliquées sur celui-ci en remplacement de la configuration standard de l’entité.

La liste suivante n’est pas exhaustive, mais elle présente les principales options reçues par un serveur DHCP qui pourraient présenter un danger pour le poste nomade :

- les serveurs de résolution de noms DNS ;
- les serveurs de temps NTP ;
- la fuseau horaire (*timezone*) ;
- le nom de machine (*hostname*) ;
- les noms de domaines.

Il est recommandé de ne pas appliquer les options ci-dessus renvoyées par le serveur DHCP dans la configuration du poste nomade. Cette mesure dépend des possibilités de configuration du client DHCP présent sur le poste nomade.

Dans un objectif de confidentialité des informations techniques du poste nomade, il peut également être pertinent d’appliquer les préconisations de la RFC 7844 permettant l’anonymisation des requêtes DHCP émises depuis le poste nomade (par exemple ne pas envoyer le *hostname* du poste dans la requête *DHCP Request*).

Le cas d’usage le plus couramment rencontré est l’envoi depuis le serveur DHCP des options de configuration des serveurs de noms DNS. L’application d’une configuration DNS non maîtrisée sur le poste nomade peut par exemple faire peser un risque de fuite d’informations via certains canaux.

La figure suivante présente un scénario d’attaque possible dans le cas où la politique de configuration des serveurs DNS en provenance du service DHCP (7.8.7.8) est appliquée sur le poste nomade en priorité vis-à-vis du serveur DNS légitime de l’entité (10.0.1.252). Dans ce scénario, la configuration du pare-feu local du poste nomade respecte les bonnes pratiques en n’autorisant que les flux DHCP hors-tunnel VPN.

Un défaut de configuration dans les fonctions de filtrage et de routage centralisées du SI de l’entité pourrait permettre au poste nomade d’émettre avec succès des requêtes DNS à destination d’un

serveur DNS public sur Internet. Ces requêtes DNS pourraient donc constituer un canal d'exfiltration de données pour un attaquant qui aurait pris le contrôle du serveur DNS ciblé. Le tunnel VPN n'apporte pas de protection spécifique dans ce scénario, les flux DNS étant autorisés au sein de celui-ci.

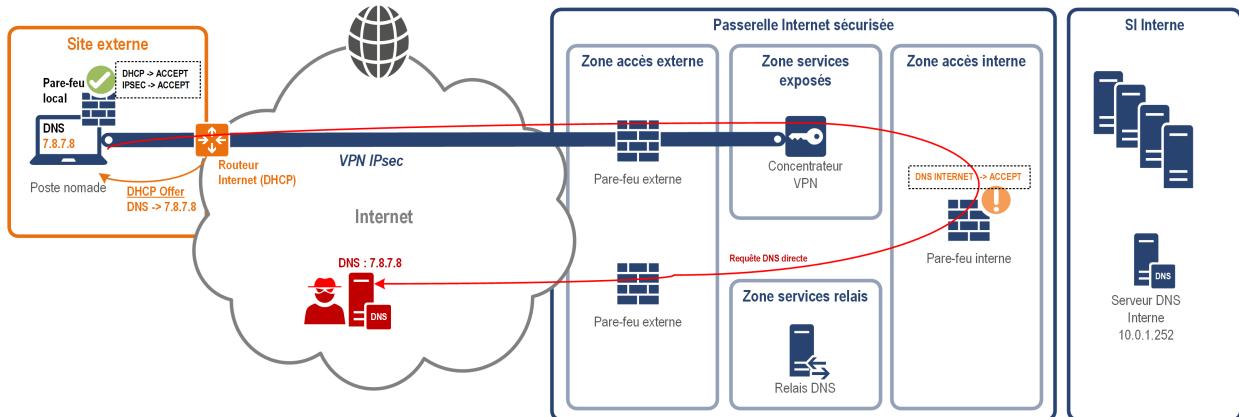


FIGURE 5 – Scénario d'attaque en lien avec un service DHCP

La figure suivante présente le scénario où le poste nomade est correctement configuré de manière à ne pas appliquer les informations de configuration DNS reçues par le serveur DHCP (7.8.7.8). Les flux DNS transitent donc vers le service DNS interne maîtrisé de l'entité (10.0.1.252), au sein du tunnel VPN. Celui-ci peut filtrer et éventuellement rediriger les requêtes si nécessaire vers un relais positionné dans la passerelle d'interconnexion à Internet.

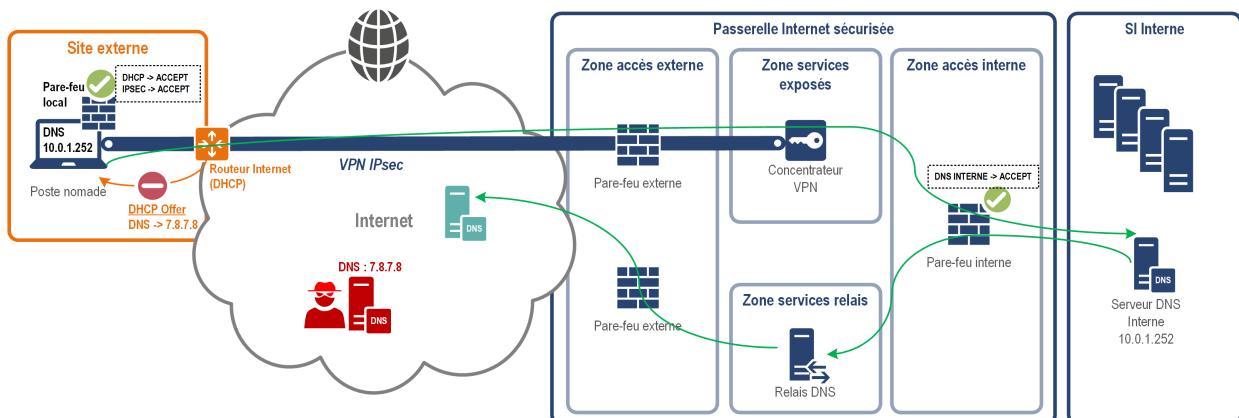


FIGURE 6 – Modèle sécurisé pour traiter les risques liés au service DHCP

L'entité ne peut pas avoir la maîtrise des serveurs DHCP en situation de nomadisme. En revanche, il est important que le client DHCP du poste nomade puisse être configuré de manière à ne pas tenir compte de toutes les informations de configuration reçues dans la réponse des serveurs DHCP.

Sauf cas d'usage très spécifique, le client DHCP doit uniquement traiter les informations suivantes en provenance du service DHCP :

- l'adressage réseau du poste nomade : l'adresse IP attribuée ainsi que le masque de sous-réseau ;
- l'adresse IP de la passerelle par défaut à contacter.

R22

Configurer le client DHCP pour restreindre au strict nécessaire les paramètres à appliquer sur le poste nomade

Il est recommandé de configurer le client DHCP du poste nomade de manière à ne récupérer que les informations strictement nécessaires à l'établissement de la connectivité réseau du poste nomade (adressage réseau et passerelle par défaut).

En particulier, il est important que les paramètres des serveurs DNS envoyés par le service DHCP ne remplacent pas les serveurs déjà configurés sur le poste nomade.

3.4.4 Portail captif

Le filtrage réalisé par le pare-feu local du poste nomade peut poser des problèmes dans le cas particulier d'un utilisateur voulant s'authentifier sur un portail captif, par exemple dans un hôtel ou dans certains transports publics. Dans ce cas, la restriction d'accès aux seuls services VPN de l'entité induit que le poste nomade ne peut pas se connecter au portail Web, puisque les requêtes HTTP et HTTPS sur les ports 80 et 443 sont bloquées.

Cependant, il est très risqué d'ouvrir de nouveaux ports dans ce cas particulier, puisqu'un filtrage strict ne peut être mis en œuvre sur les adresses IP de destination des portails captifs, celles-ci ne pouvant pas être connues à l'avance. Un accès direct vers un portail captif, c'est-à-dire sans filtrage réseau et sans *proxy*, suppose donc d'autoriser, même temporairement, toutes les requêtes HTTP et HTTPS sortantes depuis le poste nomade, ce qui présente un risque fort de compromission de ce dernier. Ce risque est d'autant plus fort que les portails captifs peuvent aussi faire l'objet d'attaques et être compromis²³. La recommandation R19 sur le filtrage strict des flux sur le poste nomade doit donc être appliquée, avec pour conséquence que tout accès à un portail captif est bloqué par le pare-feu du poste nomade.

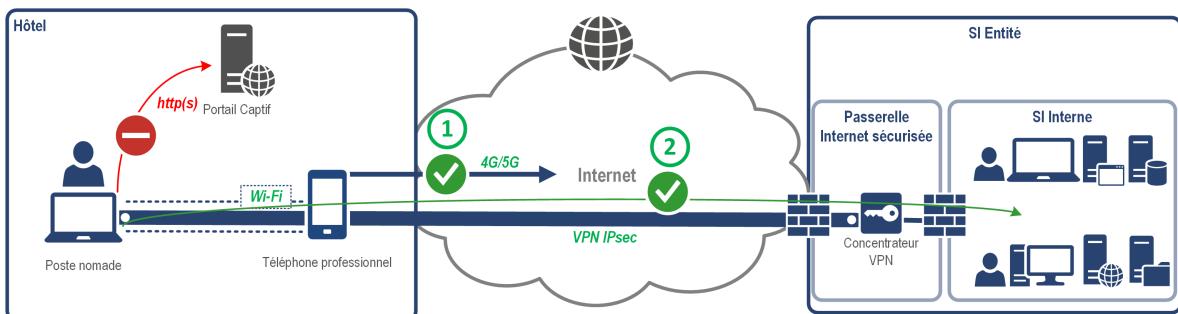
De nombreuses attaques sur des portails captifs, ciblées ou massives, ont fait l'objet de rapports d'investigation rendus publics, notamment concernant des compromissions au sein d'hôtels. Certains groupes d'attaquants profitent de vulnérabilités sur les bornes Wi-Fi peu ou mal mises à jour pour injecter du code malveillant dans les pages d'accueil du portail captif (via JavaScript par exemple). D'autres peuvent tenter d'usurper le SSID des bornes Wi-Fi légitimes et renvoyer les utilisateurs vers des sites malveillants. Il est donc nécessaire de considérer cette menace dans la stratégie de sécurisation du poste nomade.

La solution recommandée est de ne pas utiliser les portails captifs et de mettre à disposition des utilisateurs un autre moyen de connexion à Internet. Ce moyen peut être une connexion au réseau mobile (4G, 5G, etc.), soit intégrée au poste nomade (éventuellement avec une clé USB autorisée), soit via un partage de connexion d'un autre périphérique (téléphone professionnel).

L'intérêt de la mise en place d'un tunnel VPN est d'assurer un niveau de sécurité maîtrisé entre ce poste nomade et le SI interne de l'entité, ce qui permet de faire abstraction du niveau de sécurité des équipements réseaux intermédiaires de la chaîne d'accès. Si la connexion au concentrateur VPN est dépendante d'une action de configuration non maîtrisée et non sécurisée depuis le poste nomade, cela fait peser un risque non négligeable sur la protection du poste nomade en situation de nomadisme.

23. Ce type d'attaque par point d'eau ou *waterhole* est fréquemment utilisé dans le cas des portails captifs pour faire croire à l'utilisateur que la page Web affichée est légitime alors qu'elle ne l'est pas.

La figure 7 résume les flux autorisés et interdits dans le cas d'un accès alternatif à un portail captif :



1. L'équipement secondaire (téléphone professionnel) se connecte à Internet (4G/5G), puis partage sa connexion en Wi-Fi (ou USB).
2. Le poste nomade établit le tunnel VPN sur le concentrateur VPN, en utilisant le partage de connexion Internet de l'équipement secondaire.

FIGURE 7 – Connexion VPN à travers un réseau alternatif à un portail captif

R23

Bloquer l'accès aux portails captifs sur les postes nomades

Pour réduire les risques de compromission des postes nomades, il est fortement recommandé de bloquer tous les flux directs HTTP et HTTPS. Ceci a pour conséquence d'interdire l'utilisation des portails captifs.

3.4.5 Connexion des postes nomades en interne de l'entité

3.4.5.1 Risques liés au mode de connexion

Contrairement à une situation de nomadisme, où l'entité n'a pas la maîtrise des équipements permettant la connexion à un réseau d'accès (p. ex. la Box du fournisseur d'accès à Internet des utilisateurs), les postes nomades en interne se connectent généralement au moyen d'équipements réseaux gérés par l'entité (commutateurs, routeurs, bornes Wi-Fi, etc.).

Dans la plupart des entités, il est généralement possible de se connecter soit via un réseau sans-fil (Wi-Fi), soit via un réseau filaire (Ethernet). Certains usages métier peuvent nécessiter la présence de postes fixes filaires en interne de l'entité (poste de consultation, poste de visioconférence en salle de réunion, etc.)

Le niveau d'exposition est plus important dans le cas des réseaux sans-fil (attaques à distance possibles sans être forcément présent physiquement dans les bâtiments de l'entité) et il convient de traiter ce risque dans le cas de la connexion des postes présents en interne de l'entité.

Le présent guide n'a pas pour objet de détailler les risques liés au protocole Wi-Fi. Le lecteur est invité à se référer au guide de l'agence traitant ce thème pour avoir plus d'informations [18].

Cependant, lorsque les populations d'utilisateurs sont mixtes entre nomadisme et connexions fixes en interne, il peut être pertinent de mettre en place des mesures spécifiques pour sécuriser l'usage du Wi-Fi au sein de l'entité, comme par exemple :

- l'usage de protocoles d'authentification et de chiffrement des communications à l'état de l'art (WPA-Enterprise) ;

- la mise en place de 802.1x [10] pour améliorer l'authentification des équipements connectés aux réseaux locaux (Wi-Fi comme filaire);
- le cloisonnement des équipements de connexion (réseau, sécurité) entre l'usage Wi-Fi et l'usage filaire.

Certaines de ces mesures sont prises en compte dans les sections suivantes, afin d'une part de sécuriser la connexion des postes en interne de l'entité, d'autre part de protéger certains équipements de sécurité (p. ex. le concentrateur VPN) pouvant être exposés à des réseaux Wi-Fi (qui peuvent être la cible d'attaques depuis l'extérieur des locaux).

3.4.5.2 Risques liés à la détection de posture

Dans le cas où le poste nomade est utilisé aussi bien 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 permettent pas tous d'apporter un niveau de sécurité suffisant. Ces mécanismes permettent au client VPN de décider, en fonction de la situation de l'utilisateur, d'établir ou non la connexion au concentrateur VPN.

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 le poste nomade 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.

L'ensemble de ces considérations et des risques liés à un outil de détection de posture impliquent de réfléchir à d'autres architectures permettant d'assurer la sécurité des postes nomades connectés en interne.

3.4.5.3 Concentrateurs VPN internes

Pour ne pas avoir à dépendre de la fiabilité d'un outil de détection de posture, la préconisation est de généraliser le déploiement et l'utilisation de passerelles VPN aussi bien pour les usages nomade

ou interne. Cela implique la mise en place d'un ou plusieurs concentrateurs VPN internes, pour le cas où l'utilisateur se connecte à partir du SI interne de l'entité, depuis son poste 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.

Cette solution apporte deux principaux avantages. D'une part, elle simplifie l'architecture du SI de l'entité : tous les postes utilisateurs sont considérés comme des postes nomades. D'autre part, elle permet de ne pas avoir à gérer les risques liés à un SI interne qui serait trop ouvert par conception (pas ou peu de segmentation réseau, pas d'authentification 802.1x, etc.). En effet, le concentrateur VPN interne offre une fonction supplémentaire de filtrage et d'authentification avant l'accès aux ressources du SI interne.

La solution apporte également une simplification de la configuration du poste nomade 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 paramétrier 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, lorsque l'utilisateur est en situation de nomadisme interne, 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 noeuds 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 8 illustre le concept de mise en place de concentrateurs VPN distincts entre les usages interne et externe :

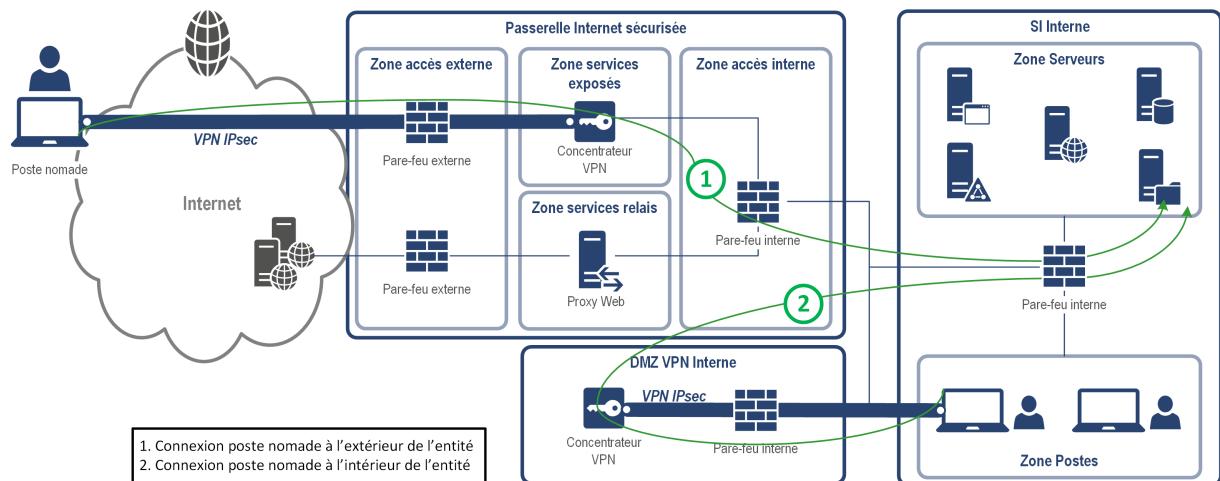


FIGURE 8 – Connexion VPN en interne et à l'extérieur du SI de l'entité à partir d'un poste nomade

R24

Généraliser l'emploi de concentrateurs VPN pour les usages nomade mais aussi interne à l'entité

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



Information

La distinction des concentrateurs VPN en fonction de l'usage (interne, nomade) doit aussi s'accompagner d'une distinction des secrets utilisés sur ces concentrateurs VPN (p. ex. les certificats pour l'authentification VPN, les secrets d'administration, etc.).

Les éléments présentés dans les sections précédentes permettent de définir l'architecture VPN adéquate en fonction de l'analyse de risque liée aux connexions d'utilisateurs nomades.

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 débrayé ou détourné 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 puisse pas être stoppé par l'utilisateur nomade.

Le mécanisme doit être lancé le plus tôt possible dans la séquence de démarrage du poste nomade, 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.

R24 -

Degrade À défaut - 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 les requêtes réalisées dans le cadre de ce contrôle doivent intégrer une fonction d'authentification robuste ;
- 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 ;
- l'outil doit être exécuté au plus tôt dans la séquence de démarrage du poste nomade.

3.4.5.4 Mutualisation des concentrateurs VPN

Dans le cas où l'on fait le choix de déployer des concentrateurs VPN internes, il est recommandé que ces équipements soient distincts des équipements traitant les connexions externes, notamment quand le niveau d'exposition des postes nomades diffère de manière significative entre ces deux situations.

Si l'on considère que les postes en situation de nomadisme présentent une exposition plus importantes aux attaques qu'en interne, il peut être pertinent d'avoir des concentrateurs VPN distincts pour chacun des usages.

Toutefois, le choix de distinguer les concentrateurs VPN pour les utilisateurs en fonction de leur situation (interne ou externe) dépend aussi et surtout de considérations relatives à un besoin en disponibilité. En effet, l'intérêt d'avoir deux concentrateurs VPN est d'une part d'assurer une répartition de la charge réseau, et d'autre part de pouvoir maintenir un accès aux utilisateurs en interne si jamais il faut déconnecter l'accès aux utilisateurs externes (et vice-versa).

R25

Dédier physiquement des concentrateurs VPN respectivement pour les connexions nomades et internes au SI

Il est recommandé que les concentrateurs VPN internes et externes reposent sur des socles physiquement dédiés à chaque usage.

Comme cela a été vu dans la section ci-dessus, les risques liés à l'usage de connectivité sans-fil (Wi-Fi) impliquent, dans une démarche de défense en profondeur, de cloisonner plus fortement les accès des postes nomades utilisant ce mode. L'objectif est ici de réduire la surface d'attaque d'un attaquant qui tenterait de compromettre une borne Wi-Fi de l'entité.

R25 +

Renforcé Dédier physiquement un concentrateur VPN pour les connexions internes en Wi-Fi

Il est recommandé de disposer de concentrateurs VPN distincts par mode de connexion (Wi-Fi et filaire). Ces concentrateurs VPN doivent dans tous les cas être positionnés dans une ou plusieurs DMZ cloisonnées du SI Interne et dédiées à la fonction VPN.

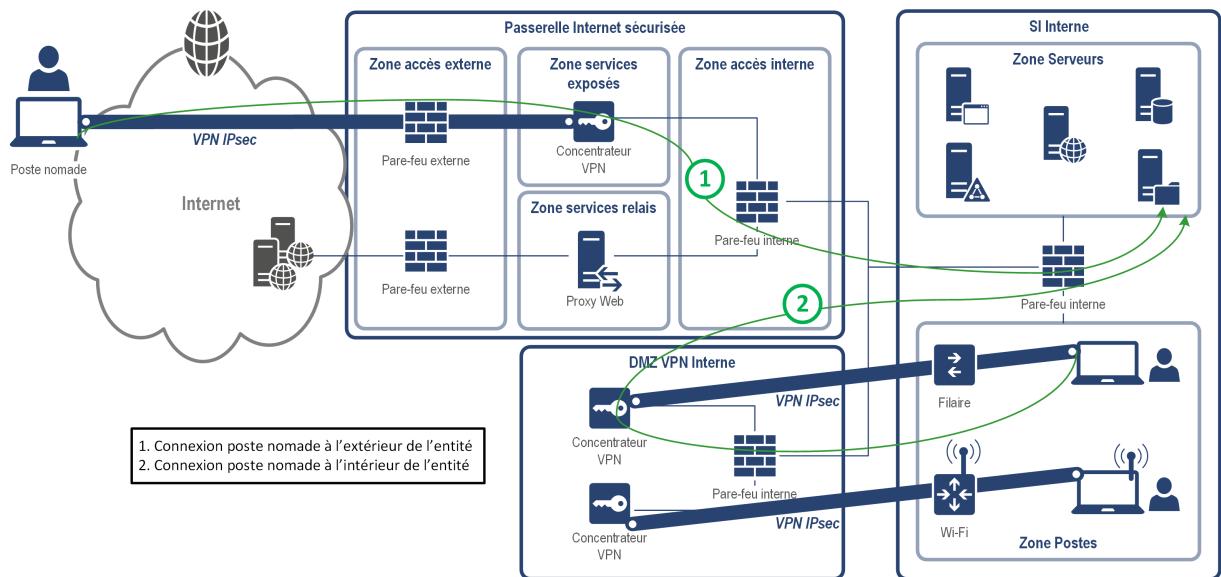


FIGURE 9 – Connexion VPN avec 3 concentrateurs VPN physiques : externe, filaire interne, Wi-Fi interne.

Dans le cas où l'entité décide de mutualiser plusieurs fonctions VPN sur un même socle physique, il est alors primordial que ces fonctions VPN soient au minimum cloisonnées logiquement par virtualisation. Cette solution dégradée a un impact sur la résilience du SI, puisque qu'un incident sur l'équipement physique (panne matérielle) englobe l'ensemble des connexions VPN des utilisateurs, internes comme externes.

R25 -

Degrado À défaut - Cloisonner logiquement par virtualisation les concentrateurs VPN mutualisés sur un même socle physique

En cas de mutualisation sur un même socle physique, les concentrateurs VPN doivent être cloisonnés par virtualisation (machines virtuelles ou *appliances* distinctes), afin de disposer de ressources et de configurations techniques propres à chaque usage.

Dans le cas où l'entité fait le choix très dégradé d'un unique concentrateur VPN pour l'ensemble des situations de l'utilisateur (interne et externe), la question se pose du chemin réseau à emprunter pour les utilisateurs internes. Deux possibilités sont offertes pour le routage des flux de connexion des postes nomades vers le concentrateur VPN :

- router directement sur une sortie Internet, afin d'accéder à la passerelle d'interconnexion depuis l'extérieur (cf. schéma figure 10);
- router vers le réseau interne, afin d'accéder à la passerelle d'interconnexion depuis l'intérieur (cf. schéma figure 11).

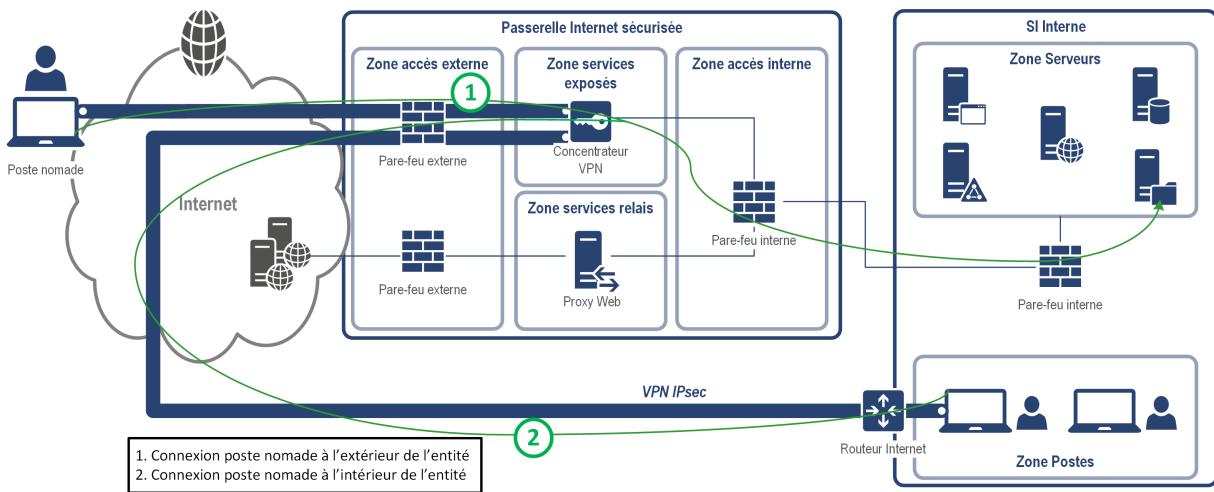


FIGURE 10 – Accès VPN interne et externe sur un même concentrateur VPN, avec routage via Internet des flux VPN internes

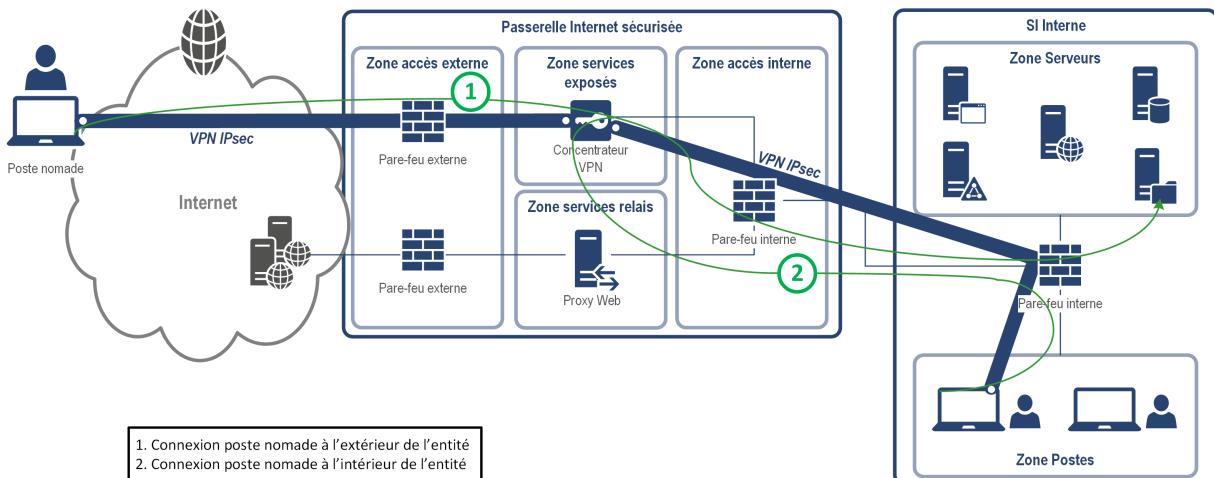


FIGURE 11 – Accès VPN interne et externe sur un même concentrateur VPN, avec routage interne des flux VPN internes

Ces deux options ont chacune des avantages et inconvénients, et doivent faire l'objet d'une analyse de risque, afin de décider de la plus pertinente pour l'entité.

Il est toutefois important d'avoir conscience que cette architecture avec un seul concentrateur VPN pose un problème de résilience et de disponibilité, en cas d'incident physique ou logiciel sur l'équipement. Cette architecture peut être complétée en mettant en place une redondance avec un second concentrateur VPN (mode actif-passif) ou bien une haute-disponibilité (mode actif-actif) si l'équipement le supporte. La configuration avec deux concentrateurs VPN redondés est dans tous les cas valable pour toutes les architectures décrites plus haut, lorsque le besoin en disponibilité est important.

3.4.5.5 Cas particulier d'une architecture VPN multi-sites

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

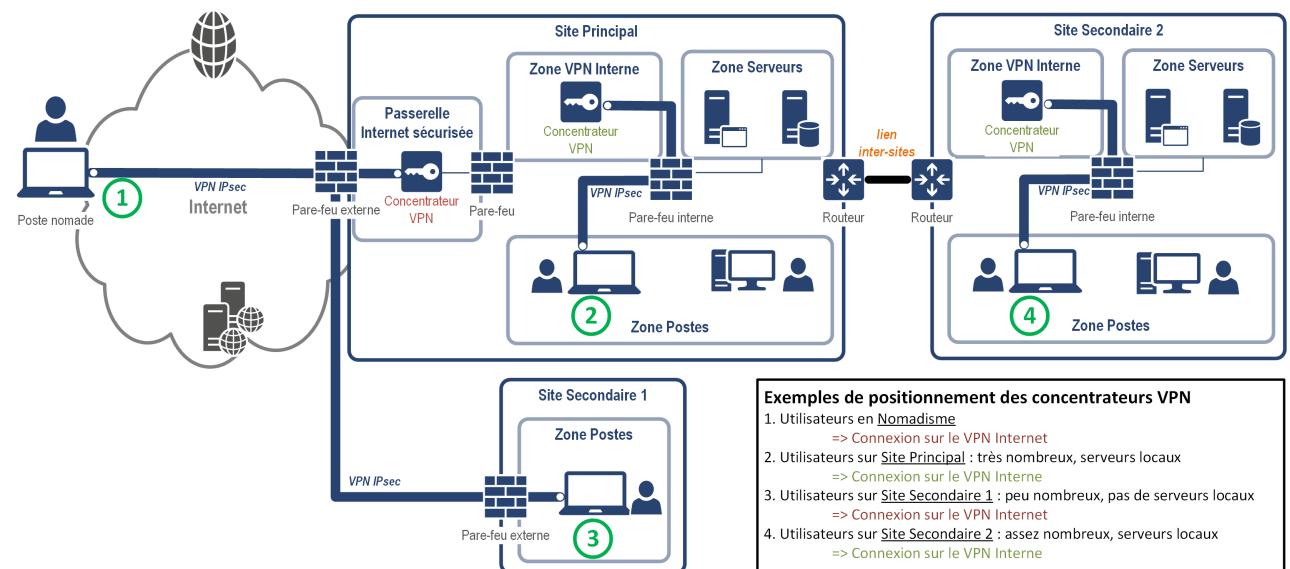


FIGURE 12 – Connexion VPN en interne et à l'extérieur du SI de l'entité dans le cas d'une entité multi-sites

3.5 Authentifications

3.5.1 Principes généraux

En situation de nomadisme, trois niveaux d'authentification doivent être considérés :

1. authentification de l'utilisateur sur le poste nomade ;
2. authentification du poste nomade sur le SI (passerelle d'interconnexion ou SI Interne) ;
3. authentification de l'utilisateur sur le SI (passerelle d'interconnexion ou SI Interne).

L'ANSSI a rédigé un guide spécifique relatif aux problématiques et enjeux autour de l'authentification. Ce guide traite en particulier de l'authentification avec mot de passe ainsi que de l'authentification multifacteur [33]. Ce chapitre a vocation à pointer les éléments structurants relatifs à l'authentification dans le cadre du nomadisme.

3.5.1.1 Authentification de l'utilisateur sur le poste nomade

L'objectif de sécurité de l'authentification de l'utilisateur sur le poste nomade est de garantir la protection de ce poste en cas de tentative d'accès illégitime en l'absence de l'utilisateur et également en cas de perte ou de vol de l'équipement.

Cette authentification va permettre de réduire le risque de piégeage logiciel du poste nomade et le risque d'atteinte en intégrité ou en confidentialité des informations stockées sur ce poste.

Cette authentification peut se faire de diverses manières, par exemple avec :

1. une carte à puce et un code *PIN* (authentification multifacteur) ;
2. le mot de passe du compte utilisateur lié à un annuaire central et dont le contrôle peut éventuellement être effectué par la présence d'un cache d'empreintes des mots de passe en local ;
3. le mot de passe d'un compte utilisateur local au poste nomade .

Quel que soit l'authentifiant, cet élément secret doit être personnel et seul l'utilisateur du poste nomade doit en avoir la connaissance ou le posséder.



Information

En complément des méthodes d'authentification énumérées ci-dessus, il est possible de prévoir une authentification supplémentaire permettant le déchiffrement du disque au démarrage du poste nomade. Cette authentification ne constitue toutefois pas une *authentification de l'utilisateur sur le poste nomade*. En effet, contrairement aux méthodes précédemment énumérées, le chiffrement du disque ne permet pas, à lui seul, de protéger le poste nomade lorsque celui-ci est démarré. Tel qu'indiqué dans la section 3.3.4, le chiffrement du disque vise, dans une logique de défense en profondeur, à protéger les données stockées d'accès illégitimes, mais seulement dans un scénario de perte ou de vol où le poste nomade est éteint.

R26

Authentifier l'utilisateur sur le poste nomade

Il est recommandé de mettre en place une authentification de l'utilisateur sur le poste nomade, par exemple au moyen d'un mot de passe ou d'une carte à puce avec un code PIN.

3.5.1.2 Authentification du poste nomade sur le SI

L'objectif de sécurité de l'authentification du poste nomade sur le SI est de garantir que le poste utilisé pour accéder au SI est un équipement maîtrisé par l'entité.

Cette authentification va permettre de réduire les risques qui résulteraient de l'utilisation de postes nomades non maîtrisés et dont le niveau de sécurité serait non conforme à la politique de sécurité de l'entité.

Le recours à un certificat machine pour authentifier le poste nomade est une bonne pratique. Ce certificat n'est pas lié à l'utilisateur du poste nomade. La clé privée associée à ce certificat doit être stockée de manière sécurisée (de préférence dans un composant matériel sécurisé comme un TPM) et sans que l'utilisateur nomade ait la capacité de l'exporter. Si cette clé privée est stockée sur le disque dur, celui-ci doit être chiffré, pour se prémunir du risque de récupération à froid²⁴ de cet élément secret par un attaquant (se reporter à la note d'information de la section 3.5.1.1).

R27

Authentifier le poste nomade sur le SI

Il est recommandé d'authentifier le poste nomade sur le SI au moyen d'un certificat machine. Il est également recommandé de protéger la clé privée de ce certificat en intégrité et en confidentialité, afin de s'assurer qu'elle ne puisse être accédée ni par l'utilisateur nomade ni par un attaquant.



Information

L'authentification du poste nomade sur le SI doit, dans la mesure du possible, être une authentification mutuelle : le poste nomade doit s'authentifier auprès d'un équipement de sécurité du SI et ce dernier doit également faire l'objet d'une authentification auprès du poste nomade, afin de s'assurer que l'équipement de sécurité du SI est bien légitime.

3.5.1.3 Authentification de l'utilisateur sur le SI

L'objectif de sécurité de l'authentification de l'utilisateur sur le SI est que l'utilisateur apporte la preuve de son identité, afin d'accéder aux ressources du SI auxquelles il est autorisé.

Ainsi, le service d'authentification de l'utilisateur sur le SI peut être mutualisé avec le service de gestion des autorisations d'accès aux ressources du SI. Les moyens les plus couramment utilisés au sein d'un annuaire sont les groupes ou rôles dans lesquels le compte utilisateur est ajouté. Cette mutualisation peut aussi prendre la forme d'attributs ajoutés dans le certificat de l'utilisateur.

24. c'est-à-dire tenter de lire les données du disque au moyen d'outils externes, ne nécessitant pas que le système d'exploitation du poste nomade soit démarré



Information

Tout utilisateur d'un SI sécurisé doit être authentifié avant de pouvoir accéder à des ressources du SI. Cette troisième authentification n'est donc pas spécifique aux situations de nomadisme. Cette authentification remplit les mêmes objectifs de sécurité que l'authentification inhérente à tout utilisateur souhaitant accéder au SI interne lorsqu'il se trouve dans les locaux de l'entité (notamment l'objectif de traçabilité).

R28

Authentifier l'utilisateur sur le SI

Il est impératif que l'utilisateur s'authentifie sur le SI, par exemple au moyen d'un mot de passe ou d'une carte à puce avec un code PIN. Cette authentification peut éventuellement être *mutualisée* avec l'authentification de l'utilisateur sur le poste nomade, dans le cas où la fonction permet la configuration d'un cache d'empreintes de mots de passe en local (p. ex. dans le cas d'un annuaire *Active Directory*).



Information

L'authentification de l'utilisateur sur le SI doit, au même titre que pour le poste nomade, être une authentification mutuelle : l'utilisateur doit s'authentifier auprès d'un équipement de sécurité du SI et ce dernier doit également faire l'objet d'une authentification auprès de l'utilisateur, afin de s'assurer que l'équipement de sécurité du SI est bien légitime.

3.5.2 Authentification multifacteur

3.5.2.1 Présentation

Un attaquant est susceptible d'usurper l'identité d'un utilisateur nomade si le processus d'authentification n'est pas suffisamment robuste ou si les secrets d'authentification ne respectent pas l'état de l'art²⁵.

Il est donc fortement recommandé, pour l'authentification de l'utilisateur nomade, de mettre en œuvre une authentification multifacteur forte²⁶, reposant sur deux secrets de catégories différentes parmi les suivantes :

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

Comme indiqué en début de chapitre, l'ANSSI a rédigé un guide qui traite notamment des authentifications multifacteur [33]. Il est donc recommandé de se référer à ce guide pour mieux appréhender les enjeux autour de ce sujet.

Quelques éléments de réflexion sont toutefois spécifiés ci-après, afin de faciliter la lecture du document. Cette section est ainsi une synthèse des points structurants à retenir dans le cadre du nomadisme et n'a pas vocation à être exhaustive sur le sujet de l'authentification multifacteur.

25. À cet égard, il est recommandé de viser une conformité au référentiel général de sécurité [30].

26. La notion d'authentification multifacteur forte (ou robuste) est expliquée dans le guide [33].

3.5.2.2 Cas particulier de la biométrie

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 relativement aisé pour un attaquant d'obtenir les empreintes d'un individu et d'en créer des copies qui seront perçues comme valides par le système authentifiant.

Quand bien même une telle usurpation serait détectée, il serait impossible, à la différence d'un certificat ou d'un mot de passe, de révoquer l'accès. En effet, cela reviendrait à révoquer l'accès de l'utilisateur légitime dans la mesure où ses facteurs biométriques sont inchangeables. Cela nécessiterait donc d'assumer le risque d'usurpation en attendant qu'une mise à jour corrige la vulnérabilité et que le système n'accepte plus les copies illégitimes.

Il est donc recommandé d'utiliser les deux facteurs *ce que je sais* et *ce que je possède* lorsqu'une authentification multifacteur est mise en œuvre dans un contexte de nomadisme numérique. L'utilisation de la biométrie seule est à proscrire.

3.5.2.3 Technologies d'authentification multifacteur dans le cas du nomadisme

Les moyens les plus répandus pour réaliser une authentification multifacteur forte d'un utilisateur en situation de nomadisme sont :

- l'usage d'une carte à puce disposant d'un composant de sécurité et d'un code *PIN* d'authentification ;
- l'usage d'un code temporaire *OTP*²⁷ généré à la demande sur un équipement professionnel différent de celui réalisant l'authentification (le téléphone professionnel de l'utilisateur dans le cas d'une authentification sur un PC portable par exemple) ;
- l'usage d'un *token* physique (disposant d'un composant de sécurité) reposant sur la norme FIDO2/U2F et d'un code *PIN* d'authentification.

Les moyens suivants sont à éviter dans la mesure du possible :

- l'envoi d'un SMS sur le téléphone professionnel, le protocole de signalisation n'étant pas considéré comme sécurisé ;
- l'utilisation d'une carte à puce ou d'un *token* physique dépourvu d'un composant de sécurité (par exemple, une clé privée copiée sur une clé USB standard et dont l'accès est protégé par une *passphrase* ne saurait constituer une solution suffisamment robuste) ;
- l'utilisation d'une solution technique multifacteur (application spécifique, code temporaire *OTP*) qui serait implémentée et présentée à l'utilisateur *sur le même équipement que celui qui réalise l'authentification* (le facteur de possession n'est alors pas *indépendant* du poste nomade à l'origine de la connexion).

3.5.2.4 Cas d'usage de l'authentification multifacteur

Cette authentification multifacteur peut avoir lieu lors de la première phase d'authentification au démarrage du poste nomade, ou bien lors de la connexion au concentrateur VPN, ou encore lorsque l'utilisateur souhaite accéder au SI Interne.

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

Ce choix dépend de la compatibilité des produits de sécurité utilisés, de la robustesse de l'implémentation de la fonctionnalité de multifacteur et également du niveau de confiance que l'on peut avoir sur les utilisateurs en situation de nomadisme. En effet, si les utilisateurs ou les postes nomades des utilisateurs ne sont pas jugés d'une confiance suffisante, il est pertinent que l'authentification multifacteur soit réalisée le plus tôt possible dans la cinématique d'authentification. De cette manière, les possibilités de l'attaquant sont contraintes au maximum dès la première barrière de connexion²⁸.

R29

Mettre en place une authentification multifacteur forte pour l'utilisateur nomade

Il est recommandé de mettre en place une authentification multifacteur pour l'utilisateur nomade. Elle peut être implémentée par différents moyens (carte à puce, OTP sur un téléphone mobile, etc.) et à différentes étapes de l'authentification (ouverture de session, connexion au VPN, etc.).

28. Par exemple, un attaquant qui aurait réussi à compromettre complètement le poste nomade d'un utilisateur devrait néanmoins attendre que celui-ci soit authentifié en multifacteur, afin de pouvoir utiliser le canal de connexion ouvert pour accéder au SI. Il ne pourrait donc pas se contenter de compromettre le mot de passe de l'utilisateur pour le réutiliser et agir de manière plus indépendante.

3.5.3 Modèles d'authentification en nomadisme

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

- l'utilisateur sur le poste nomade ;
- le poste nomade sur la passerelle d'interconnexion ou le SI Interne ;
- l'utilisateur sur la passerelle d'interconnexion ou le SI Interne.

Il est donc important, d'une part que ces trois étapes soient présentes dans le modèle d'authentification retenue, et d'autre part qu'il y ait au moins une des deux authentifications de l'utilisateur qui soit une authentification multifacteur.

Par souci de concision et de clarté, ces trois types d'authentification seront respectivement désignées par la suite « authentification 1 », « authentification 2 » et « authentification 3 ».

Plusieurs modèles sont possibles pour gérer ce processus d'authentification en situation de nomadisme. Il peut être envisageable de faire reposer une partie des authentifications sur le concentrateur VPN, mais en s'assurant que les protocoles utilisés sont jugés suffisamment robustes et que le produit retenu supporte les fonctionnalités requises (p. ex. authentification multifacteur).

Dans une démarche de défense en profondeur, il est pertinent de rechercher une diversité technologique et de répartir le processus d'authentification sur des composants techniques issus de différents constructeurs. Ce faisant, une vulnérabilité affectant l'un de ces composants ne provoque pas la compromission de l'ensemble du modèle d'authentification.

Dans le cas où les besoins de sécurité sont importants, il est également possible d'ajouter une barrière supplémentaire de sécurité, par exemple par la mise en œuvre d'un service d'authentification dédié, qui serait positionné en coupure entre le concentrateur VPN et le SI interne. Ce serveur d'authentification peut prendre la forme d'un portail Web d'authentification avec un dépôt d'affichage.

Les exemples suivants traitent de modèles d'authentification rencontrés usuellement en situation de nomadisme. Ces exemples n'ont pas vocation à être exhaustifs mais visent à illustrer le propos de ce chapitre. Pour chacun des scénarios, un texte explique les enjeux de sécurité et permet de mettre en lumière les points forts et les faiblesses de l'architecture. Ces exemples présentent les étapes d'authentification en situation de nomadisme, à partir de l'instant où le poste nomade démarre.

3.5.3.1 Modèle d'authentification A

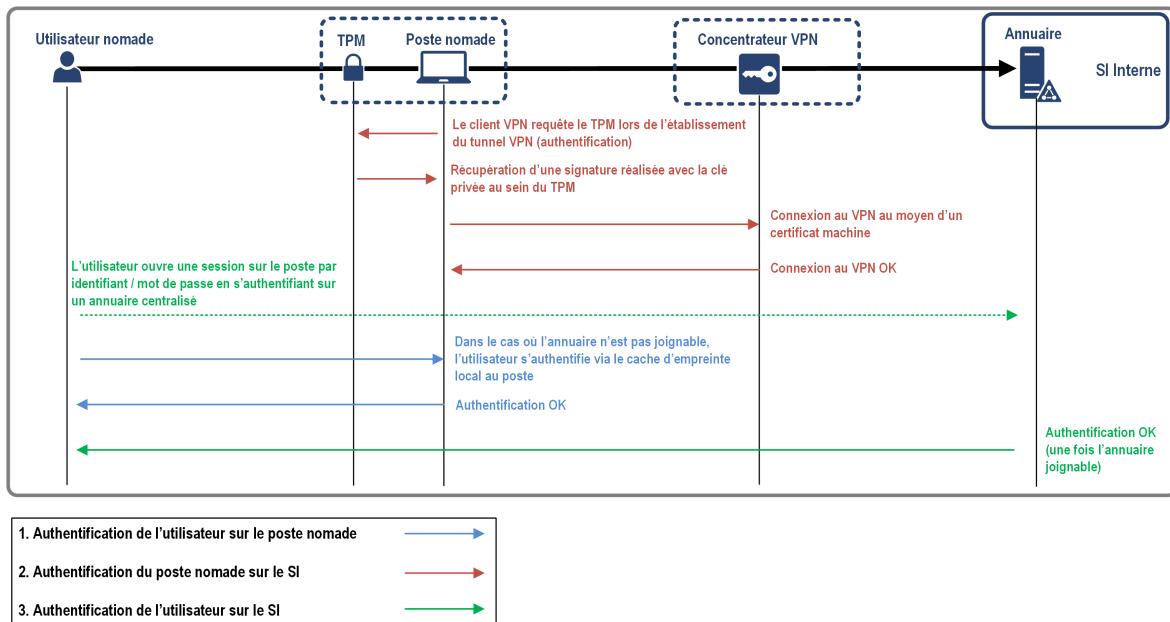


FIGURE 13 – Modèle d'authentification A

Dans ce modèle d'authentification A, le poste nomade dispose d'un OS Microsoft Windows. L'authentification 1 est assurée par la saisie du mot de passe du compte utilisateur lié à un annuaire centralisé (*Active Directory*) et dont le contrôle est effectué localement par la présence d'un cache d'empreinte des mots de passe sur le poste dans le cas où l'annuaire n'est pas joignable (par exemple si la connexion au tunnel VPN n'est pas encore effective).

L'authentification 2 est faite de manière totalement transparente pour l'utilisateur : au démarrage du système d'exploitation, le service VPN est configuré avec une clé privée stockée dans le TPM²⁹ et initie la négociation conduisant à l'établissement d'un canal VPN. Les opérations cryptographiques d'authentification avec la clé privée restent confinées au sein du TPM.

Deux cas de figure peuvent être rencontrés concernant l'authentification 3 suivant que l'annuaire centralisé est accessible ou n'est pas accessible au moment où l'utilisateur saisit son mot de passe :

- l'annuaire est accessible : l'authentification 3 et l'authentification 1 sont concomitantes ;
- l'annuaire n'est pas accessible : l'authentification 1 est réalisée en premier lieu et l'authentification 3 est faite ultérieurement, de manière transparente pour l'utilisateur, lorsque l'annuaire devient accessible (tunnel VPN établi).

Au delà de la sécurité, la proposition est intéressante d'un point de vue ergonomique car l'établissement de la connexion VPN est automatique dès le démarrage du poste nomade. En conséquence, il est fort probable que le tunnel soit déjà monté lorsque l'utilisateur achèvera l'ouverture de sa session sur le poste nomade. L'accès aux ressources du SI interne sera quasi-immédiat (succès de l'authentification 3).

29. Un certificat machine est associé à cette clé privée.



Avis

Ce modèle présente un niveau de sécurité acceptable, notamment par la mise en œuvre d'un TPM qui protège le secret du certificat machine nécessaire à l'établissement du tunnel VPN (authentification 2).

Ce modèle ne met cependant pas en œuvre de mécanisme d'authentification multifacteur pour l'utilisateur. Cette faiblesse est d'autant plus dommageable que les authentifications 1 et 3 reposent sur le même secret.

3.5.3.2 Modèle d'authentification B

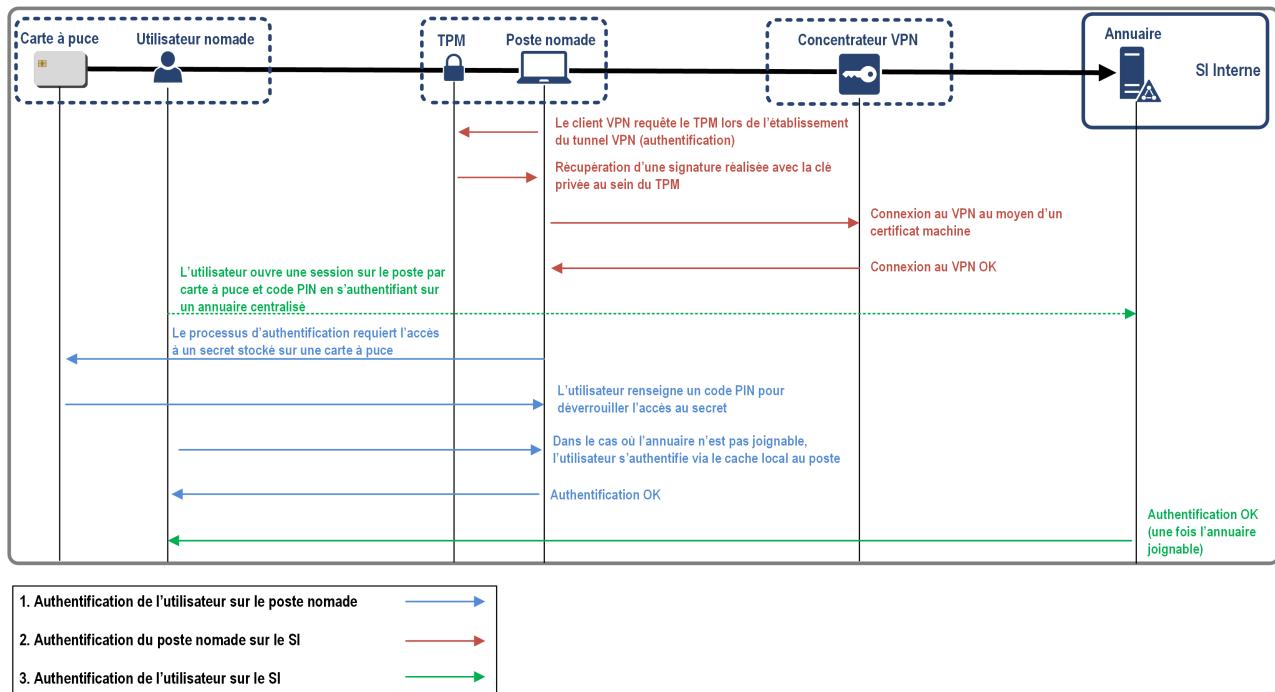


FIGURE 14 – Modèle d'authentification B

Le modèle d'authentification B est une variante du modèle A (cf. figure 13), toujours avec un poste nomade Windows. La seule différence avec ce dernier est l'ajout d'un composant carte à puce permettant à l'utilisateur de réaliser une authentification multifacteur pour les authentifications 1 et 3 : lors de la phase d'authentification, l'utilisateur renseigne un code PIN permettant de déverrouiller l'accès à la clé privée présente dans la carte à puce. Cette clé privée est liée au certificat de l'utilisateur, l'ensemble permettant de réaliser l'authentification sur l'annuaire *Active Directory*.

Le système de cache d'empreinte local au poste nomade est compatible avec l'authentification par carte à puce dans un environnement *Active Directory*³⁰.

L'authentification 2 est équivalente au modèle A (cf. figure 13), avec l'utilisation d'un certificat machine et de sa clé privée dans un TPM pour l'authentification sur le concentrateur VPN.



Avis

Ce modèle compense la faiblesse du modèle précédent, par la mise en place d'une authentification multifacteur de l'utilisateur au moyen d'une carte à puce et d'un code PIN. Elle répond donc au risque d'une compromission du mot de passe de l'utilisateur utilisé dans les authentifications 1 et 3, et apporte les garanties de sécurité suffisantes pour contrer une menace de type cybercriminelle.

30. L'utilisation de carte à puce sur les systèmes Windows n'empêche pas les attaques de type *pass-the-hash* ou *pass-the-ticket*. Il est important que des politiques de sécurité soient correctement définies sur *Active Directory* concernant l'utilisation des cartes à puce. Cette politique décrit notamment la mise en place d'une rotation régulière des mots de passe aléatoires générés automatiquement et liés aux comptes utilisateurs (se référer au guide suivant[3])

3.5.3.3 Modèle d'authentification C

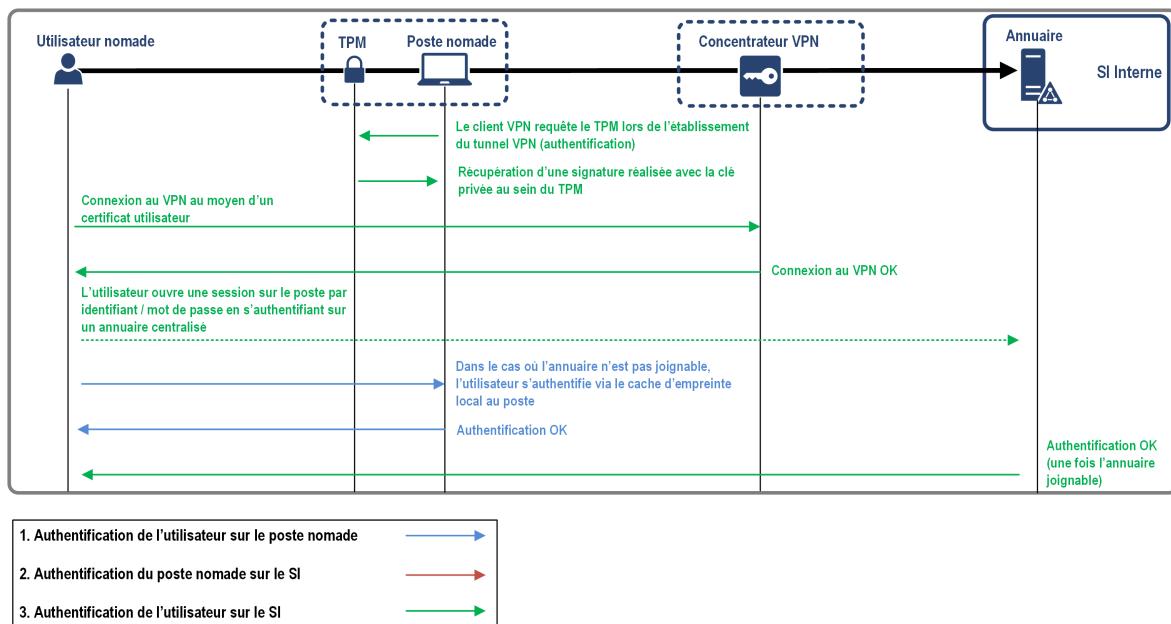


FIGURE 15 – Modèle d'authentification C

Le modèle d'authentification C est également une variante du modèle A (cf. figure 13) en environnement Windows. La seule différence se situe dans la configuration du client VPN, où un certificat utilisateur est paramétré en lieu et place d'un certificat machine (authentification 2)³¹.

Les authentifications 1 et 3 sont les mêmes que pour le modèle A (cf. figure 13), avec l'utilisation d'un système de cache d'empreintes local lors de l'ouverture de la session utilisateur sur le poste nomade et l'authentification *implicite* aux ressources du SI interne lorsque l'annuaire centralisé est joignable.



Avis

Le niveau de sécurité de ce modèle est affaibli en comparaison du modèle A. En effet, un certificat utilisateur et sa clé privée associée sont plus facilement récupérables par un attaquant ou même par l'utilisateur lui-même, que dans le cas d'un certificat machine où l'accès nécessite des priviléges d'administrateur local sur le poste nomade. Une personne mal intentionnée serait donc susceptible d'extraire et de copier ces éléments sur un poste de travail non maîtrisé (ex : poste personnel), afin de s'authentifier sur le concentrateur VPN et ainsi de disposer d'un accès au réseau de l'entité³².

31. Dans un environnement Windows, cette configuration se concrétise par l'ajout du certificat dans le magasin utilisateur plutôt que dans le magasin système.

32. Des mesures de sécurité palliatives peuvent toutefois être configurées sur le poste nomade pour empêcher l'export des secrets liés aux certificats utilisateurs (en positionnant l'option *non-exportable* dans les gabarits Windows par exemple).

3.5.3.4 Modèle d'authentification D

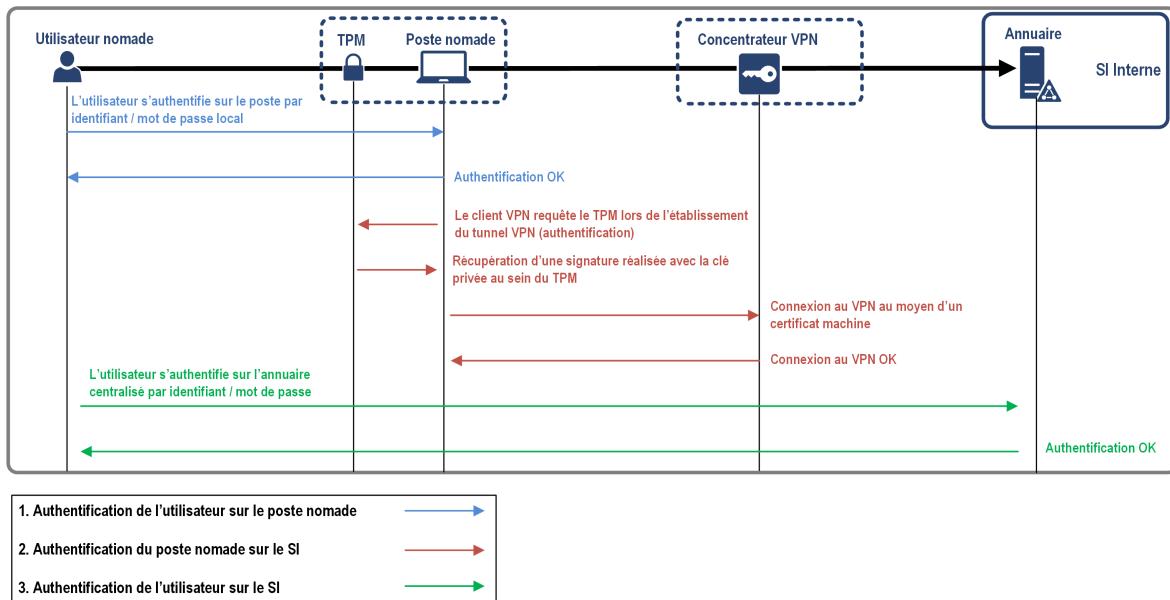


FIGURE 16 – Modèle d'authentification D

Ce modèle d'authentification D différencie ici l'authentification 1 et l'authentification 3. Elle est usuellement mise en place dans les environnements Linux, où l'utilisateur s'authentifie d'abord sur son poste nomade au moyen d'un compte local (authentification 1), puis s'authentifie, après établissement du tunnel VPN, sur un annuaire du SI interne (authentification 3). Cette authentification 3 peut, par exemple, être réalisée au moyen d'un serveur *Active Directory*, ou bien en installant un royaume *Kerberos* sur Linux, ou encore avec un serveur *OpenLDAP*.

L'authentification 2 est équivalente à celle du modèle A (cf. figure 13), avec l'utilisation d'un certificat machine et de sa clé privée dans un TPM pour s'authentifier sur le concentrateur VPN.



Avis

Ce modèle est légèrement meilleur que le modèle A d'un point de vue sécurité. Les authentifications 1 et 3 sont complètement indépendantes et les secrets utilisés sont – en théorie – différents. En revanche, l'absence d'authentification multifacteur affaiblit la solution et n'est pas contre-balancée par la nécessité, pour l'attaquant, de devoir compromettre deux secrets plutôt qu'un seul.

3.5.3.5 Modèle d'authentification E

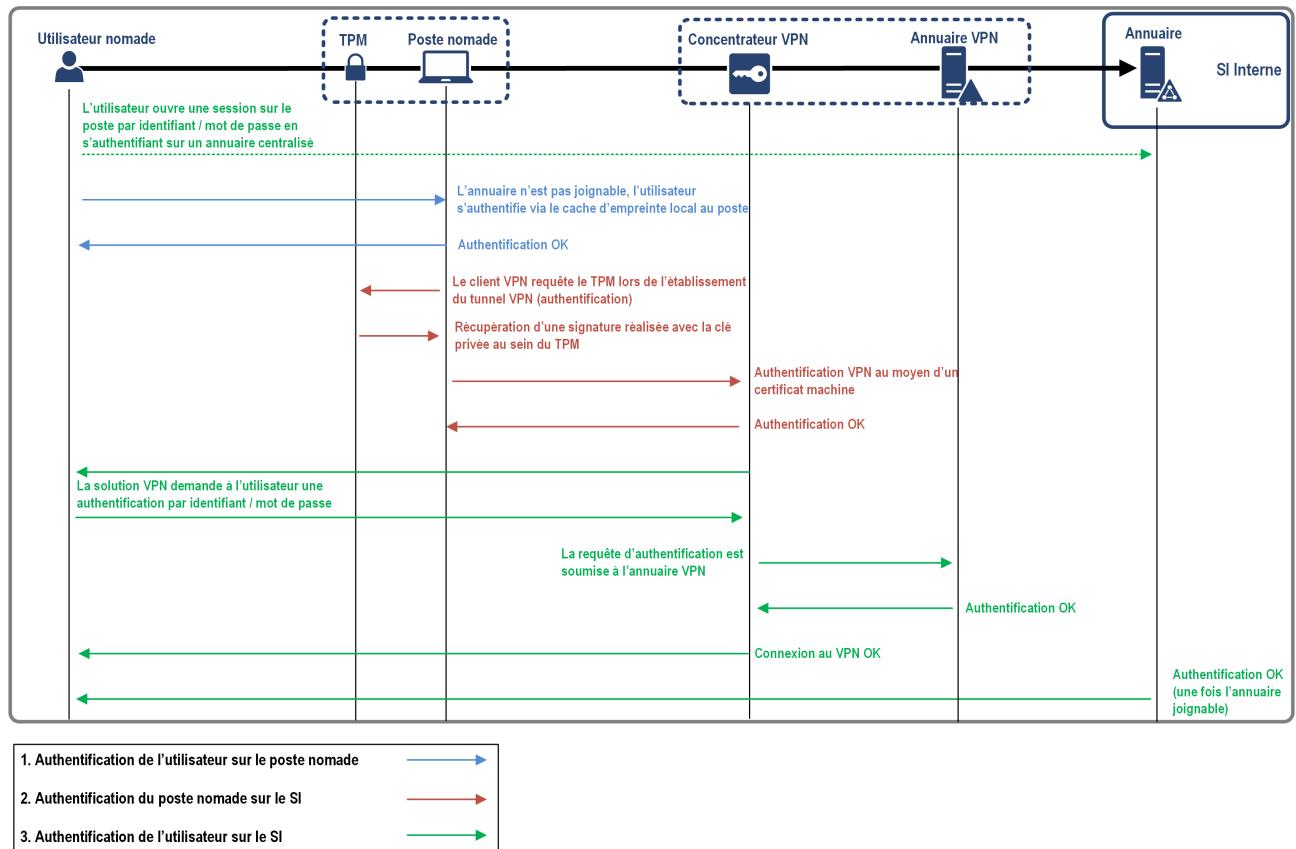


FIGURE 17 – Modèle d'authentification E

Ce modèle d'authentification E est également une variante du modèle A (cf. figure 13) avec un poste nomade Windows. Elle renforce la phase d'authentification sur le concentrateur VPN en y ajoutant une demande d'authentification par mot de passe utilisateur. Cette authentification est complémentaire de l'authentification avec le certificat machine. Elle n'est compatible qu'avec certains produits de sécurité et implique l'installation d'un annuaire supplémentaire, dédié aux accès nomades.

Les authentifications 1 et 3 sont de même nature que celles du modèle A (cf. figure 13), avec l'utilisation d'un cache d'empreintes local lors de l'ouverture de la session utilisateur sur le poste nomade et l'authentification *implicite* aux ressources du SI interne lorsque l'annuaire centralisé est joignable.



Avis

Ce modèle présente l'avantage de complexifier la tâche d'un attaquant qui tente d'accéder au VPN. Cette première barrière nécessite deux authentifications consécutives. Toutefois, ces deux authentifications sont moins robustes qu'une authentification multifactor : un attaquant qui aurait compromis le poste nomade pourrait récupérer les deux secrets : certificat machine et mot de passe de l'utilisateur. L'autre avantage de ce modèle est qu'il repose sur deux annuaires distincts, un dédié à l'authentification VPN et l'autre à l'authentification sur le SI interne.

3.5.3.6 Modèle d'authentification F

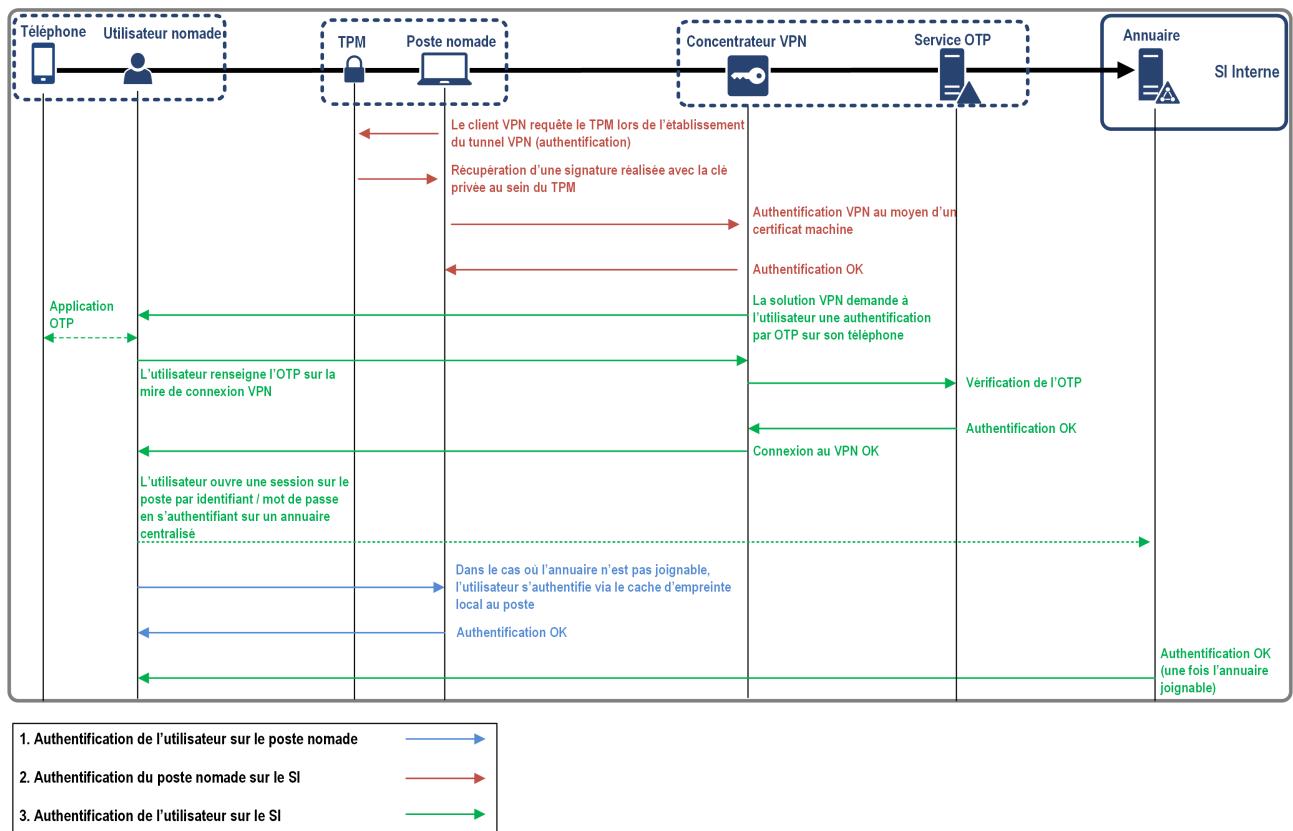


FIGURE 18 – Modèle d'authentification F

Le modèle d'authentification F est une variante du modèle E (cf. figure 17) avec un poste nomade Windows. La seule différence réside dans la configuration du client VPN, où une authentification multifacteur est implémentée au moyen d'une fonction OTP sur le téléphone professionnel de l'utilisateur.

Cette authentification se fait donc en complément de l'authentification avec le certificat machine. Elle implique la configuration d'un composant logiciel supplémentaire pour gérer l'enrôlement des terminaux mobiles et la génération de secrets temporaires (OTP).

Les authentifications 1 et 3 sont de même nature que celles du modèle A (cf. figure 13), avec l'utilisation d'un cache d'empreintes local lors de l'ouverture de la session utilisateur sur le poste nomade et l'authentification *implicite* aux ressources du SI interne lorsque l'annuaire centralisé est joignable.

Avis

Ce modèle compense la faiblesse du modèle E, par la mise en place d'une authentification multifacteur de l'utilisateur au moyen d'un code à usage unique (OTP) sur un équipement distinct (téléphone professionnel). Cela répond au risque d'une compromission du mot de passe utilisé par l'utilisateur pour se connecter au concentrateur VPN. Il faut bien s'assurer que le facteur de possession (téléphone professionnel) pour l'authentification multifacteur est bien sous la maîtrise de l'entité.

3.5.4 Infrastructure de gestion de clés

Il est fortement conseillé de recourir à des certificats pour la mise en œuvre de solutions VPN IPsec ou VPN TLS, ainsi que pour la fonction de chiffrement des disques du poste nomade.

Il est donc nécessaire de se reposer sur une infrastructure de gestion de clés (IGC) pour la gestion de ces certificats.

L'autorité de certification en charge de la délivrance des certificats pour les postes nomades doit être dédiée aux usages du nomadisme et maîtrisée par l'entité. Elle est ainsi isolée des autres autorités de certification, ce qui assure un cloisonnement fort en cas de compromission d'une des autorités de certification. 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 pour le nomadisme doit être une autorité intermédiaire (ou subordonnée) dédiée.

La gestion des gabarits de certificats ainsi que des suites cryptographiques utilisées est développée dans le guide de l'agence sur les mécanismes cryptographiques [26].

R30

Mettre en place une IGC maîtrisée par l'entité et dédiée au nomadisme

Il est recommandé de ne pas recourir à une IGC publique externe pour les besoins propres au nomadisme. L'IGC doit donc être maîtrisée par l'entité et ne pas être mutualisée avec d'autres besoins. Il est toutefois possible de déployer une ou plusieurs autorités intermédiaires dédiées au nomadisme et s'appuyant sur une IGC racine déjà existante au sein de l'entité.

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.).

Les recommandations suivantes rappellent les bonnes pratiques liées à la gestion de certificats.

R31

Protéger les éléments secrets liés aux certificats nomades dans des composants sécurisés

Il faut s'assurer que le stockage des clés privées est sécurisé dans les différents contextes d'utilisation.

Pour le poste nomade, il est recommandé de stocker les éléments secrets sur une carte à puce sécurisée équipée d'un crypto-processeur, ou bien dans un composant TPM.

Pour le SI Interne ou la passerelle d'interconnexion (concentrateur VPN, IGC, etc.), il est recommandé d'utiliser un équipement HSM³³.

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

³³. *Hardware security module* : équipement matériel dédié au stockage et au traitement des éléments cryptographiques et disposant à la fois de protections logiques et physiques contre un accès illégitime.

Il faut rester vigilant, notamment dans le cas où la solution VPN repose sur le magasin de certificats Windows pour la gestion des autorités de certification de confiance. Il convient alors de bien mesurer les impacts d'une suppression d'autorités de certification de confiance sur le comportement du poste nomade. Il est dans ce cas possible de configurer le magasin des postes nomades avec une politique de sécurité *GPO* sur le domaine *Active Directory* dont ces postes dépendent, de manière à restreindre la liste des autorités de certification valides.

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

R32

Configurer strictement l'autorité de certification légitime sur les postes nomades

Il est fortement recommandé de configurer le poste nomade et le client VPN de manière à ne faire confiance qu'à l'autorité de certification légitime pour monter le tunnel VPN entre le poste et le SI de l'entité.

3.5.5 Vérification de la validité des certificats

Un certificat peut être révoqué en cas de perte, de vol voire de compromission du poste nomade sur lequel il est installé, mais il peut aussi devenir invalide lorsque sa durée de validité est 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 DN - Subject Distinguished Name, SAN - Subject Alternative Name*), les restrictions d'usage cryptographiques (*KU - Key usage*) ainsi que les restrictions d'usage liées au service (*EKU - 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.

L'opération de vérification d'un certificat lors de l'établissement du tunnel VPN doit entraîner l'interruption de la connexion si au moins un des attributs contrôlés est invalide.

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

1. par le téléchargement périodique d'un fichier *CRL*³⁴ 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 ou un autre équipement dédié disposant des droits de signature (*Key usage = CRL signing*) à chaque fois qu'il est mis à jour;
2. par un service *OCSP*³⁵ mis à disposition sur un élément de la plateforme de l'autorité de certification;
3. 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,

34. *Certificate revocation list*.

35. *Online certificate status protocol* : service Web permettant de fournir un résultat signé indiquant la validité ou non d'un certificat. Ce service s'appuie généralement sur un fichier CRL disponible localement en cache et synchronisé régulièrement.

sans que le client n'ait à requérir 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.

Le concentrateur VPN doit être en mesure de vérifier la validité des certificats VPN clients avant de leur autoriser à monter le tunnel VPN. Cette vérification doit également être effectuée côté client pour se prémunir du risque d'usurpation d'un concentrateur VPN (ce scénario d'attaque n'est toutefois pas trivial car l'attaquant doit être en mesure non seulement de compromettre la clé privée du concentrateur VPN mais également d'usurper son adresse IP publique ou son nom DNS).

La récupération de l'information de validité des certificats ne pose pas de problème au concentrateur VPN dans la mesure où il est généralement placé à proximité des services de distribution CRL ou OCSP, ou bien en capacité de joindre facilement ces services. Cette récupération peut s'avérer plus complexe pour le poste nomade, car elle doit s'effectuer avant l'ouverture complète du tunnel VPN, ce qui peut nécessiter l'autorisation d'un flux supplémentaire sortant sur le poste nomade pour télécharger le fichier CRL à jour ou émettre une requête vers le serveur OCSP. Cela augmente la surface d'attaque du poste nomade car ce flux sortant vers Internet ne bénéficie pas du même niveau de protection qu'un flux similaire transitant au sein du tunnel VPN. Aussi, il est recommandé d'utiliser le mécanisme d'agrafage OCSP lorsque le logiciel Client VPN et le concentrateur VPN supportent cette fonctionnalité.

R33

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

Cette vérification doit se faire avant que l'établissement de la connexion VPN ne soit complet. Cette fonction doit faire partie de l'analyse de risque à mener pour le nomadisme.

La figure 19 présente la recommandation d'usage pour le contrôle de la validité des certificats des concentrateurs VPN :

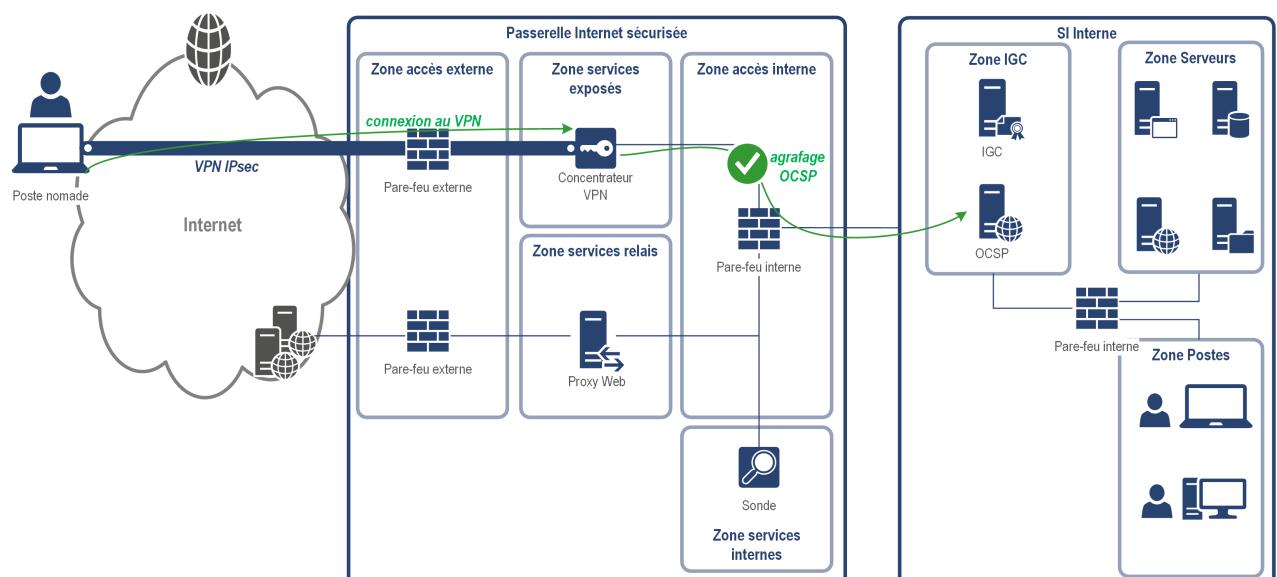


FIGURE 19 – Vérification de la validité des certificats des concentrateurs VPN par agrafage OCSP

Dans le cas où la fonctionnalité d'agrafage OCSP n'est pas supportée, il faut mener une analyse pour décider quelle mesure 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 courte (un mois par exemple) pour le concentrateur VPN et les renouveler régulièrement.

R33 -

Degradé À défaut - Vérifier la validité des certificats concentrateurs VPN par l'ouverture d'un flux direct sur le poste nomade ou par une mesure organisationnelle

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

La figure 20 présente la recommandation alternative pour le contrôle de la validité des certificats des concentrateurs VPN :

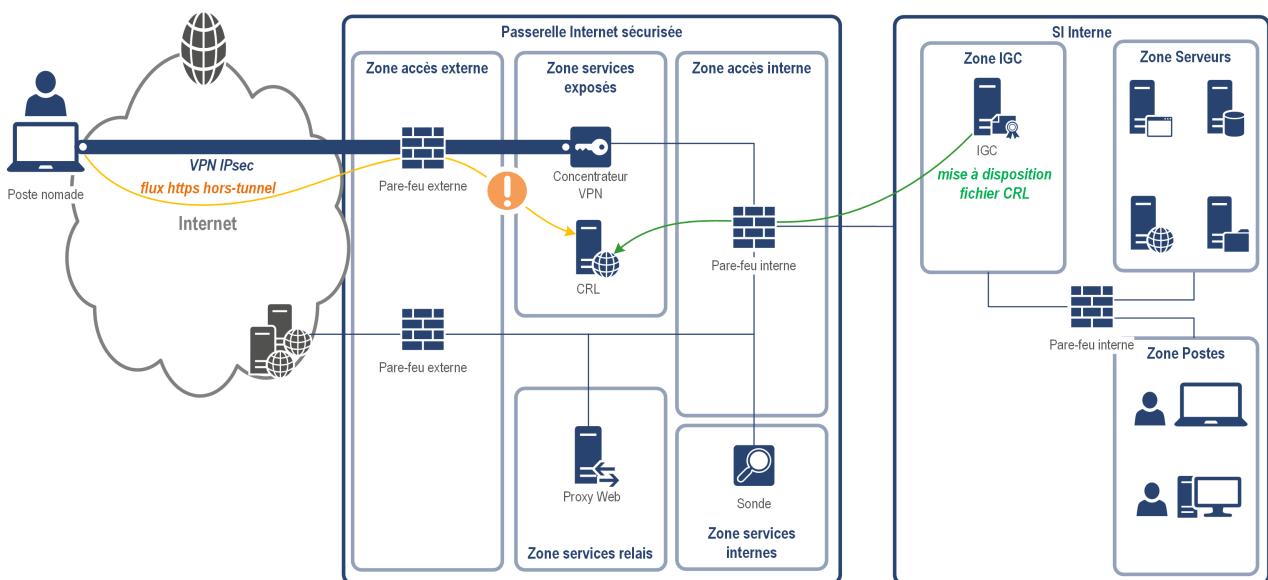


FIGURE 20 – Vérification de la validité des certificats des concentrateurs VPN par fichier CRL

3.6 Passerelle d'interconnexion

3.6.1 Zones d'accès du SI interne

La passerelle d'accès au SI interne doit suivre le schéma directeur proposé dans le guide de l'ANSSI sur les passerelles Internet sécurisées [25]. Comme indiqué dans la figure 3 sur l'architecture VPN, plusieurs zones doivent être implémentées au sein de la passerelle Internet sécurisée, en ce qui concerne les connexions nomades :

- une zone d'accès externe, incluant un ou plusieurs pare-feux externes, connectés en frontal sur Internet;
- une zone de services exposés, incluant un ou plusieurs équipements de terminaison VPN;
- une zone de services relais, incluant des services d'infrastructure pouvant éventuellement être utilisés comme fonctions de protection dans le cadre du nomadisme (p. ex. des *reverse-proxy*);
- une zone d'accès interne, incluant un ou plusieurs pare-feux internes, protégeant le SI interne de l'entité;
- une zone de services internes, incluant par exemple des fonctions de sécurité complémentaires, qui n'entrent pas nécessairement en jeu dans la cinématique de connexion des utilisateurs nomades (p. ex. une sonde de détection d'intrusion réseau).

Cette passerelle d'interconnexion peut contenir plusieurs services d'infrastructure comme un serveur de collecte de journaux dédié, un serveur de relais DNS, etc. Le choix de l'architecture de la passerelle d'interconnexion (notamment le positionnement des éléments) est à définir en fonction du contexte de l'entité et de l'analyse de risque liée au nomadisme. Cette analyse de risque repose notamment sur la confiance que l'on accorde aux postes nomades, c'est-à-dire sur le niveau de sécurité de ceux-ci mais aussi leur exposition à des réseaux non maîtrisés, des environnements plus permissifs.

Dans une situation de nomadisme, où la confiance est moindre, il est pertinent d'étudier des mesures de sécurité complémentaires pour protéger l'accès aux applications métier. Ces mesures peuvent se décliner de plusieurs façons, par exemple :

1. ajouter des fonctions de protection supplémentaires dans la passerelle d'interconnexion pour l'accès des utilisateurs nomades ;
2. mettre en place des services répliqués d'infrastructure (p. ex. un annuaire) ou métier (p. ex. une application web) dans une zone interne cloisonnée et dédiée aux utilisateurs nomades.

Ces deux stratégies sont complémentaires et permettent d'une part de protéger le SI interne et d'autre part de limiter l'impact d'une compromission de l'un des services accédés vers d'autres ressources internes de l'entité. Ces mesures s'insèrent dans une démarche de défense en profondeur pour l'accès au SI de l'entité [16].

Les figures 21 et 22 illustrent la problématique présentée ci-dessus :

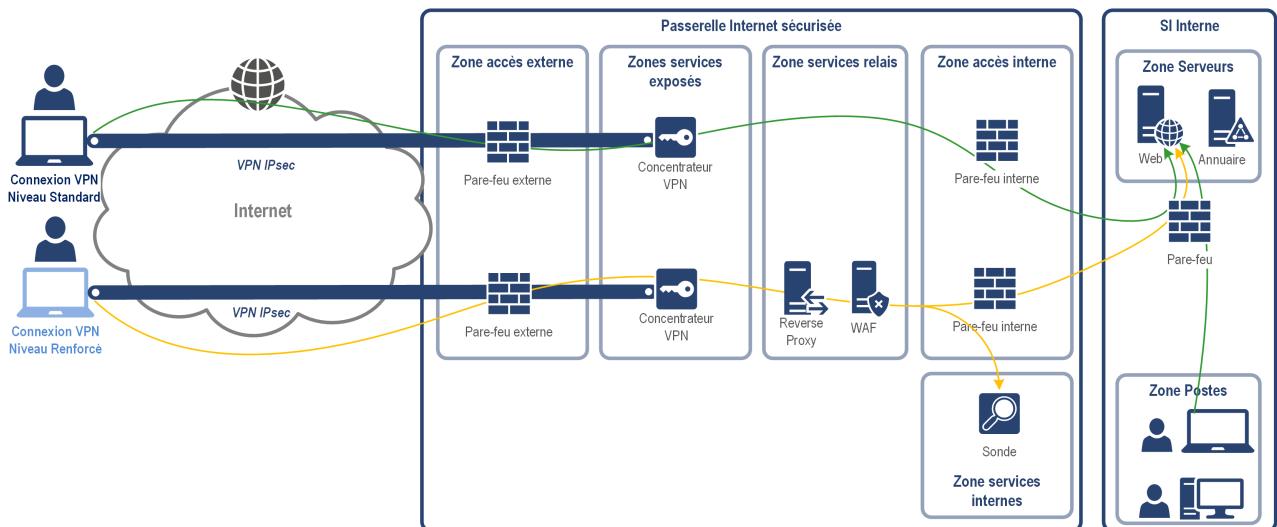


FIGURE 21 – Mise en place de fonctions de protection supplémentaires pour les utilisateurs nomades à risque

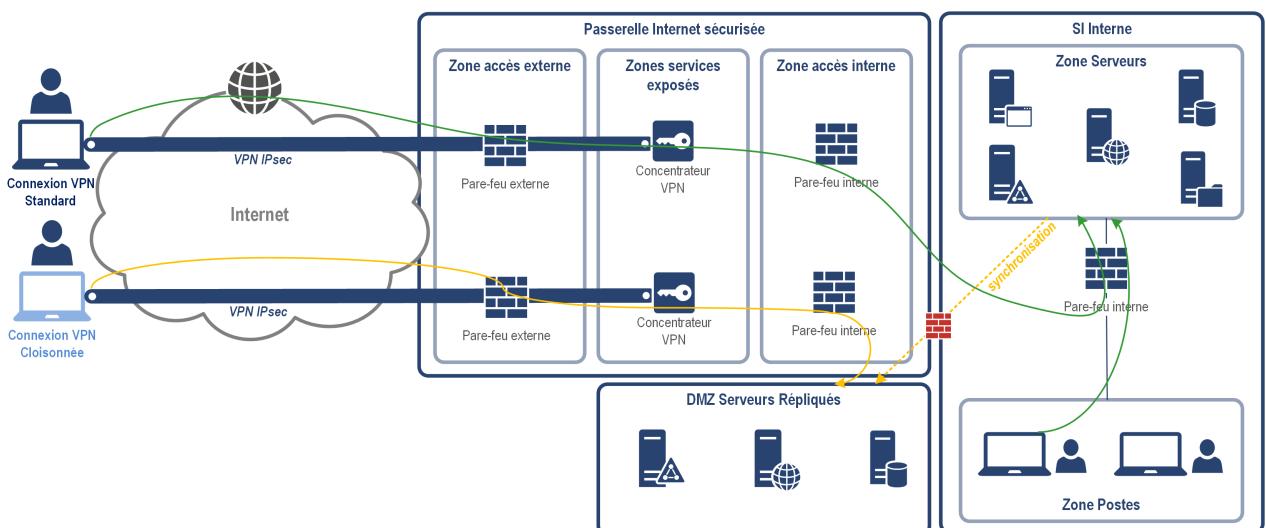


FIGURE 22 – Mise en place de services répliqués et cloisonnés pour les utilisateurs nomades à risque

R34

Implémenter des fonctions de sécurité complémentaires au sein de la passerelle d'interconnexion du nomadisme

Il est recommandé de mettre en place des fonctions de sécurité indépendantes et complémentaires dans la passerelle d'interconnexion du nomadisme pour protéger le SI interne et réduire le risque d'une compromission depuis un poste nomade.

Il est recommandé que les équipements de cette passerelle d'interconnexion VPN soient physiquement dédiés à cet usage. Le fait de mutualiser cette infrastructure avec d'autres services de connexion à distance (liens vers les partenaires, télémaintenance, relais messagerie, sites web publics, etc.) présente un risque de latéralisation en cas de compromission d'une des parties.

R35

Mettre en place des équipements physiquement dédiés au nomadisme dans la passerelle d'interconnexion

Il est recommandé de dédier le matériel nécessaire à la connexion des utilisateurs nomades, au sein de la passerelle d'interconnexion.

S'il n'est pas possible de dédier physiquement les équipements de nomadisme au sein de la passerelle d'interconnexion, alors il est obligatoire de mettre en place un cloisonnement logique, par exemple au moyen :

- de *VLAN*³⁶ et *VRF*³⁷ pour la partie réseau ;
- d'instances virtuelles de pare-feu ;
- de virtualisation de serveurs (voir les guides de l'ANSSI relatifs à la virtualisation [6, 17]).

Il peut être acceptable de mutualiser sur un même socle physique certains éléments liés au nomadisme avec d'autres fonctions du SI (proxy web sortant, ressources internes exposées sur Internet, etc.).

Il convient de prendre en compte l'ordre de priorité suivant dans les choix de mutualisation de ressources de la passerelle d'interconnexion pour des finalités différentes, du plus acceptable (légèrement dégradé) au moins acceptable (très dégradé) :

1. la mutualisation des commutateurs réseaux ;
2. la mutualisation du pare-feu externe ;
3. la mutualisation du pare-feu interne ;
4. la mutualisation du concentrateur VPN ;
5. la mutualisation du service d'authentification utilisé (*radius*, *ldap*, etc.) si celui-ci est externe au concentrateur VPN.

R35 -

Degrade À défaut - Mettre en place un cloisonnement logique pour les fonctions de nomadisme dans la passerelle d'interconnexion

À défaut d'une infrastructure physique dédiée, il est fortement recommandé 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.

36. *Virtual LAN* : réseau local virtuel, également appelé réseau de commutation logique.

37. *Virtual routing and forwarding* : ce mécanisme permet de créer plusieurs instances de table de routage sur un même routeur physique.

Si le cloisonnement physique (voir logique) présente un intérêt pour les équipements liés au nomadisme vis-à-vis d'autres fonctions du SI, il est également important d'étudier et d'appliquer un cloisonnement au sein même de la fonction de nomadisme, entre les différents éléments qui la composent.

R36

Cloisonner physiquement chaque élément de la passerelle d'interconnexion lié au nomadisme

Il est recommandé de dédier le matériel pour chaque élément de la chaîne de connexion des utilisateurs nomades, au sein de la passerelle d'interconnexion.

R36 -

Degrade À défaut - Cloisonner logiquement chaque élément de la passerelle d'interconnexion lié au nomadisme

Il est recommandé d'avoir au minimum des machines virtuelles dédiées à chaque élément de la chaîne de connexion des utilisateurs nomades, dans le cas où celles-ci reposent sur un même socle physique.

Les pare-feux externes de la passerelle d'interconnexion à Internet doivent être le plus minimaliste possible, afin de réduire leur surface d'attaque au maximum. En particulier, il est recommandé que ces pare-feux se limitent uniquement à du filtrage réseau sur les couches du modèle OSI 3 et 4 (IP, TCP, UDP). Les fonctions de filtrage au niveau applicatif (couche du modèle OSI 5 à 7) doivent être désactivées sur ces équipements (module *l7-filter* sur iptables, *deep packet inspection*, fonctions IDS-IPS, *traffic-filtering*, etc.).

Les recommandations pour l'architecture et la configuration des pare-feux exposés à Internet sont développées dans le guide de l'agence relatif à ce sujet [21].

En outre, si les pare-feux externes peuvent être mutualisés pour plusieurs finalités de l'entité (VPN nomade, services web exposés, proxy Internet sortant, etc.), il est en revanche très fortement recommandé que ces pare-feux externes reposent sur des socles physiques dédiés à cet usage et ne soient pas mutualisés avec d'autres fonctions de sécurité de la passerelle d'interconnexion.

R37

Dévier un ou plusieurs socles physiques pour la fonction de pare-feu externe exposé à Internet

Il est recommandé que la fonction de sécurité la plus exposée (pare-feu externe) repose sur un ou plusieurs socles physiques dédiés.

R38

Restreindre les fonctionnalités des pare-feux externes uniquement à du filtrage sur les couches réseaux

Le filtrage des pare-feux exposés à Internet ou pare-feux externes doit se limiter à du filtrage réseau (niveaux 3 et 4 du modèle OSI) et ne doit pas implémenter des fonctions de filtrage applicatif (niveaux 5 à 7 du modèle OSI).

3.6.2 Flux réseau entre postes nomades

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

R39

Interdire tous les flux de communication directs entre les postes nomades

Il est fortement recommandé de configurer l'équipement de terminaison VPN de façon à ce que la communication entre les postes nomades au sein du même sous-réseau soit interdite. Toute connexion depuis le poste nomade doit passer impérativement par la passerelle d'interconnexion.

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 recommandé de ne pas publier d'applications métiers internes 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, rendre une application métier aussi sensible que la messagerie professionnelle accessible directement sur Internet pose le problème de la légitimité des équipements qui accèdent à ce service (p. ex. des équipements personnels). Il suffit qu'un équipement d'accès soit compromis (p. ex. en exploitant une vulnérabilité du navigateur Web) pour qu'un attaquant puisse accéder facilement à des informations sensibles de l'entité. De même, en utilisant un *Keylogger*³⁸, 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 doivent donc transiter, au même titre que toutes les applications métiers des utilisateurs nomades, par le tunnel VPN sécurisé et la passerelle d'interconnexion de l'entité.

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

La figure 23 illustre les recommandations d'usage pour l'accès aux services applicatifs en situation de nomadisme :

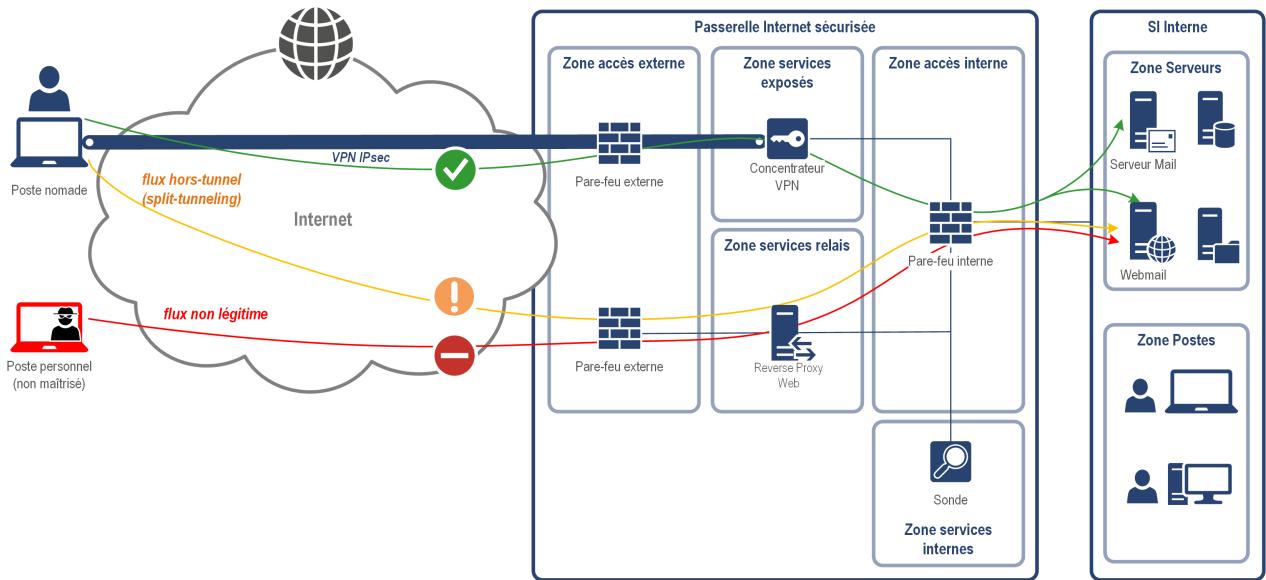


FIGURE 23 – Accès aux services applicatifs en situation de nomadisme

R40

Ne pas exposer d'applications métiers directement sur Internet

Il est important de conserver la maîtrise de l'information et le besoin de confidentialité en n'exposant pas directement sur Internet les applications métiers. Celles-ci ne doivent être accessibles qu'une fois le poste nomade connecté au VPN de l'entité.

Cette problématique est en lien avec les éléments de réflexion présentés plus haut dans la section 3.4.3 avec le cas nominal de *full-tunneling* et le cas dégradé de *split-tunneling*. En effet, dans le cas où l'entité fait le choix d'exposer des applications métiers internes directement sur Internet, cela signifie que certains flux réseaux du poste nomade transitent directement sur Internet, sans la garantie de protection du tunnel VPN.

Si l'entité fait ce choix, elle sera donc exposée à deux risques :

- la surface d'attaque de son SI interne sera plus importante (les services exposés sont potentiellement plus vulnérables);
- la surface d'attaque des postes nomades sera également plus importante (le *split-tunneling* devra être activé pour l'accès à ces services).

Il est donc important que l'accès à ces applications métier soit restreint avec une fonction d'authentification des postes nomades distincte de l'authentification utilisateur au sein de l'application. Cette authentification peut se réaliser au moyen de certificats machine installés sur les postes nomades et dont la clé privée n'est pas accessible par l'utilisateur. La vérification de ces certificats peut par exemple être réalisée avec un serveur intermédiaire *reverse-proxy* et une configuration stricte reposant sur mTLS (*mutual TLS*). L'objectif de ces mesures de sécurité est de limiter l'exposition de services sur Internet aux seuls équipements légitimes de l'entité.

Dégradé À défaut - Authentifier les postes nomades avec une fonction dédiée en cas d'exposition d'applications métiers sur Internet

Dans le cas où des applications métiers sont directement exposées sur Internet, il est recommandé de limiter les accès à ces applications aux seuls équipements légitimes de l'entité. Cette mesure implique d'implémenter une fonction d'authentification des postes nomades reposant sur un service dédié et distinct de l'authentification applicative.

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 *cloud* public, la question de l'accès à ces applications métiers doit également être posée pour les utilisateurs nomades.

Cette question rejoint les éléments de réflexion présentés plus haut dans la section 3.4.3 dans le cas nominal de *full-tunneling* et le cas dégradé de *split-tunneling*. La recommandation est donc de ne pas autoriser un accès direct depuis les postes nomades aux ressources *cloud* pour les utilisateurs en situation de nomadisme. Les flux réseau permettant l'accès des utilisateurs nomades aux services d'un *cloud* public doivent transiter par le SI de l'entité, au travers du tunnel VPN. Cela implique qu'il y ait également une *continuité* du tunnel VPN entre le SI de l'entité et l'environnement *Cloud*.

Le SI de l'entité 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 24 présente la recommandation d'usage pour un accès à un service *cloud* en situation de nomadisme.

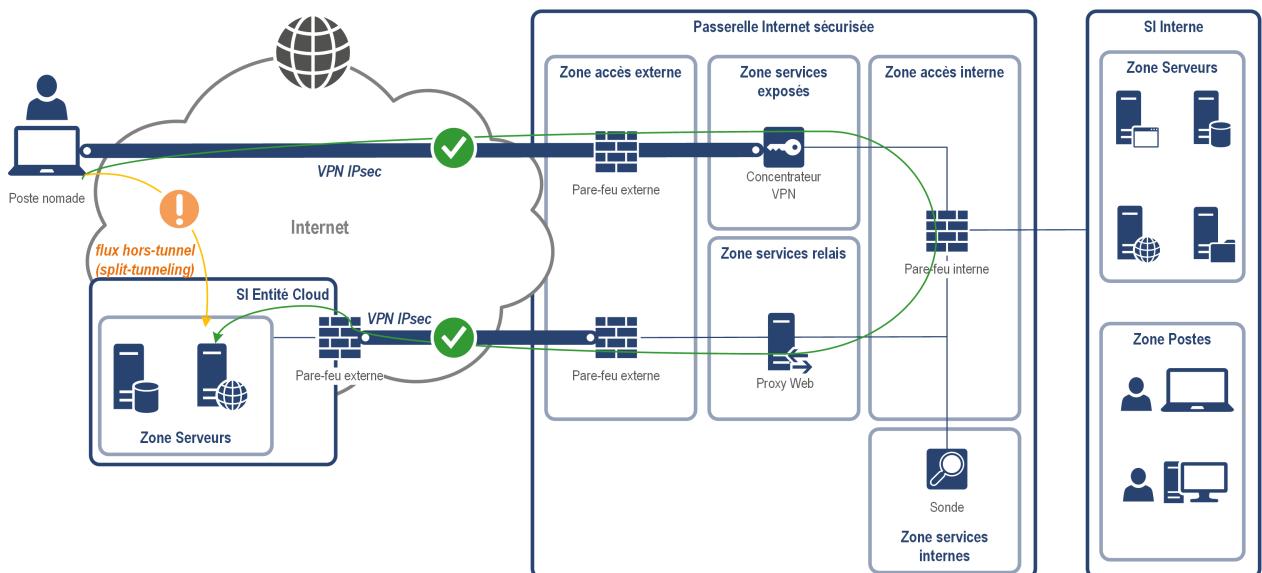


FIGURE 24 – Accès aux services applicatifs dans le *cloud*

R41

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.

Dans le cas où la mise en place de *split-tunneling* est décidée par l'entité pour accéder à des applications spécifiques dans le *cloud*, il faut alors respecter les règles et restrictions d'usage présentées dans le tableau de la section 3.4.3.2.

Ces accès à des ressources dans le *Cloud* via le *split-tunneling* sur le poste nomade doivent être limités au strict besoin opérationnel.

R41 -

Degrado À défaut - Sécuriser les accès directs aux ressources présentes dans le cloud pour les utilisateurs nomades

Dans un mode dégradé, si la mise en place de *split-tunneling* pour des accès directs vers le *cloud* est retenue, il est recommandé que cet accès respecte les exigences de sécurité minimales relatives au chiffrement et à l'authentification des flux (p. ex. via l'usage de TLS à l'état de l'art), à la journalisation des connexions, ainsi qu'à un filtrage strict vers les services concernés.

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.

R42

Réaliser un filtrage au sein de la passerelle d'interconnexion sur les applications autorisées en nomadisme

Ce filtrage peut s'opérer sur les pare-feux situés à la suite du concentrateur VPN, c'est-à-dire les pare-feux internes de la passerelle d'interconnexion à Internet. Dans une démarche de défense en profondeur, le filtrage réseau peut également être configuré en complément au niveau du pare-feu local du poste nomade.

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.

Ce filtrage doit prendre en compte la complexité des applications métier, afin que son implémentation et sa maintenance sur les équipements de sécurité soit au juste niveau de granularité. Ce filtrage réseau peut apporter un bénéfice rapide en matière de sécurité dans le cas où les applications accédées en situation de nomadisme sont homogènes (par exemple si toutes les applications métier sont des applications Web).

3.7.4 Protocoles utilisés

Une fois le tunnel VPN établi entre le poste nomade et le concentrateur VPN dans la passerelle d’interconnexion 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 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 postes nomades ou du canal d’interconnexion VPN, les données applicatives ne sont pas lisibles facilement par l’attaquant.

R43

Privilégier l’utilisation de protocoles chiffrés et authentifiés pour l’accès aux applications métier 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 (HTTP, FTP, TELNET, etc.), mais plutôt des protocoles sécurisés standards (HTTPS, SFTP, 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 nomade. Par exemple, sur un serveur Windows, il est possible d’activer la mise en cache hors ligne et la synchronisation automatique de répertoires partagés sur 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*³⁹, ou bien encore de mettre en place des outils complets de partage documentaire, dédiés à la consultation hors-ligne de documents.

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 nomade tout ou partie des répertoires synchronisés.

Dans le cas où le poste nomade ne dispose pas d’un chiffrement de disque 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.

Cette restriction s’applique dans le cas où elle ne répond pas à un besoin métier bien précis. L’utilisation de services SaaS d’édition de documents, comme par exemple *Office 365* chez Microsoft,

39. *Network file system*.

n'entre pas dans ce cas d'usage puisque ces services sont généralement configurés pour conserver localement une copie des documents édités, et ce afin d'être en mesure de pouvoir justement travailler en mode hors ligne, lorsque la connectivité réseau vers Internet fait défaut.

En outre, l'enjeu de la protection en confidentialité des données sur le poste nomade se pose différemment dans la mesure où le stockage centralisé de ces données n'est pas géré localement par l'entité sur des équipements dédiés, mais s'appuie sur des ressources exposées sur Internet et mutualisées entre plusieurs entités.

La recommandation est donc surtout pertinente pour des infrastructures de stockage locales (*on-premise*) pour se prémunir d'un défaut de protection sur les postes nomades.

R44

Restreindre au strict besoin métier l'utilisation de la synchronisation de documents hors ligne pour les utilisateurs nomades

Le risque lié à la synchronisation de données entre le SI de l'entité et le poste nomade est à étudier avec soin. Il faut éviter de stocker localement des informations sensibles sur le poste nomade, si cela n'est pas nécessaire d'un point de vue métier.

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 [20], 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 la liste de produits qualifiés, ou à défaut certifiés, pendant la phase de conception du SI pour les utilisateurs nomades. Dans le cas où certaines fonctionnalités ne seraient pas présentes sur ces produits, il faut alors mener une analyse de risque 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.

R45

Privilégier l'utilisation de matériels et 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. Il est important de mettre en œuvre un SI dédié à l'administration de l'entité incluant l'administration des équipements liés au nomadisme, conformément au guide d'administration sécurisée publié par l'ANSSI [27].

R46

Respecter les recommandations du guide d'administration sécurisée de l'ANSSI pour les ressources liées au nomadisme

L'administration des équipements liés au nomadisme doit suivre les recommandations formulées dans le guide de l'ANSSI [27].

Il faut également veiller à maintenir en conditions opérationnelles et de sécurité (MCO/MCS⁴⁰) les équipements liés au nomadisme, suivant un processus formalisé, documenté et validé.

40. 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 impliqués dans la mise en œuvre du service de nomadisme ;
- industrialiser les moyens d'administration et d'exploitation des équipements liés au nomadisme ;
- mettre à jour le *master* des postes nomades régulièrement ;
- se tenir informé des vulnérabilités et attaques potentielles sur les équipements utilisés dans le cadre du nomadisme ;
- mettre en place des procédures de résolution d'incidents pour tous les niveaux de support des utilisateurs nomades.

R47

Assurer le MCO et MCS des éléments contribuant au nomadisme

Il faut veiller à mettre en place au minimum un même niveau de maintien en condition opérationnelle et de sécurité pour le nomadisme que celui déjà existant pour le SI interne de l'entité. En particulier, cette politique doit prendre en compte et prioriser le MCO et le MCS des équipements exposés directement à Internet.



Attention

Le maintien en condition de sécurité des postes nomades est d'autant plus critique dans le cas où le *split-tunneling* est activé sur ceux-ci. Le poste nomade est alors plus exposé à des scénarios d'attaque en lien avec des services exposés sur Internet (p. ex. des attaques par point d'eau ou *waterhole*), ce qui augmente le risque de compromission en cas de vulnérabilité sur le poste nomade. L'application des correctifs de sécurité sur le système d'exploitation ainsi que sur les applications installées sur le poste nomade doit donc être réalisée le plus rapidement possible après la publication par les éditeurs concernés.

4.3 Supervision

La supervision des postes nomades est plus difficile que la supervision des postes en interne de l'entité, entre autres parce que :

- la localisation des postes nomades est par nature changeante ;
- la fréquence de connexion est très variable selon les cas ;
- l'attribution d'un poste nomade à un utilisateur 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*⁴¹. Cet outil doit notamment permettre de fournir des indicateurs sur les postes nomades, comme par exemple :

41. *Entreprise Mobility Management*.

- les informations techniques du poste nomade (nom de machine ou *hostname*, modèle, système d'exploitation, etc.);
- l'horodatage de la dernière connexion au SI;
- le dernier rapport d'antivirus;
- le dernier utilisateur connecté;
- la version des mises à jour de sécurité critiques installées;
- la liste des applications installées sur le poste;
- la conformité du poste nomade par rapport à un modèle de sécurité déterminé.

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

R48

Prévoir une supervision de l'état de sécurité des postes nomades

La supervision des postes nomades doit permettre à l'entité de connaître leur niveau de sécurité et son évolution dans le temps. Il est recommandé de disposer d'une fonction de visualisation des principaux indicateurs et alertes concernant les postes nomades.

4.4 Journalisation

La journalisation des événements liés au nomadisme est une composante importante pour la détection, le suivi et la réponse aux incidents de sécurité. Il est recommandé de s'appuyer sur les guides de bonnes pratiques de la journalisation de l'ANSSI [28, 29].

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

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

R49

Mettre en place une journalisation des différents éléments liés au nomadisme en suivant les recommandations des guides de l'ANSSI

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

4.4.1 Liste d'événements à journaliser

Le SI doit journaliser les événements les plus pertinents des éléments de l'infrastructure vus précédemment. Voici quelques exemples d'événements importants dans le cadre du nomadisme, sachant que cette liste n'est pas exhaustive :

- ouvertures de sessions utilisateur (réussites, échecs, certificats expirés, etc.);

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

4.4.2 Centralisation des journaux

Il est également nécessaire de centraliser les journaux d'événements de sécurité de l'ensemble des équipements impliqués dans le nomadisme. Cela implique d'étudier l'architecture adéquate, pour réaliser de manière sécurisée la collecte des journaux, depuis les éléments liés au nomadisme vers les serveurs de collecte.

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

Il est donc recommandé d'utiliser le mode *push* mais en tenant compte des réserves suivantes.

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 (le SI de supervision). 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.

R50

Privilégier le mode push pour la centralisation des journaux des équipements nomades

Il est recommandé d'utiliser le mode *push* pour l'envoi des journaux vers un collecteur centralisé. Ce flux doit être sécurisé (au moyen de TLS par exemple), filtré au moyen d'un pare-feu, et contrôlé par une fonction de détection.

Le serveur de collecte de journaux d'événements doit donc être positionné dans une zone cloisonnée du reste des services d'administration et de supervision de l'entité, de manière à ce qu'une compromission de ce serveur ne puisse faire l'objet d'une latéralisation vers d'autres éléments plus sensibles du SI interne ou du SI d'administration.

4.5 Détection

4.5.1 Analyse et corrélation d'événements

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 sont horodatés sur une source de temps unique et sécurisée.

R51

Mettre en place un système d'analyse et de corrélation d'événements pour le nomadisme

Un système d'analyse et de corrélation d'événements (*SIEM*) doit être mis en place pour être en mesure de répondre aux incidents sur le SI. Ce système peut être intégré directement dans le système utilisé pour le SI interne de l'entité, si celui-ci existe déjà. Le système d'horodatage doit être unique et les équipements impliqués dans le nomadisme doivent se synchroniser avec les mêmes sources de temps.

Le SI doit lever une alerte lorsque certains événements ou combinaisons d'événements se produisent. Voici quelques exemples d'alertes, qui ne sont pas exhaustifs :

- ouvertures de sessions multiples pour un même utilisateur depuis plusieurs IP publiques;
- ouverture de session depuis une IP publique d'un pays étranger;
- ouverture de session à un horaire anormal;
- connexion de support USB et volume important de données copiées depuis le poste nomade;
- création d'un compte local sur le poste nomade;
- requêtes DNS directes sur Internet une fois le tunnel VPN monté;
- effacement des journaux d'événements locaux;
- tentatives d'accès direct sur Internet une fois le tunnel VPN monté;
- requêtes LDAP anormales vers l'annuaire AD;
- tentatives d'installation d'applications.

4.5.2 Sonde de détection d'intrusion

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

Cet équipement doit permettre de détecter un comportement anormal sur les flux réseaux des postes nomades et doit être en mesure d'alerter rapidement les administrateurs du SI de l'entité.

R52

Mettre en œuvre une sonde de détection dans le SI incluant les flux de nomadisme

Cette sonde doit être positionnée au sein de la passerelle d'interconnexion. Il est préférable de l'installer dans une zone dédiée, entre le concentrateur VPN et le pare-feu interne (comme représenté sur la figure 3). L'objectif est que la sonde soit en mesure d'analyser l'ensemble des flux entrants et sortants du SI interne de l'entité et également que cette analyse puisse se faire sur des flux déchiffrés (en sortie du concentrateur VPN).

Le système de détection doit lever une alerte lorsque la sonde réseau détecte des comportements anormaux. Voici quelques exemples d'alertes, qui ne sont pas exhaustifs :

- volume de données transférées sur le poste nomade anormalement élevé;
- nombre de requêtes DNS anormalement élevé ou avec une taille de données utiles du paquet anormale;
- suites cryptographiques utilisées lors d'un *handshake* TLS obsolètes;
- incohérence dans la taille des paquets UDP par rapport aux applications temps-réel (audioconférence, visioconférence);
- séquencement des trames TCP non cohérent, paquets mal-formés.



Information

De manière plus générale, le lecteur peut approfondir tous ces sujets en s'appuyant sur le référentiel des prestataires de détection d'incidents de sécurité (PDIS) [32].

Annexe A

Sécurisation d'un poste nomade partagé entre plusieurs utilisateurs

Dans le cas où un poste nomade doit être partagé entre plusieurs utilisateurs nomades, des actions sont possibles pour renforcer la sécurisation du poste nomade et réduire le risque d'accès illégitimes aux données d'un des utilisateurs par un autre utilisateur.

Dans un premier temps, il est recommandé de mettre en place une procédure de réinitialisation de poste nomade (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 de définir une politique de sécurité stricte sur les postes nomades partagés, qui impose à chaque utilisateur un répertoire de travail qui lui est propre, dans lequel ses documents peuvent être déposés.

Une restriction des droits et priviléges est donc à faire pour la mise en œuvre de cette solution et l'utilisateur ne doit en aucun cas disposer de droits d'administrateur local sur son poste nomade. À titre d'exemple, cette restriction des droits peut se faire par l'application de GPO dans le cas d'un poste nomade Windows. Il est par exemple possible d'utiliser les répertoires de profils prédéfinis par Windows pour le stockage des données de chaque utilisateur, et de proscrire la création de répertoires locaux sur les disques durs du poste nomade.

En complément, il est possible de proposer aux utilisateurs des solutions de chiffrement applicatif des données stockées dans leurs répertoires de travail. Ces solutions peuvent nécessiter une action manuelle de l'utilisateur (l'utilisateur doit faire le choix de chiffrer un document spécifique déjà présent dans son répertoire de travail) ou bien être rendues transparentes et automatiques (l'utilisateur renseigne au démarrage de sa session un mot de passe de déchiffrement global d'une zone logique de son disque, ce qui déverrouille une partition logique permettant de visualiser et interagir avec l'ensemble de ses documents).

Enfin, l'usage d'une solution de coffre-fort de mots de passe installée localement sur le poste permet d'assurer un cloisonnement des secrets d'authentification entre les différents utilisateurs du poste nomade. Il est d'ailleurs fortement recommandé de ne pas activer l'enregistrement et la saisie automatique des mots de passe sur les applications du poste nomade (p. ex. les navigateurs Web).

Annexe B

Évolutions du guide

B.1 Nouvelles recommandations

Les recommandations suivantes font leur apparition ou font l'objet d'une modification importante dans la version 2.0 du guide :

R8, R9, R9+, R11+, R13, R17, R19-, R22, R23, R25, R25+, R25-, R30, R34, R36, R36-, R37
R38, R40-, R41-, R50.

B.2 Mises à jour entre les versions 1.0 et 2.0

Outre les mises à jour de forme (notamment les schémas), le guide a fait l'objet de mises à jour de fond entre les versions 1.0 et 2.0 dont les principales sont énumérées ci-après :

- ajout de précisions sur le *Secure Boot UEFI* dans la section 3.3.3;
- ajout de la notion de chiffrement de disque avec un composant de sécurité dans la section 3.3.4;
- clarification de la section relative à la restriction des privilèges de l'utilisateur 3.3.6;
- modification de la doctrine concernant le VPN IPsec et TLS dans la section 3.4.2;
- ajout d'une section relative au *split-tunneling* 3.4.3.2;
- ajout d'une section relative au protocole DHCP 3.4.3.4;
- modification de la section relative au VPN en interne de l'entité 3.4.5;
- intégration et modification de l'ancienne annexe D dans une nouvelle section relative aux architectures d'authentifications 3.5.3;
- modification de la section relative à la passerelle d'interconnexion VPN 3.6;
- mise en cohérence de la section relative au *Cloud* vis-à-vis du *split-tunneling* en 3.7.2.

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

Afin de permettre aux lecteurs ayant déjà travaillé sur la base de la première version du guide [22], dénommée v1.0 dans la suite du texte, il est proposé une matrice de rétrocompatibilité permettant de trouver les ajouts, suppressions ou équivalences de recommandations.



Attention

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

Référence v1.0	Référence actuelle	Référence v1.0	Référence actuelle
R1	R1	Inexistant	R22 (section sur le DHCP)
R2	R2	Inexistant	R23 (recommandation sur le portail captif)
R3	R3	R20	R24
R4	R4	R20-	R24-
R5	R5	Inexistant	R25, R25+, R25- (recommandations sur le cloisonnement des différents concentrateurs VPN)
R5-	R5-	R21	R26 (Découpage de la R21 en 3 recommandations)
R6	R6	R21	R27
R7	R7	R21	R28
R8	R8	R22	R29
Inexistant	R9 (chiffrement avec TPM) R9+ (chiffrement avec TPM et carte à puce)	Inexistant	R30 (recommandation sur la maîtrise de l'IGC)
R9	R9-	R23	R31
R10	R10	R24	R32
Inexistant	R11 (Clarification de la notion de débrayage du VPN)	R25	R33
R11	R11+	R25-	R33-
R12	R12	Inexistant	R34 (recommandation de défense en profondeur sur la passerelle d'interconnexion)
Inexistant	R13 (recommandation sur IPv6)	R26	R35
R13	R14	R26-	R35-
R14	R15	Inexistant	R36 (recommandation sur le cloisonnement des éléments de la DMZ)
R15	R16	Inexistant	R36- (recommandation sur le cloisonnement des éléments de la DMZ)
R16-	R17 (Mise à jour de la doctrine sur IPsec et TLS)	Inexistant	R37 (recommandation sur le pare-feu externe)
R16	R17+	Inexistant	R38 (recommandation sur le pare-feu externe)
R17	R18	R27	R39
R18	R19	R28	R40
Inexistant	R19- (recommandation dégradée sur le <i>split-tunneling</i>)	Inexistant	R40- (recommandation dégradée sur l'accès direct à des applications)
R19	R21	R29	R41
R19-	R21-	Inexistant	R41- (recommandation dégradée en cohérence avec le <i>split-tunneling</i>)

Référence v1.0	Référence actuelle	Référence v1.0	Référence actuelle
R30	R42		
R31	R43		
R32	R44		
R33	R45		
R34	R46		
R35	R47		
R36	R48		
R37	R49		
Inexistant	R50 (recommandation sur le mode <i>push</i> des journaux)		
R38	R51		
R39	R52		
R40	Suppression (Renvoi vers le guide DR)		

Liste des recommandations

R1	Intégrer le nomadisme dans la PSSI de l'entité	11
R2	Réaliser l'inventaire des activités des utilisateurs compatibles avec le nomadisme	13
R3	Maîtriser la gestion des utilisateurs nomades	13
R4	Sensibiliser et former les utilisateurs nomades	14
R5	Dévier le poste nomade à un utilisateur nomade identifié	14
R5-	Dégradé À défaut - Renforcer la sécurité dans le cas de postes nomades partagés	15
R6	Maîtriser le poste nomade de l'utilisateur nomade	16
R7	Mettre à disposition des moyens de protection physique du poste nomade	17
R8	Maîtriser l'intégrité de la séquence de démarrage du poste nomade	19
R9	Mettre en œuvre une solution de chiffrement de disque avec un TPM	21
R9+	Renforcé Mettre en œuvre une solution de chiffrement de disque avec un TPM et une carte à puce	21
R9-	Dégradé À défaut - Mettre en œuvre une solution de chiffrement de disque sans composant de sécurité physique	22
R10	Maîtriser la connexion de périphériques amovibles sur le poste nomade	23
R11	Interdire à l'utilisateur la modification de la configuration des moyens de protection et de connexion au SI de l'entité	24
R11+	Renforcé Établir le tunnel VPN automatiquement au démarrage du poste nomade et interdire toute action manuelle de l'utilisateur	25
R12	Réduire la surface d'attaque sur le système d'exploitation du poste nomade	26
R13	Désactiver IPv6 sur le poste nomade si celui-ci n'est pas nécessaire	26
R14	Mettre en œuvre les fonctions de sécurité du système d'exploitation sur le poste nomade	27
R15	Activer des mécanismes de mise en quarantaine et de remédiation pour les postes nomades non à jour des correctifs de sécurité	28
R16	Réduire la durée d'inactivité avant verrouillage automatique de la session utilisateur	28
R17	Mettre en œuvre un tunnel VPN IPsec ou VPN TLS à l'état de l'art pour le canal d'interconnexion nomade	30
R17+	Renforcé Mettre en œuvre un tunnel VPN IPsec à l'état de l'art pour le canal d'interconnexion nomade	30
R18	Activer le pare-feu local sur le poste nomade	31
R19	Interdire le <i>split-tunneling</i> sur le poste nomade et autoriser les seuls flux nécessaires pour monter le tunnel VPN	33
R19-	Dégradé À défaut - En cas d'usage du <i>split-tunneling</i> mettre en œuvre une configuration stricte visant à limiter les risques de compromission	35
R20-	Dégradé À défaut - N'autoriser la navigation Internet en <i>split-tunneling</i> sur le poste nomade que via un proxy de confiance	35
R21	Bloquer les flux DNS vers Internet et configurer directement les adresses IP publiques des concentrateurs VPN sur le client	36

R21-	Dégradé À défaut - Sécuriser et maîtriser les flux DNS pour la résolution du nom du concentrateur VPN	36
R22	Configurer le client DHCP pour restreindre au strict nécessaire les paramètres à appliquer sur le poste nomade	39
R23	Bloquer l'accès aux portails captifs sur les postes nomades	40
R24	Généraliser l'emploi de concentrateurs VPN pour les usages nomade mais aussi interne à l'entité	43
R24-	Dégradé À défaut - Mettre en place un mécanisme de détection de l'environnement de l'utilisateur nomade	43
R25	Dévier physiquement des concentrateurs VPN respectivement pour les connexions nomades et internes au SI	44
R25+	Renforcé Dévier physiquement un concentrateur VPN pour les connexions internes en Wi-Fi	44
R25-	Dégradé À défaut - Cloisonner logiquement par virtualisation les concentrateurs VPN mutualisés sur un même socle physique	45
R26	Authentifier l'utilisateur sur le poste nomade	49
R27	Authentifier le poste nomade sur le SI	49
R28	Authentifier l'utilisateur sur le SI	50
R29	Mettre en place une authentification multifacteur forte pour l'utilisateur nomade	52
R30	Mettre en place une IGC maîtrisée par l'entité et dédiée au nomadisme	61
R31	Protéger les éléments secrets liés aux certificats nomades dans des composants sécurisés	61
R32	Configurer strictement l'autorité de certification légitime sur les postes nomades	62
R33	Vérifier la validité des certificats client et concentrateur VPN via le mécanisme d'agrafage OCSP	63
R33-	Dégradé À défaut - Vérifier la validité des certificats concentrateurs VPN par l'ouverture d'un flux direct sur le poste nomade ou par une mesure organisationnelle	64
R34	Implémenter des fonctions de sécurité complémentaires au sein de la passerelle d'interconnexion du nomadisme	66
R35	Mettre en place des équipements physiquement dédiés au nomadisme dans la passerelle d'interconnexion	67
R35-	Dégradé À défaut - Mettre en place un cloisonnement logique pour les fonctions de nomadisme dans la passerelle d'interconnexion	67
R36	Cloisonner physiquement chaque élément de la passerelle d'interconnexion lié au nomadisme	68
R36-	Dégradé À défaut - Cloisonner logiquement chaque élément de la passerelle d'interconnexion lié au nomadisme	68
R37	Dévier un ou plusieurs socles physiques pour la fonction de pare-feu externe exposé à Internet	68
R38	Restreindre les fonctionnalités des pare-feux externes uniquement à du filtrage sur les couches réseaux	68
R39	Interdire tous les flux de communication directs entre les postes nomades	69
R40	Ne pas exposer d'applications métiers directement sur Internet	70
R40-	Dégradé À défaut - Authentifier les postes nomades avec une fonction dédiée en cas d'exposition d'applications métiers sur Internet	71

R41	Interdire un accès direct aux ressources présentes dans le <i>cloud</i> pour les utilisateurs nomades	72
R41-	À défaut - Sécuriser les accès directs aux ressources présentes dans le <i>cloud</i> pour les utilisateurs nomades	72
R42	Réaliser un filtrage au sein de la passerelle d'interconnexion sur les applications autorisées en nomadisme	72
R43	Privilégier l'utilisation de protocoles chiffrés et authentifiés pour l'accès aux applications métier au travers du tunnel VPN	73
R44	Restreindre au strict besoin métier l'utilisation de la synchronisation de documents hors ligne pour les utilisateurs nomades	74
R45	Privilégier l'utilisation de matériels et logiciels disposant d'un visa de sécurité de l'ANSSI	75
R46	Respecter les recommandations du guide d'administration sécurisée de l'ANSSI pour les ressources liées au nomadisme	75
R47	Assurer le MCO et MCS des éléments contribuant au nomadisme	76
R48	Prévoir une supervision de l'état de sécurité des postes nomades	77
R49	Mettre en place une journalisation des différents éléments liés au nomadisme en suivant les recommandations des guides de l'ANSSI	77
R50	Privilégier le mode <i>push</i> pour la centralisation des journaux des équipements nomades	78
R51	Mettre en place un système d'analyse et de corrélation d'événements pour le nomadisme	79
R52	Mettre en œuvre une sonde de détection dans le SI incluant les flux de nomadisme	80

Bibliographie

- [1] *Le modèle Zero Trust.*
Avis scientifique et technique, ANSSI, avril 2021.
<https://cyber.gouv.fr/publications/le-modele-zero-trust>.
- [2] *CORPUS DOCUMENTAIRE IPSEC DR À DESTINATION DES INDUSTRIELS.*
Référentiel, ANSSI, février 2023.
<https://cyber.gouv.fr/publications/corpus-documentaire-ipsec-dr-destination-des-industriels-version-10>.
- [3] *Recommandations de sécurité relatives à Active Directory.*
Note technique DAT-NT-017/ANSSI/SDE/NP v1.1, ANSSI, septembre 2014.
<https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-active-directory>.
- [4] *Recommandations de configuration matérielle de postes clients et serveurs x86.*
Note technique DAT-NT-024/ANSSI/SDE/NP v1.0, ANSSI, mars 2015.
<https://cyber.gouv.fr/publications/recommandations-de-configuration-materielle-de-postes-clients-et-serveurs-x86>.
- [5] *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.
- [6] *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://cyber.gouv.fr/publications/recommandations-de-securite-pour-les-architectures-basees-sur-vmware-vsphere-esxi>.
- [7] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation.*
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.
<https://cyber.gouv.fr/guide-windows10-vsm>.
- [8] *Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10.*
Guide ANSSI-BP-036 v1.2, ANSSI, juillet 2017.
<https://cyber.gouv.fr/guide-windows10-collecte-donnees>.
- [9] *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://cyber.gouv.fr/guide-windows-restrictions-logicielles>.
- [10] *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux.*
Guide ANSSI-BP-043 v1.0, ANSSI, août 2018.
<https://cyber.gouv.fr/guide-802-1x>.

- [11] *Recommandations de sécurité relatives à un système GNU/Linux.*
Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022.
<https://cyber.gouv.fr/guide-linux>.
- [12] *Recommandations de sécurité relatives aux déploiements de conteneur Docker.*
Fiche technique ANSSI-FT-082 v1.0, ANSSI, septembre 2020.
<https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-au-deploiement-de-conteneurs-docker>.
- [13] *Maîtriser les risques de l’infogérance. Externalisation des systèmes d’information.*
Guide Version 1.0, ANSSI, décembre 2010.
<https://cyber.gouv.fr/guide-externalisation>.
- [14] *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://cyber.gouv.fr/hygiene-informatique>.
- [15] *Bonnes pratiques à l’usage des professionnels en déplacement.*
Guide ANSSI-GP-065 v3.0, ANSSI, mai 2019.
<https://cyber.gouv.fr/publications/bonnes-pratiques-lusage-des-professionnels-en-deplacement>.
- [16] *La défense en profondeur appliquée aux systèmes d’information.*
Guide Version 1.1, ANSSI, juillet 2004.
<https://cyber.gouv.fr/defense-profondeur>.
- [17] *Problématiques de sécurité associées à la virtualisation des systèmes d’information.*
Note technique DAT-NT-011/ANSSI/SDE/NP v1.1, ANSSI, septembre 2013.
<https://cyber.gouv.fr/virtualisation>.
- [18] *Recommandations de sécurité relatives aux réseaux Wi-Fi.*
Note technique DAT-NT-005/ANSSI/SDE/NP v1.0, ANSSI, septembre 2013.
<https://cyber.gouv.fr/guide-wifi>.
- [19] *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://cyber.gouv.fr/guide-ipsec>.
- [20] *Achat de produits de sécurité et de services de confiance qualifiés.*
Guide ANSSI-PA-045 v2.0, ANSSI, janvier 2017.
<https://cyber.gouv.fr/achat-rgs>.
- [21] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet.*
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.
<https://cyber.gouv.fr/guide-pare-feux-internet>.
- [22] *Recommandations sur le nomadisme numérique.*
Guide ANSSI-PA-054 v1.0, ANSSI, octobre 2018.
<https://cyber.gouv.fr/guide-nomadisme-numerique>.
- [23] *Maîtrise du risque numérique - l’atout confiance.*
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
<https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance>.

- [24] *Recommandations de sécurité relatives à TLS.*
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
<https://cyber.gouv.fr/guide-tls>.
- [25] *Recommandations relatives à l'interconnexion d'un système d'information à Internet.*
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.
<https://cyber.gouv.fr/guide-interconnexion-si-internet>.
- [26] *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.*
Guide ANSSI-PG-083 v2.0, ANSSI, janvier 2020.
<https://cyber.gouv.fr/publications/mecanismes-cryptographiques>.
- [27] *Recommandations relatives à l'administration sécurisée des systèmes d'information.*
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
<https://cyber.gouv.fr/guide-admin-si>.
- [28] *Recommandations de sécurité pour l'architecture d'un système de journalisation.*
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
<https://cyber.gouv.fr/guide-journalisation>.
- [29] *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory.*
Guide ANSSI-PB-090 v1.0, ANSSI, janvier 2022.
<https://cyber.gouv.fr/guide-journalisation-windows>.
- [30] *Référentiel général de sécurité (RGS).*
Référentiel Version 2.0, ANSSI, juin 2012.
<https://cyber.gouv.fr/rgs>.
- [31] *Instruction interministérielle n°901.*
Référentiel Version 1.0, ANSSI, janvier 2015.
<https://cyber.gouv.fr/ii901>.
- [32] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences.*
Référentiel Version 2.0, ANSSI, décembre 2017.
<https://cyber.gouv.fr/pdis>.
- [33] *Authentification multifacteurs et mots de passe.*
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
<https://cyber.gouv.fr/guide-authentification>.
- [34] *Instruction générale interministérielle n°1300.*
Référentiel, SGDSN, août 2021.
<https://cyber.gouv.fr/igi1300>.
- [35] *Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte.*
Guide ANSSI-PG-075 v1.2, ANSSI, septembre 2021.
<https://cyber.gouv.fr/guide-archi-sensible-dr>.

Version 2.0 - 13/11/2023 - ANSSI-PA-054

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

ISBN : 978-2-11-167134-8 (papier)

ISBN : 978-2-11-167135-5 (numérique)

Dépôt légal : Novembre 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

cyber.gouv.fr / conseil.technique@ssi.gouv.fr

