RECOMMANDATIONS RELATIVES À L'INTERCONNEXION D'UN SYSTÈME D'INFORMATION À INTERNET

GUIDE ANSSI

ANSSI-PA-066
19/06/2020

PUBLIC VISÉ :

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

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations relatives à l'interconnexion d'un système d'information à Internet** ». Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab [19].

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

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

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	08/12/2011	Version initiale N°3248/ANSSI/ACE
2.0	18/06/2019	Refonte du plan, ajout d'un chapitre sur l'accès aux contenus Web, nouveau modèle de guide ANSSI
3.0	19/06/2020	Modifications de forme, ajout d'un chapitre sur le service de messagerie électronique

Table des matières

1 Introduction

1.1 Objectif du guide

Ce guide de l'ANSSI a pour objectif de fournir des recommandations d'architecture technique pour l'interconnexion d'un système d'information (SI) d'une entité – publique ou privée – avec un réseau public. Le postulat est que le réseau public interconnecté est Internet car il s'agit du cas le plus fréquent. Il peut y avoir transposition à d'autres contextes, par exemple l'interconnexion au réseau d'un partenaire. Le guide traite aussi bien des flux sortants que des flux entrants vis-à-vis du SI de l'entité.

Attention

Les SI interconnectés avec Internet sont réputés héberger des données publiques ou non sensibles.
Pour les SI hébergeant des données sensibles ou à *Diffusion Restreinte* (DR) au sens de l'II 901 [17], l'application des recommandations de ce guide est nécessaire [1] mais non suffisante. Les lecteurs sont invités à se référer à la réglementation [17] dans l'attente de toute autre publication de l'ANSSI.
Les SI hébergeant des données classifiées de défense au sens de l'IGI 1300 [15] requièrent des passerelles multi-niveaux qui dépassent le cadre de ce guide ; ils ne sont donc pas traités ici.

Ce guide s'adresse à un public technique disposant de connaissances basiques d'architecture réseau et capable d'adapter les recommandations en fonction de ses contraintes et de ses enjeux.

1.2 Organisation du guide

Ce guide contient le socle nécessaire à la construction de l'interconnexion (chapitres 2 et 3). Des compléments sur les fonctions de sécurité de services applicatifs sont fournis ensuite : sur l'accès aux contenus hébergés sur le Web (chapitre 4) et sur le service de messagerie électronique (chapitre 5).

1.3 Convention de lecture

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

1. Les recommandations de type R - (cf. section 1.3) sont fortement déconseillées dans le cas des SI sensibles ou DR. Au contraire, les recommandations de type R + sont fortement conseillées pour ces SI.

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

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

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

R -

Recommandation alternative de premier niveau

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

R --

Recommandation alternative de second niveau

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

R +

Recommandation renforcée complémentaire

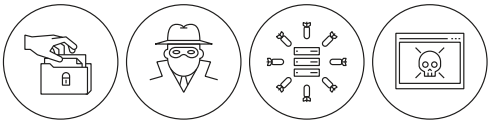
Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

La liste récapitulative des recommandations est disponible en page 51.

1.4 Menaces considérées

Pour de nombreuses entités, l'interconnexion de leur SI avec Internet est nécessaire, tant ce dernier offre une richesse de services et d'opportunités numériques. Néanmoins il constitue aussi, de manière incontestable aujourd'hui, une source de menaces. Parmi les plus courantes, il est possible de citer :

- l'exfiltration de données depuis le SI de l'entité vers Internet, portant atteinte à leur confidentialité ;
- l'intrusion pour porter atteinte à l'intégrité ou la disponibilité du SI de l'entité ;
- l'usurpation d'identité en accédant à des ressources de l'entité pour rebondir et mener des attaques vers d'autres cibles ;
- le déni de service pour nuire à la disponibilité de l'accès Internet et donc à la productivité ou à l'image de l'entité ;
- l'accès par les collaborateurs à des sites Web interdits par la charte d'utilisation interne voire par la loi.



Si l'accroissement de l'externalisation de services et, potentiellement, du patrimoine informationnel de l'entité dans le nuage (*cloud*) – qui n'est pas le sujet de ce guide – est une réalité, il ne doit pas faire oublier que l'accès à ces services est tout autant critique et doit être sécurisé. La performance et la disponibilité de l'accès à Internet peuvent devenir aussi critiques que l'accès au réseau privé de l'entité.

1.5 Hygiène informatique et pré-requis

Dans le guide d'hygiène informatique [3] publié par l'ANSSI en 2017, le déploiement d'une passerelle sécurisée d'accès à Internet fait l'objet d'une mesure spécifique (mesure 22) ; ce guide en est une déclinaison.

Afin de ne pas surcharger ce guide et de se concentrer sur les recommandations spécifiques au contexte, les lecteurs sont invités à se référer au guide d'hygiène informatique pour en appliquer les mesures élémentaires, dont notamment :

- former les équipes opérationnelles afin que celles-ci maîtrisent les solutions déployées ;
- maintenir une cartographie, précisant notamment les points d'interconnexion avec Internet ;
- segmenter le SI en zones homogènes ;
- maîtriser les risques de l'infogérance en cas d'externalisation ;
- définir une politique de mise à jour ;
- activer et configurer les journaux des composants les plus importants.

1.6 Expression du besoin

En premier lieu, il est indispensable d'identifier clairement et formellement les besoins métier liés à Internet, pour construire et sécuriser l'architecture technique d'interconnexion spécifique à l'entité. Pour les phases ultérieures, ce travail préliminaire doit faciliter l'établissement de matrices de flux et de règles de contrôles d'accès.

Information

Dans ce guide, on convient qu'un *flux* désigne un flux de données, reposant généralement sur IP, pouvant être transporté sur TCP ou UDP et ayant un sens (entrant ou sortant) vis-à-vis d'Internet ou du SI de l'entité.

R1

Déterminer l'ensemble des services nécessitant l'interconnexion à Internet

Afin de déployer une infrastructure d'interconnexion répondant au juste besoin fonctionnel de l'entité, il est nécessaire d'établir de manière exhaustive une liste des services du SI de l'entité (applications métier, services d'infrastructure) nécessitant une interconnexion à Internet, en distinguant les flux entrants et les flux sortants.
Cette liste doit être mise à jour dès que nécessaire et revue régulièrement.

À titre d'exemple, voici une liste non exhaustive de services nécessitant une interconnexion à Internet :

- la navigation Web ;
- la récupération de sources ou de mises à jour logicielles depuis des sites de confiance ;
- la résolution de noms DNS publics ;
- les services publics de l'entité exposés sur Internet (ex. : hébergements Web, DNS publics) ;
- les services d'infrastructures de l'entité exposés sur Internet (ex. : passerelle VPN IPsec ou TLS pour les accès nomades, passerelle VPN IPsec pour des tunnels site à site) ;
- les services collaboratifs de l'entité exposés sur Internet (ex. : messagerie électronique, téléphonie, visioconférence, portail Extranet) ;
- les services métier de l'entité exposés sur Internet (ex. : EDI [2]) ;
- l'accès à Internet pour les visiteurs.

Information

La mise en œuvre de passerelles VPN pour les accès nomades est traitée de manière détaillée dans le guide de l'ANSSI sur le nomadisme numérique [13] en cohérence avec la doctrine de ce guide plus générique.

Par ailleurs, la conception d'une passerelle d'interconnexion ne se limite pas au choix d'un boîtier (ou *appliance*) multi-services sur étagère. Elle nécessite en premier lieu l'identification des fonctions de sécurité à mettre en œuvre sur l'interconnexion et de leur position dans l'architecture. Le choix de chaque équipement constituant la passerelle doit se faire sur la base de trois critères :

- son apport sur le plan de la sécurité ;
- sa robustesse ;
- la capacité pour l'équipe technique chargée de le mettre en œuvre de le maîtriser et de le maintenir dans un état sécurisé.

À cet effet, s'agissant de la robustesse, l'emploi de produits disposant d'un visa de sécurité [3] de l'ANSSI est recommandé.

2. Échange de données informatisées.
3. https://www.ssi.gouv.fr/visa-de-securite.

2
Architecture et fonctions de sécurité de l'interconnexion

2.1 Précisions sur le concept de zone démilitarisée

En informatique, le concept militaire de *zone démilitarisée* (DMZ [4]) est régulièrement réutilisé pour désigner un sous-réseau (concrètement, quelques équipements) séparant deux zones de confiance hétérogène notamment grâce à des pare-feux réalisant un filtrage périmétrique de part et d'autre (cf. figure 2.1).

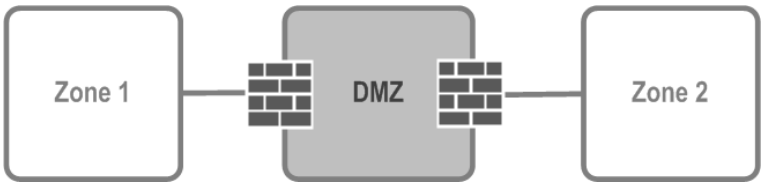


FIGURE 2.1 – Zone démilitarisée

Dans le cas d'une interconnexion à Internet au moyen d'une DMZ, différents points de filtrage et d'analyse du trafic sont également nécessaires pour traiter les risques liés aux menaces identifiées (cf. section 1.4). Pour cela, il convient donc de limiter tout accès direct qui serait simplement routé entre le SI interne de l'entité et Internet. Concrètement, la DMZ disposant d'un filtrage périmétrique, d'une part avec Internet et d'autre part avec le SI interne de l'entité, doit également intégrer, autant que nécessaire, des relais applicatifs implémentant des fonctions de sécurité (ex. : serveur mandataire – *proxy* – pour les accès Web, résolveur DNS pour les requêtes de noms DNS publics).

De plus, la DMZ est ici considérée comme une zone neutre et perdable. En effet, sa sensibilité n'est pas nulle (des données du SI de l'entité peuvent y être exposées ou au moins y transiter) mais une attaque en intégrité ou en confidentialité sur ses composants ne doit pas remettre en cause de manière irréversible et durable le bon fonctionnement du SI de l'entité. À titre d'exemple, la compromission d'un relais de messagerie au sein d'une DMZ pourrait amener à décider sa destruction et sa reconstruction sans que les boîtes aux lettres électroniques hébergées et protégées de manière *ad hoc* dans le SI interne de l'entité ne soient elles-mêmes détruites.

4. L'acronyme anglais DMZ pour *demilitarized zone* est le plus couramment utilisé.

Passerelle d'interconnexion sécurisée

Une passerelle d'interconnexion sécurisée est constituée d'une ou plusieurs « DMZ » qui doivent être des zones neutres, perdables, protégées par des pare-feux périmétriques et servant, en leur sein et autant que possible, à la rupture protocolaire et à l'analyse du trafic échangé entre un réseau public et le SI interne de l'entité.

Pour la suite du guide, on convient de parler de *passerelle Internet sécurisée*. De plus, dans un souci de simplification, on convient de parler de *la* DMZ constituant la passerelle Internet sécurisée dans les principes d'architecture générale. Elle sera utilement décomposée en plusieurs DMZ dans les principes d'architecture détaillée (section 2.4).

2.2 Filtrage et cloisonnement

2.2.1 Filtrage périmétrique et filtrage interne

Le fournisseur d'accès à Internet (FAI) de l'entité propose généralement son service en positionnant un routeur d'accès (éventuellement appelé *box* pour les plus petits modèles intégrés) dans les locaux de l'entité. Cet équipement est sous responsabilité du FAI. Même s'il est présenté comme embarquant des fonctions de sécurité, c'est avant tout un équipement réseau de routage et non un équipement de sécurité. Afin de maîtriser la sécurité périmétrique du SI de l'entité, celle-ci doit mettre en œuvre un premier niveau de filtrage IP sous son contrôle et indépendant du routeur d'accès (cf. figure 2.2).

R2

Déployer un pare-feu maîtrisé entre la DMZ et le routeur d'accès Internet

L'interconnexion entre Internet et la DMZ doit être protégée de façon périmétrique par une fonction de filtrage IP assurée par un pare-feu. Ce dernier est dit *externe* ; il doit être maîtrisé par l'entité (ou un prestataire mandaté à cet effet) et ne doit pas être contournable.
Une matrice des flux correspondant au juste besoin opérationnel doit être définie, mise en œuvre sur ce pare-feu et revue régulièrement.

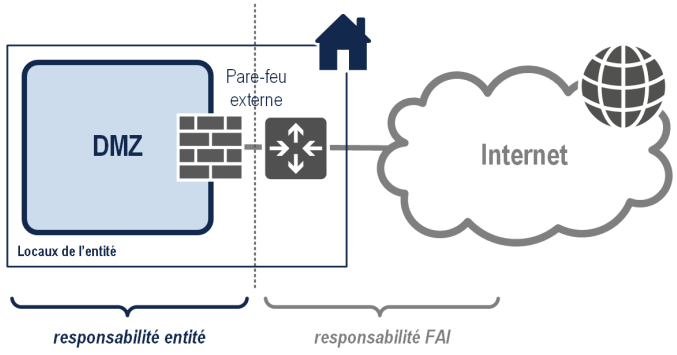


FIGURE 2.2 – Filtrage périmétrique avec Internet grâce à un pare-feu externe

Seules les ressources (ex. : postes de travail, serveurs) ayant un besoin opérationnel légitime de connexion à Internet doivent être autorisées à y accéder. Un découpage du SI interne en zones homogènes, amenant à un adressage en sous-réseaux IP distincts, doit permettre de déterminer quelles sont les zones autorisées à accéder à la passerelle Internet sécurisée. Une fonction de filtrage doit dès lors être mise en œuvre entre le SI interne et la DMZ (cf. figure 2.3).

R3

Déployer un pare-feu maîtrisé entre le SI interne et la DMZ

L'interconnexion entre le SI interne et la DMZ doit être protégée de façon périmétrique par une fonction de filtrage IP assurée par un pare-feu. Ce dernier est dit *interne* ; il doit être maîtrisé par l'entité (ou un prestataire mandaté à cet effet) et ne doit pas être contournable.
Une matrice des flux correspondant au juste besoin opérationnel doit être définie, mise en œuvre sur ce pare-feu et revue régulièrement.

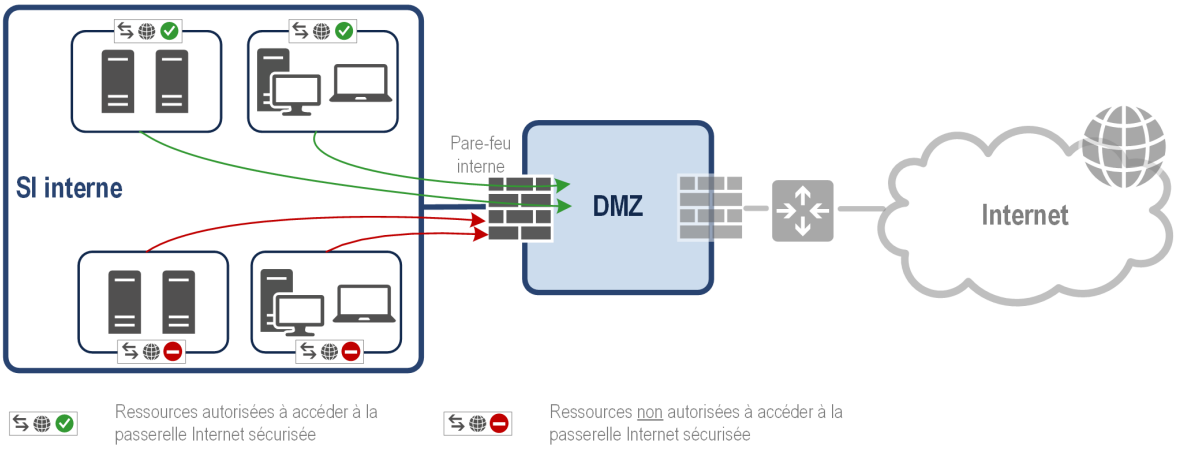


FIGURE 2.3 – Filtrage périmétrique avec le SI interne grâce à un pare-feu interne

Information

Pour la suite du guide, la *passerelle Internet sécurisée* inclut la DMZ d'interconnexion entre le SI interne de l'entité et Internet ainsi que les pare-feux périmétriques qui la protègent. Celle-ci est ainsi représentée sur la figure 2.4.

R4

Rendre incontournable la passerelle Internet sécurisée

Tout système d'information nécessitant une interconnexion avec Internet doit être protégé par une passerelle Internet sécurisée mettant en œuvre au minimum des fonctions de filtrage périmétrique ainsi que des services applicatifs relais.
Cette passerelle doit être incontournable. En particulier, tout autre accès à Internet pour des besoins spécifiques, potentiellement non compatibles avec la passerelle (ex. : accès Internet à des fins de test « comme à la maison », sans aucune fonction de sécurité depuis un poste dédié) doit être réalisé depuis des infrastructures physiquement distinctes.

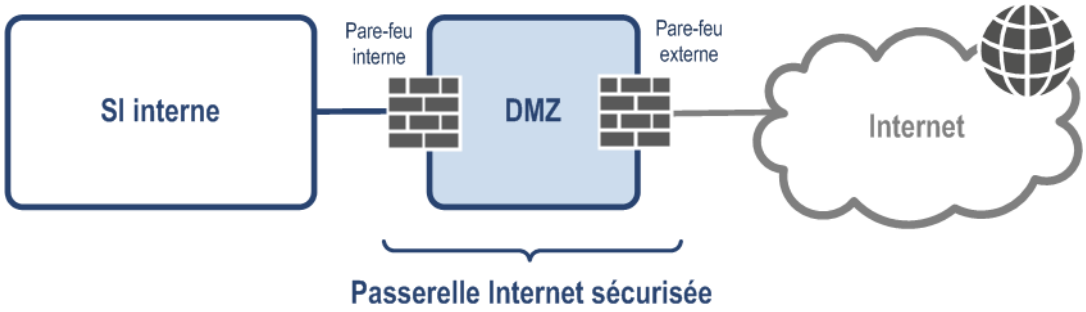


FIGURE 2.4 – Interconnexion du SI interne de l'entité et d'Internet au moyen d'une passerelle Internet sécurisée

Information

D'ores et déjà, il convient de préciser que les pare-feux interne et externe doivent être physiquement distincts dans une démarche de défense en profondeur. Plus de détails sont fournis dans le paragraphe 2.4.4.
Par ailleurs, s'agissant de la question de la diversification technologique des pare-feux interne et externe et des niveaux de visas de sécurité recommandés, le guide [11] de l'ANSSI est dédié à ce sujet ; le lecteur est invité à s'y référer.
Enfin, l'ANSSI publie également des recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu [5] et pour son nettoyage [9].

Dans le cas où certains services applicatifs sont directement hébergés au sein de la passerelle Internet sécurisée (ex. : hébergement d'un serveur Web), il est souhaitable de filtrer les flux entre les serveurs métier (ex : serveur Web) et les serveurs relais applicatifs (ex. : serveur mandataire inverse – *reverse proxy*). Dans ce cas, un ou plusieurs pare-feux dit *intermédiaires* sont déployés en coupure pour assurer le filtrage (cf. figures 2.13 et 2.15).

R5

Déployer si nécessaire des pare-feux intermédiaires dans la passerelle Internet sécurisée

Afin de filtrer les flux internes de la passerelle Internet sécurisée entre des serveurs métier et des serveurs relais, la mise en œuvre d'un ou plusieurs pare-feux intermédiaires complémentaires est recommandée.

2.2.2 Cloisonnement et cinématique des flux

Des flux très hétérogènes peuvent transiter par la passerelle Internet sécurisée à l'initiative du SI de l'entité vers Internet (services accédés) ou, à l'inverse, des flux à l'initiative d'Internet vers le SI de l'entité (services hébergés). Suivant la confiance accordée à la zone source (généralement plus élevée lorsqu'il s'agit du SI de l'entité que d'Internet) et suivant les besoins de sécurité du service (ex. : hébergement d'un simple site Web *versus* accès nomade des administrateurs en VPN IPsec), les mesures de sécurité sont différentes. Dès lors, des chaînes de traitement distinctes doivent être construites et cloisonnées au sein de la passerelle Internet sécurisée ; celles-ci sont constituées par exemple de serveurs relais applicatifs, d'équipements réseau d'accès et de sécurité.

R6

Cloisonner les flux au sein de chaînes de traitement homogène

Afin d'adapter les mesures de sécurité en fonction de la source des flux et des besoins de sécurité du service, autant de chaînes de traitement distinctes doivent être construites et cloisonnées au sein de la passerelle Internet sécurisée.
La nature du cloisonnement, physique de préférence ou logique à défaut, dépend des besoins de sécurité et de l'exposition des services et doit être déterminée par une analyse de risque.

Information

Cette recommandation R6 est volontairement généraliste mais sera déclinée dès que nécessaire par service (ex. : accès à la navigation Web *versus* hébergement Web) et est appliquée sur le schéma d'architecture multi-services (cf. figure 2.22 en p. 26).

En outre, il est recommandé que la cinématique des flux vis-à-vis de la passerelle Internet sécurisée respecte des règles simples mais strictes, illustrées par la figure 2.5 :

- tout flux en provenance du SI et à destination d'Internet (accès) est initié par le client du SI vers la passerelle Internet sécurisée puis de la passerelle Internet sécurisée vers Internet ;
- tout flux en provenance d'Internet et à destination du SI (hébergement) est initié par le client sur Internet vers la passerelle Internet sécurisée ; au sein de cette passerelle, les serveurs reçoivent à la fois des flux provenant d'Internet et du SI ; en d'autres termes, il n'y a pas de flux initié depuis la passerelle Internet sécurisée vers le SI.

R7

Respecter une cinématique sécurisée des flux

Le principe d'un flux initié depuis une zone de plus haute confiance vers une zone de moindre confiance doit ici être adapté au contexte d'une passerelle Internet sécurisée, respectivement vis-à-vis d'Internet et du SI de l'entité.
Il est recommandé en particulier de ne pas initialiser de flux depuis la passerelle Internet sécurisée vers le SI interne de l'entité.

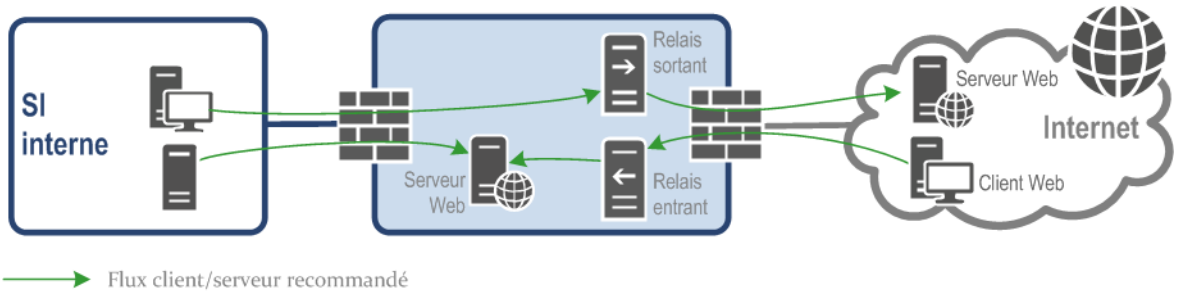


FIGURE 2.5 – Exemple de cinématique sécurisée des flux vis-à-vis de la passerelle Internet sécurisée

La recommandation R7 n'est malheureusement pas applicable à l'ensemble des flux entrants (ex. : cas d'un relais de réception de messagerie, cf. figure 2.6). Une alternative, d'un niveau de sécurité moindre, consiste à limiter le nombre de serveurs pouvant initialiser une connexion vers le SI interne. Dès lors, il est indispensable de bien cloisonner les ressources concernées au sein du SI.

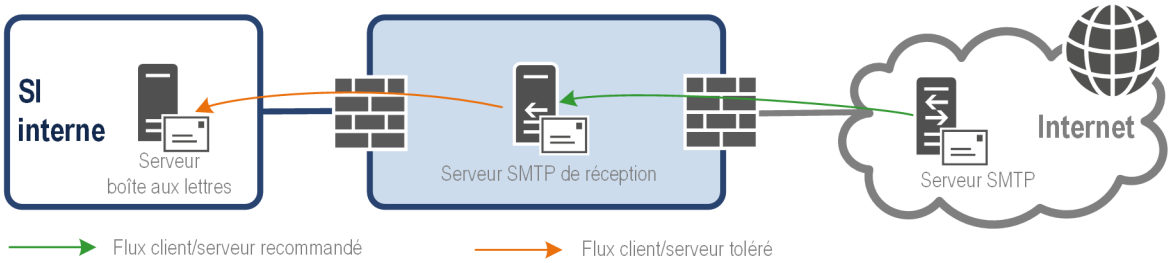


FIGURE 2.6 – Exemple de cinématique alternative et moins sécurisée de flux entrants vis-à-vis de la passerelle Internet sécurisée

2.3 Fonctions de sécurité génériques de l'interconnexion

Au-delà du filtrage au moyen de pare-feux et des principes de cloisonnement, la passerelle Internet sécurisée doit répondre à des besoins de détection afin de réagir au plus tôt en cas d'incident de sécurité et d'authentification à des fins de contrôle d'accès et d'imputabilité.

2.3.1 Rupture protocolaire et analyse de flux

L'interconnexion avec un réseau de moindre confiance (ici Internet) impose à l'entité un principe de base : tout flux entrant ou sortant doit au minimum bénéficier d'une rupture protocolaire afin de ne pas exposer sur Internet la pile IP des ressources de l'entité et, suivant les cas, bénéficier d'une analyse dans l'objectif de détecter une fuite de données ou l'introduction d'un code malveillant.

Rupture protocolaire

Une rupture protocolaire consiste à casser en entrée et reconstruire en sortie la communication entre deux ressources (généralement un client et un serveur) au niveau d'une des couches du modèle OSI [5].
Les protocoles en entrée et en sortie peuvent être distincts suivant les contraintes techniques de l'environnement et les objectifs de sécurité.

R8

Procéder à une rupture protocolaire des flux

Afin de se prémunir de connexions malveillantes directes entre une ressource de l'entité et une ressource sur Internet (ex. : un serveur de commande et contrôle), une rupture protocolaire doit être mise en œuvre au sein de la passerelle Internet sécurisée.

R9

Procéder à une analyse des flux en fonction de l'analyse de risque

Pour éviter toute fuite de données ou introduction de codes malveillants, une analyse des flux est recommandée lors de cette rupture protocolaire.

5. *Open System Interconnections*.

Attention

Cette recommandation s'applique dès lors qu'au moins une des parties n'est pas de confiance, comme un site Web hébergé sur Internet auquel accède un client de l'entité ou un client Web sur Internet qui accède à un site Web hébergé par l'entité.
Dans le cas de deux points de confiance maîtrisés par l'entité utilisant Internet comme réseau de transport, comme un client VPN déployé sur un poste nomade de l'entité et un concentrateur VPN hébergé par l'entité, la rupture du tunnel VPN n'est pas recommandée afin de préserver la confiance dans la confidentialité, l'intégrité et l'authenticité des flux.

En tant que moyens de détection des incidents de sécurité, l'architecture de la passerelle Internet sécurisée peut également prévoir l'ajout de dispositifs permettant une copie du trafic (*taps* réseau), et de sondes de sécurité pour analyser ce trafic dupliqué. Il est alors recommandé que ces équipements de sécurité disposent d'un visa de sécurité de l'ANSSI. Dans certains cas, la mise en œuvre de ces équipements est imposée par la législation (ex. : aux interconnexions pour les SI sensibles au sens de l'II 901 [17] ou pour les systèmes d'information d'importance vitale au sens de la loi de programmation militaire 2013).

2.3.2 Authentification

Pour les besoins d'authentification au sein de la passerelle Internet sécurisée, il est indispensable de ne pas exposer un annuaire hébergé dans le SI interne directement aux équipements de la passerelle Internet sécurisée. En effet, une vulnérabilité d'un de ses équipements pourrait amener à une prise de contrôle de cet annuaire puis du SI interne. Trois solutions d'architecture sont envisageables suivant le niveau de sécurité visé et les méthodes d'authentification permises par les équipements de la passerelle Internet sécurisée :

- un annuaire dédié au sein de la passerelle Internet sécurisée, synchronisé à l'initiative d'un annuaire hébergé sur le SI interne, contenant les données correspondant au strict besoin opérationnel et, sauf contrainte exceptionnelle, en lecture seule ; cette solution respecte la cinématique sécurisée des flux (cf. R7) et est adaptée aux flux entrants et sortants ;
- un serveur mandataire inverse d'authentification (ex. : *reverse proxy* LDAP) hébergé au sein de la passerelle Internet sécurisée, configuré avec les restrictions idoines pour des échanges avec un annuaire hébergé sur le SI interne ; cette solution évite l'hébergement des données d'authentification dans la passerelle Internet sécurisée, est adaptée aux flux entrants et sortants mais déroge à la cinématique sécurisée des flux (cf. R7) ;
- un serveur mandataire dédié à l'authentification au sein du SI interne et requêtant un annuaire du SI interne ; dans ce cas, aucune authentification n'est nécessaire au sein de la passerelle Internet sécurisée ; c'est la solution la plus sécurisée mais qui est adaptée aux flux sortants uniquement et est potentiellement coûteuse à déployer et à maintenir.

La réutilisation d'une base d'authentification existante (ex. : celle des postes bureautiques) est possible grâce à des mécanismes standards (ex. : RADIUS, LDAPS).

Les figures 2.7, 2.8 et 2.9 illustrent ces trois solutions pour des flux sortants.

R10

Ne pas exposer d'annuaire du SI interne aux ressources de la passerelle Internet sécurisée

En aucun cas un annuaire du SI interne ne doit être directement requêté par les équipements de la passerelle Internet sécurisée pour les besoins propres d'authentification. Trois architectures sont proposées pour y répondre :

- un annuaire dédié, minimaliste et en lecture seule, au sein de la passerelle Internet sécurisée (cf. figure 2.7) ;
- un serveur mandataire inverse d'authentification au sein de la passerelle Internet sécurisée (cf. figure 2.8) ;
- un serveur mandataire au sein du SI de l'entité dédié aux besoins d'authentification de la passerelle Internet sécurisée (cf. figure 2.9).

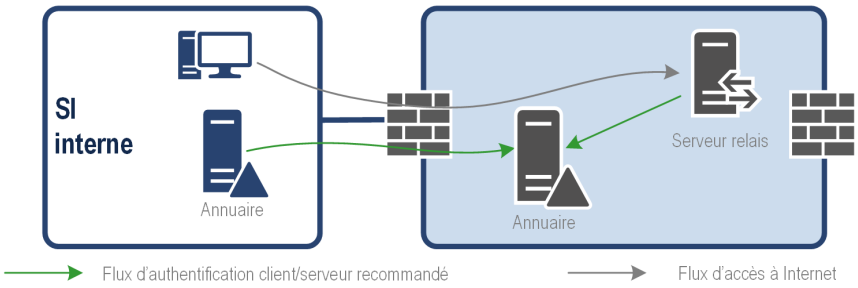


FIGURE 2.7 – Annuaire dédié au sein de la passerelle Internet sécurisée, synchronisé à l'initiative d'un annuaire du SI interne et requêté par un serveur relais applicatif

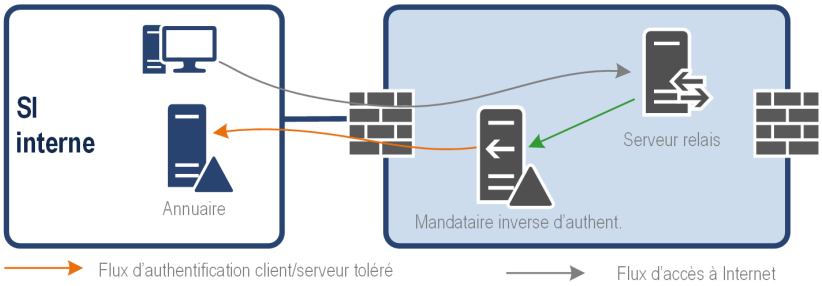


FIGURE 2.8 – Serveur mandataire inverse d'authentification au sein de la passerelle Internet sécurisée, requêtant un annuaire du SI interne et requêté par un serveur relais applicatif

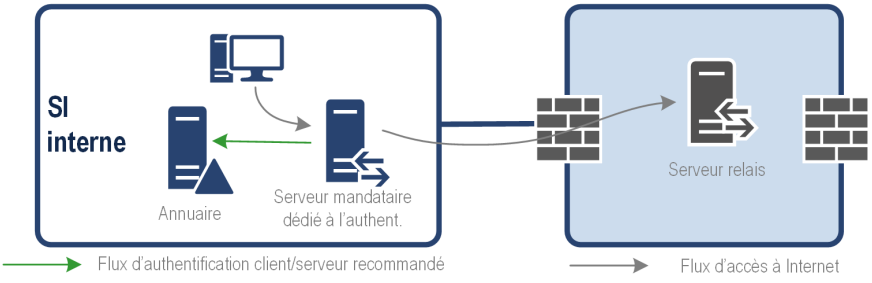


FIGURE 2.9 – Serveur mandataire au sein du SI interne dédié aux besoins d'authentification de la passerelle Internet sécurisée et y transférant les requêtes

2.4 Architecture détaillée

Cette section présente des architectures détaillées d'une passerelle Internet sécurisée classées par niveau de sécurité décroissant. Dans tous les cas, on distingue cinq types de zones (regroupements de ressources logicielles ou matérielles) :

- la *zone d'accès interne* pour le filtrage entre le SI interne et la passerelle Internet sécurisée ;
- la *zone de services internes* pour les ressources dédiées au fonctionnement de la passerelle Internet sécurisée ;
- la *zone de services exposés* pour l'hébergement éventuel [6] de serveurs métier (ex. : serveur Web, serveur de transfert de fichiers) ;
- la *zone de services relais* pour la rupture protocolaire et l'analyse des flux ;
- la *zone d'accès externe* pour le filtrage entre la passerelle Internet sécurisée et Internet.

Avant d'aborder les alternatives possibles d'architecture de passerelle Internet sécurisée, une représentation macroscopique de ces zones est proposée sur la figure 2.10.

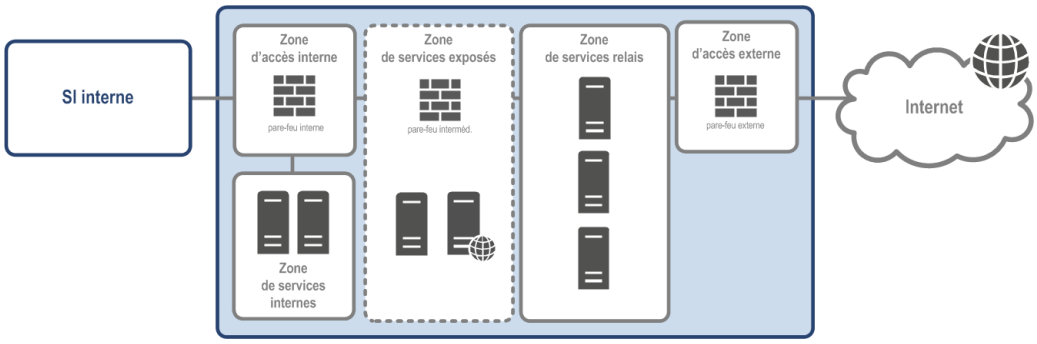


FIGURE 2.10 – Représentation macroscopique des zones d'une passerelle Internet sécurisée

2.4.1 Rappels sur les risques de la mutualisation par virtualisation

Les facilités opérationnelles permises par la mutualisation par virtualisation peuvent inciter à regrouper différentes ressources logicielles (services, applicatifs ou réseau), sur une même ressource physique. Ce regroupement peut consister à exécuter différentes applications sur le même système d'exploitation ou à mettre en œuvre des techniques de virtualisation plus ou moins lourdes.

Dans le contexte de la passerelle Internet sécurisée, les risques liés à la mutualisation des ressources sont les suivants :

- déni de service : le dysfonctionnement d'une des applications installées sur une machine physique peut entraîner une indisponibilité de l'ensemble des services s'exécutant sur la machine ;
- compromission de services : si un attaquant parvient à prendre le contrôle d'un service donné, il lui sera généralement beaucoup plus facile de compromettre les différents services s'exécutant sur la même machine physique (par escalade locale de privilège par exemple ou attaques de plus bas niveau [7]).

6. Cette zone, déployée ou non suivant le contexte, est volontairement représentée en pointillés sur la figure 2.10.
7. Les vulnérabilités Spectre et Meltdown affectant plusieurs familles de processeurs et pouvant conduire à des fuites de données sont deux exemples récents à la date de parution de ce guide. Cf. https ://cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-001/.

L'opportunité d'exécuter sur une même machine plusieurs services doit être évaluée en prenant en compte les recommandations suivantes :

- il est recommandé de n'héberger sur une même machine physique que les ressources d'une même zone (cf. figure 2.11) ;
- il est recommandé de n'héberger sur une même machine physique que des services identiques du point de vue fonctionnel et de la sécurité. Par exemple, il est déconseillé d'exécuter sur la même machine un serveur Web et un *reverse proxy* Web ;
- il est recommandé d'isoler sur une même machine physique les services notoirement moins bien sécurisés (dans les respect des deux recommandations précédentes) ;
- il n'est pas souhaitable d'héberger sur une même machine physique un serveur nominal et son éventuel serveur de secours.

R11

Évaluer les risques de mutualisation par virtualisation

Les opportunités permises par la virtualisation doivent être mises au regard des risques qu'elle présente.
Le principe de précaution doit prévaloir : des ressources peuvent être virtualisées et mutualisées sur un socle physique commun à la condition que les services qu'elles portent aient des besoins de sécurité et une exposition homogènes.

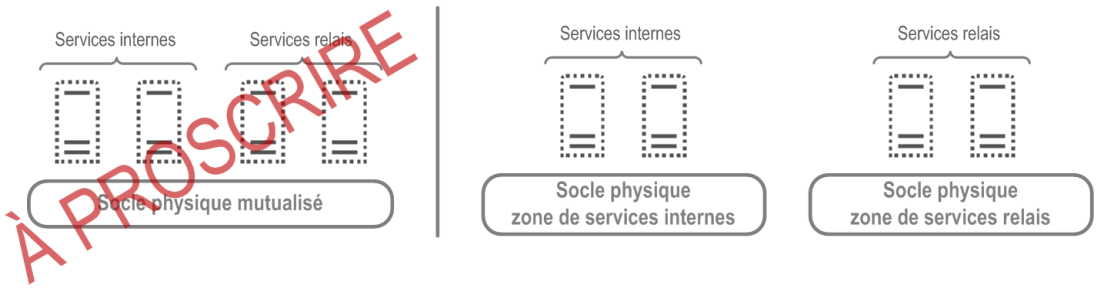


FIGURE 2.11 – Exemples de (non) mutualisation par virtualisation

2.4.2 Cas 1 : absence de mutualisation par virtualisation entre zones

La solution ayant le niveau de sécurité le plus élevé consiste à dédier des équipements physiques pour chaque zone y compris pour la commutation réseau (cf. figures 2.12 et 2.13). En effet, la forte exposition des zones d'accès interne et externe incite à ne pas mutualiser des fonctions de filtrage ou de commutation réseau sur un même équipement physique, quand bien même celui-ci permettrait de déployer des instances virtuelles.

R12

Déployer une passerelle Internet sécurisée à base d'équipements physiques dédiés par zone

Afin de garantir le cloisonnement effectif entre chaque zone de la passerelle Internet sécurisée et *in fine* entre le SI interne et Internet, il est recommandé de dédier des équipements physiques par zone, y compris pour le filtrage et la commutation réseau.

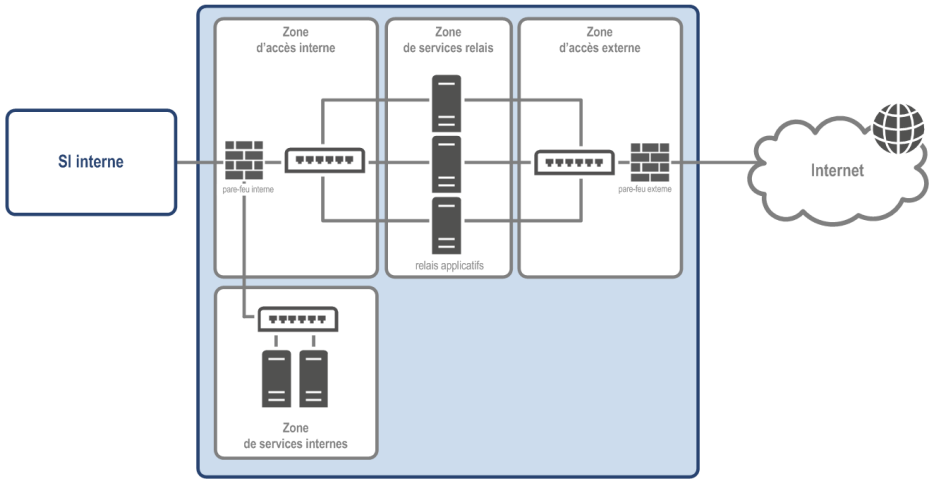


FIGURE 2.12 – Architecture recommandée d'une passerelle Internet sécurisée (sans zone de services exposés)

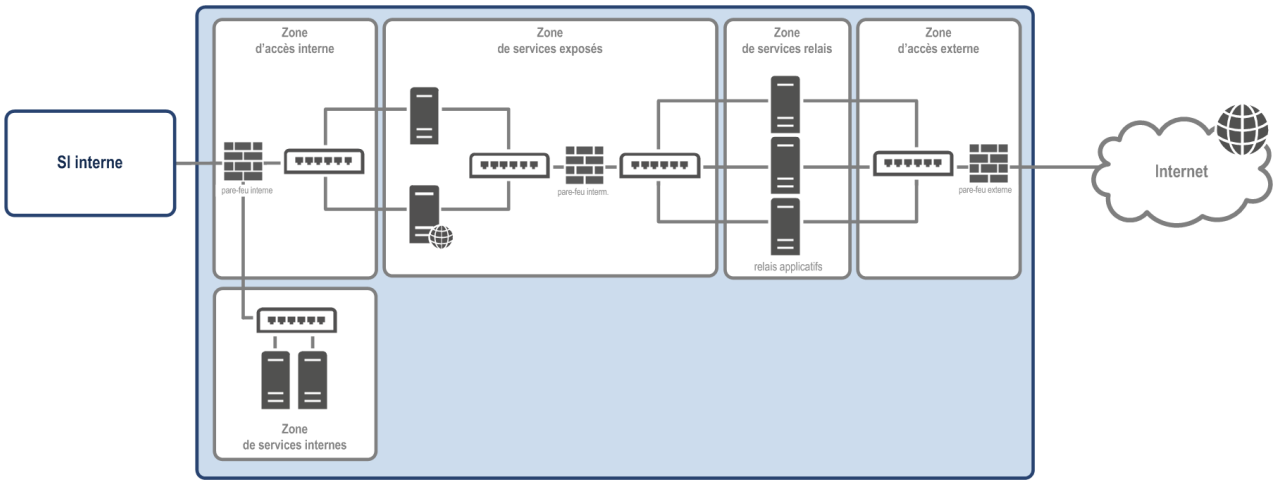


FIGURE 2.13 – Architecture recommandée d'une passerelle Internet sécurisée (avec zone de services exposés)

2.4.3 Cas 2 : mutualisation physique de la commutation réseau

Une solution d'un niveau de sécurité moindre consiste à mutualiser physiquement la commutation réseau au niveau de la zone de services relais (cf. figure 2.14) voire de la zone de services exposés (cf. figure 2.15). Dans ce cas, une segmentation logique doit toutefois être réalisée à l'aide de VLAN (*Virtual Local Area Network*). Le durcissement réalisable sur le commutateur mutualisé est en effet moindre que celui-ci réalisable sur les serveurs de la zone de services relais (ou de la zone de services exposés) disposant de deux interfaces physiques.

R12 -

Déployer une passerelle Internet en acceptant la mutualisation de certains équipements de commutation réseau

La dérogation à l'architecture la plus sécurisée consiste à mutualiser les équipements de commutation réseau pour les zones d'accès interne, des services relais et d'accès externe de la passerelle Internet sécurisée.
Dans ce cas, des commutateurs physiques dédiés respectivement à la zone de services internes et à l'éventuelle zone de services exposés doivent être maintenus.

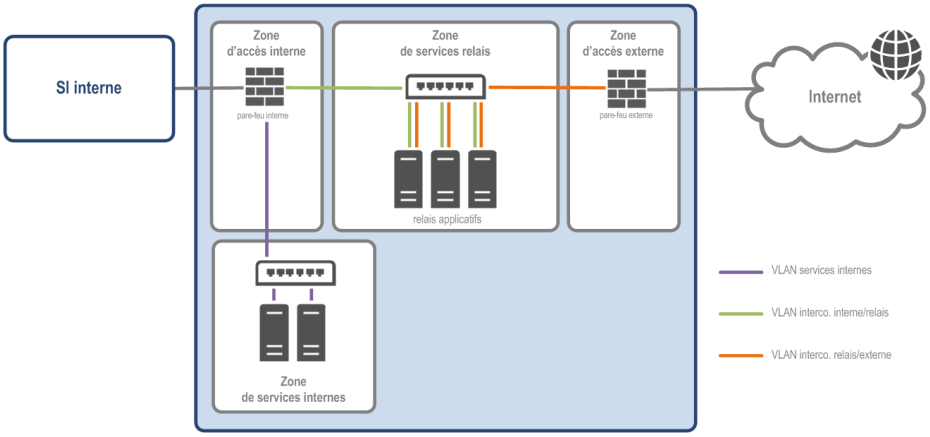


FIGURE 2.14 – Architecture d'une passerelle Internet sécurisée avec mutualisation d'une partie de la commutation réseau (sans zone de services exposés)

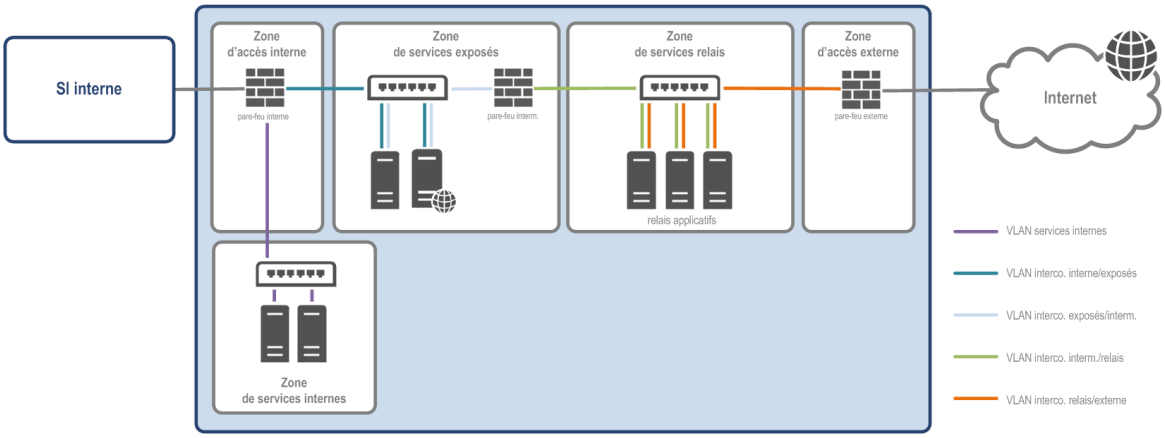


FIGURE 2.15 – Architecture d'une passerelle Internet sécurisée avec mutualisation d'une partie de la commutation réseau (avec zone de services exposés)

Information

L'ANSSI publie un guide de recommandations pour la sécurisation d'un commutateur de desserte [1] qu'il est utile de consulter à cette occasion.

2.4.4 Cas 3 : mutualisation du filtrage à proscrire

Une solution d'un niveau de sécurité moindre consisterait à mutualiser le filtrage de la passerelle Internet sécurisée vers Internet et vers le SI interne (c'est-à-dire les pare-feux interne et externe) sur un seul équipement physique.

Attention

Il est important de comprendre que, dans cette architecture, la compromission de l'unique pare-feu ou une erreur de configuration peut donner un accès direct entre le SI interne et Internet, ce dont on cherche à se protéger.

Cette architecture (cf. figure 2.16) n'est pas recommandée. En particulier, elle n'est pas conforme aux exigences de l'II 901 [17] pour les SI sensibles ou *Diffusion Restreinte*.

R13

Proscrire toute mutualisation des pare-feux interne et externe

En raison de la forte exposition des zones d'accès interne et externe, toute mutualisation des pare-feux interne et externe, même à l'aide d'instances virtuelles distinctes déployées sur un socle physique commun, doit être proscrite.

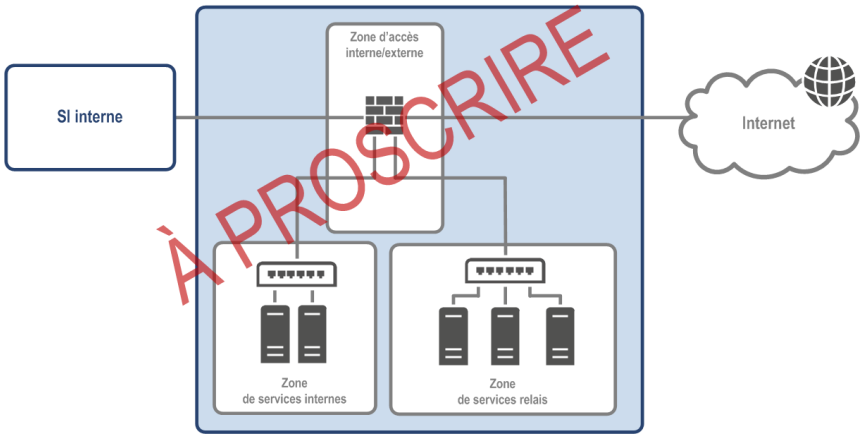


FIGURE 2.16 – Architecture à proscrire d'une passerelle Internet sécurisée avec mutualisation du filtrage

2.4.5 Gestion du cas d'exception des connexions directes

L'architecture recommandée (R12) permet, grâce à une coupure physique, de garantir qu'aucune communication n'est possible entre les pare-feux interne et externe sans passer par la zone de services relais. Sans cette coupure physique – c'est le cas de l'architecture alternative (R12-) – il existe un risque qu'un flux sortant transite directement sans qu'il ne soit filtré au niveau applicatif. Toutefois, certains flux sortants peuvent être difficiles voire impossibles à traiter par un relais applicatif.

En premier recours, il est nécessaire d'étudier avec attention les possibilités de configuration du logiciel client nécessitant un accès à Internet (ex. : configuration *proxy* HTTP) et l'ensemble des

configurations permises par le relais. Par exemple, l'utilisation de tunnels grâce à la méthode HTTP CONNECT sur un serveur mandataire HTTP peut répondre à certains cas d'usage. Il convient dès lors d'être extrêmement attentif à la configuration associée du serveur mandataire s'agissant des restrictions d'adresses IP source/destination et de ports TCP destination.

En dernier recours, il peut être nécessaire de raccorder directement les pare-feux externe et interne par un lien physique sans passage par un serveur relais (cf. figure 2.17). Dans ce cas, la gestion des matrices de flux et du routage doit être d'autant plus stricte sur ces deux pare-feux. De plus, seules des zones dédiées du SI interne doivent être autorisées à utiliser ce chemin d'accès ; ces zones doivent apparaître explicitement sur la cartographie du SI et être filtrées suivant le strict besoin opérationnel.

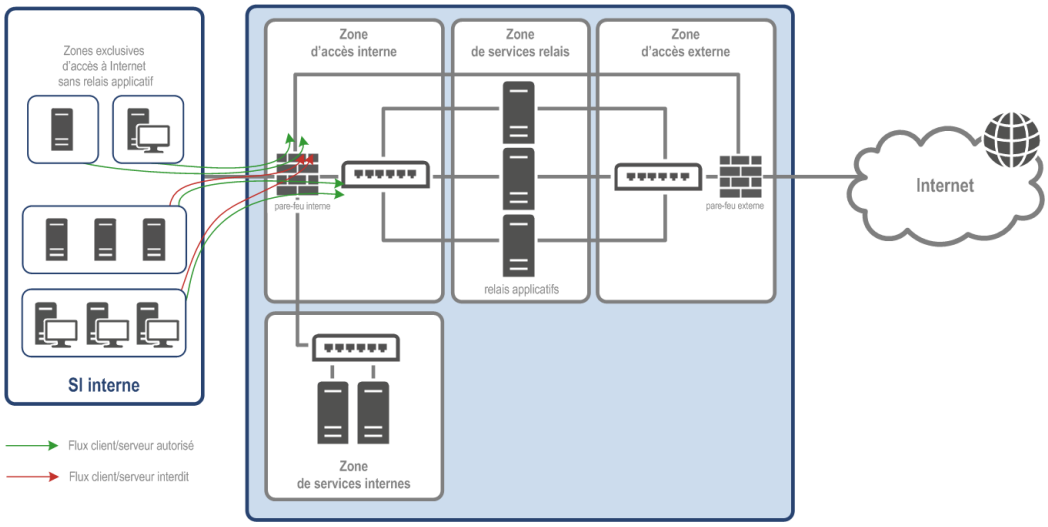


FIGURE 2.17 – Architecture d'une passerelle Internet sécurisée avec lien physique direct entre zones d'accès interne et externe

2.4.6 Cas particulier du DNS

Le protocole DNS permettant la conversion de noms de domaine en adresses IP est aujourd'hui indispensable pour accéder légitimement à des ressources aussi bien sur les réseaux privés que sur Internet. Dans le même temps, il peut constituer un canal privilégié d'exfiltration de données pour un attaquant qui en détournerait l'usage initial. Par exemple, cela peut être mis en œuvre après activation d'une charge malveillante (par hameçonnage, piégeage de clé USB, etc.) depuis une ressource (poste de travail ou serveur) connectée à Internet. Il est donc indispensable de bloquer toute possibilité technique d'établir un canal DNS direct (ou indirect) depuis une ressource du SI interne vers Internet.

Si l'exhaustivité des recommandations relatives à une architecture DNS n'est pas l'objet de ce guide, il convient d'évoquer celles nécessaires à la compréhension des choix d'architecture recommandés pour une passerelle Internet sécurisée :

- des résolveurs DNS doivent être dédiés dans le SI interne pour les résolutions de noms DNS internes (adressage privé de l'entité) ;
- des résolveurs DNS doivent être dédiés dans la passerelle Internet sécurisée pour les résolutions de noms DNS publics (adressage sur Internet) ;

- les résolveurs pré-cités ne doivent pas communiquer entre eux ;
- les ressources du SI interne (postes de travail, serveurs) ne doivent adresser leurs requêtes de noms DNS internes qu'aux résolveurs DNS internes ; en conséquence le pare-feu interne doit par défaut bloquer tous les flux DNS ;
- les relais de la passerelle Internet sécurisée ne doivent adresser les requêtes de noms DNS publics qu'aux résolveurs DNS publics.

Ces recommandations sont représentées sur la figure 2.18.

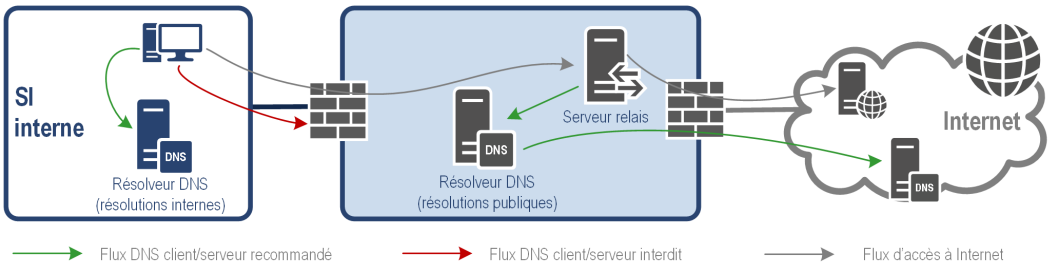


FIGURE 2.18 – Cinématique des flux DNS

2.5 Raccordement des sites géographiques

Pour une entité disposant de plusieurs sites géographiques reliés par un réseau privé étendu (WAN [8]), il est possible de mutualiser la passerelle Internet sécurisée. Dans ce cas, on parle d'architecture multi-sites (cf. figure 2.19).

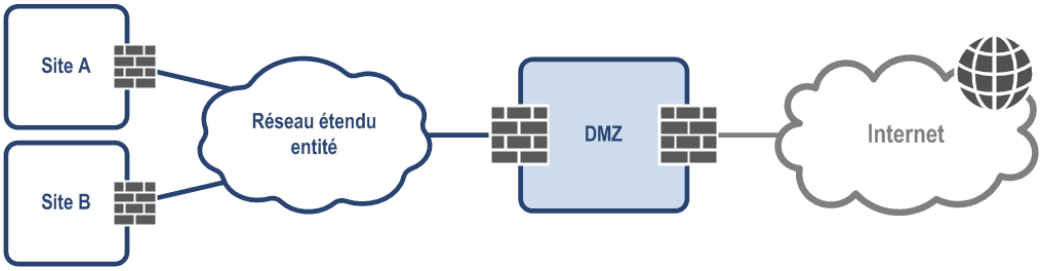


FIGURE 2.19 – Architecture multi-sites

La minimalisation du nombre d'accès à Internet est recommandée dans la mesure où elle simplifie l'exploitation. Toutefois, pour répondre aux besoins de grandes entités (avec de nombreux utilisateurs) ou d'entités disposant de sites géographiques éloignés, il peut être nécessaire, généralement pour des raisons de performance, de démultiplier ce type de passerelle. On parle alors d'architecture multi-zones (cf. figure 2.20).

8. L'acronyme anglais WAN pour *Wide Area Network* est le plus couramment utilisé.

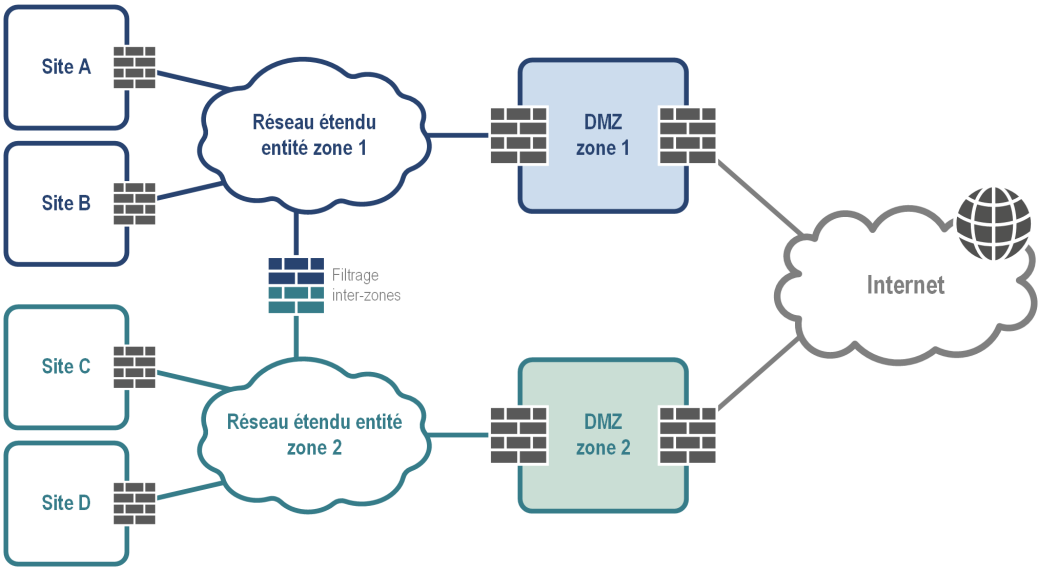


FIGURE 2.20 – Architecture multi-zones

R14

Homogénéiser les passerelles Internet sécurisées dans le cas d'une architecture multi-zones

Dans le cas d'une architecture multi-zones nécessitant de démultiplier le point d'accès à Internet et donc la passerelle Internet sécurisée, il est recommandé de déployer la même architecture (ou un sous-ensemble) et les mêmes produits pour chaque passerelle Internet sécurisée.

Attention

Certaines entités choisissent de mettre en œuvre un service « d'évasion Internet locale ». Cette solution, qui consiste à router le trafic à destination d'Internet vers un accès Internet local au site, est généralement motivée pour des questions de performance en évitant la remontée de trafic Internet jusqu'à une passerelle Internet sécurisée centralisée. Toutefois, du point de vue de la sécurité, elle n'est pas satisfaisante dès que :

- une simple liste de contrôle d'accès (*Access control list*) sur le routeur d'accès est la seule protection périmétrique vis-à-vis d'Internet (non respect de la recommandation R2) ;
- les flux entrants et sortants ne sont pas analysés (non respect de la recommandation R9) ou sont échangés sans protection cryptographique suffisante avec un prestataire externe (cf. recommandation R15).

Toutefois, pour ne pas remettre en cause le concept d'un réseau étendu s'appuyant sur Internet comme réseau de transport, des solutions existent. Par exemple, l'accès Internet local au site peut servir à l'établissement d'un tunnel IPsec et au routage des flux jusqu'à une passerelle Internet sécurisée de l'entité. La conception et la sécurisation d'une telle architecture dépassent le cadre de ce guide.

2.6 Externalisation des fonctions de relais

Pour des raisons opérationnelles ou budgétaires, l'entité peut souhaiter externaliser, généralement grâce à une offre de service logiciel à la demande (SaaS [9]), certaines fonctions de relais (ex. : serveur mandataire, antispam). Si du point de vue de la sécurité, une telle offre peut présenter des avantages de maintien en condition de sécurité et de mise à disposition de fonctions avancées, il est recommandé que cette offre soit qualifiée selon le référentiel d'exigences SecNumCloud [18].

Par ailleurs, dans le cadre d'une analyse de risque, il convient pour l'entité d'identifier les risques spécifiques à l'externalisation d'un de ces services qui sont à considérer comme critiques (cf. le guide afférent de l'ANSSI [2]).

Quoi qu'il en soit, il est nécessaire de protéger en intégrité et en confidentialité l'interconnexion du SI de l'entité avec le fournisseur de service. La mise en place d'un tunnel VPN IPsec est donc recommandée dans ce cas (cf. figure 2.21).

R15

Utiliser une offre qualifiée par l'ANSSI pour les fonctions relais externalisées

Si l'entité fait le choix d'externaliser dans le *cloud* une fonction relais, il est recommandé que le service afférent soit qualifié selon le référentiel d'exigences SecNumCloud [18] de l'ANSSI.
De plus, il est recommandé que l'interconnexion avec le fournisseur du service soit réalisée au travers d'un tunnel VPN IPsec à l'état de l'art (cf. le guide IPSec [7] de l'ANSSI).

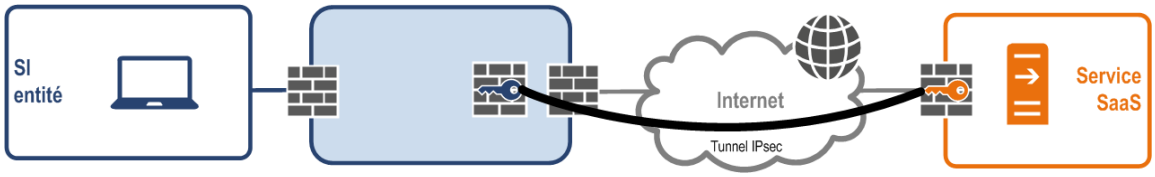


FIGURE 2.21 – Raccordement de la passerelle Internet sécurisée avec un service SaaS assurant une fonction relais

À la date de publication de ce guide, il n'existe pas de telle offre qualifiée par l'ANSSI. Toutefois, pour des entités ayant peu de ressources internes à consacrer à l'exploitation de ces services, il peut être préférable de recourir dès à présent à des services spécialisés externalisés.

R15 -

Évaluer rigoureusement les risques d'une offre non qualifiée par l'ANSSI pour les fonctions relais externalisées

Pour des entités souhaitant externaliser une fonction relais vers une offre de service non qualifiée par l'ANSSI, l'analyse de risque doit être menée avec d'autant plus de rigueur et d'exhaustivité.

9. L'acronyme anglais SaaS pour *Software as a Service* est le plus couramment utilisé.

2.7 Schéma d'architecture multi-services

En conclusion de ce chapitre consacré à l'architecture d'une passerelle Internet sécurisée, il est proposé sur la figure 2.22 un schéma d'architecture multi-services reprenant différents cas d'usage de la passerelle Internet sécurisée qui ne se veulent toutefois pas exhaustifs.

Voici quelques remarques sur les mutualisations et cloisonnements représentés (les numéros de cette liste sont reportés sur la figure 2.22 sous la forme ① à ⑧).

Conformément à la recommandation R6 :

1. les pare-feux périmétriques (internes d'une part et externes d'autre part) sont dédiés par chaîne d'usage : flux entrants liés à l'hébergement, flux VPN entrants pour l'accès des collaborateurs au SI, flux sortants ;
2. pour les pare-feux externes, le choix d'un cloisonnement physique (*n* pare-feux physiques dédiés), logique (*n* pare-feux virtuels dédiés sur un socle de pare-feu physique) ou hybride doit être déterminé par l'analyse de risque ;
3. la remarque 2 s'applique également pour les pare-feux internes ;
4. s'agissant des ressources (serveurs, etc.) de la zone de services relais, celles-ci sont dédiées par chaîne d'usage et le choix d'un cloisonnement physique (une ressource physique dédiée) ou logique (une machine virtuelle dédiée sur un socle physique mutualisé) doit être déterminé par l'analyse de risque ;

Par ailleurs :

5. les pare-feux internes et externes ne sont pas mutualisés conformément à la recommandation R13 ;
6. les flux VPN entrants pour l'accès des collaborateurs au SI ne font pas l'objet d'une analyse en amont du concentrateur VPN pour ne pas interrompre le flux IPsec (ou TLS) chiffré et authentifié, conformément au message d'avertissement page 14 ;
7. les flux de synchronisation d'annuaire sont à l'initiative de l'annuaire du SI interne vers l'annuaire dédié de la passerelle Internet sécurisée conformément aux recommandations R7 et R10 ;
8. la passerelle Internet sécurisée est administrée depuis un système d'information d'administration sécurisé, conformément à la recommandation R16 (cf. section 3.1).

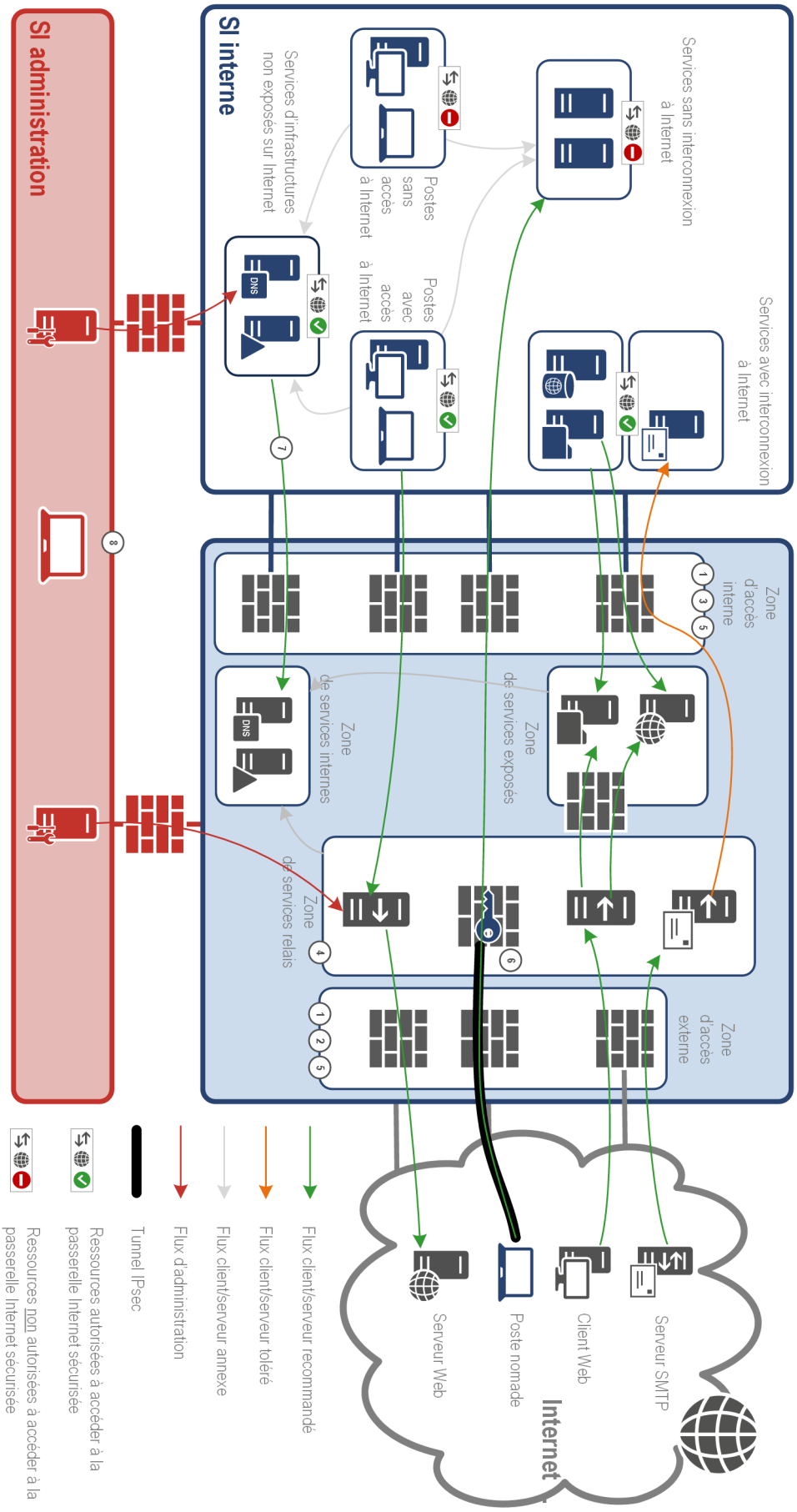


FIGURE 2.22 – Architecture multi-services de la passerelle Internet sécurisée

3
Sécurisation de l'interconnexion

3.1 Administration

Comme toute partie d'un SI, la passerelle Internet sécurisée doit être administrée de manière sécurisée. Pour cela, le lecteur doit se référer aux recommandations de l'ANSSI relatives à l'administration sécurisée.

R16

Administrer de manière sécurisée la passerelle Internet sécurisée

La passerelle Internet sécurisée doit être administrée de manière sécurisée selon les recommandations de l'ANSSI rassemblées dans le guide afférent [12].

3.2 Disponibilité

Comme évoqué en introduction, la disponibilité de l'accès Internet peut être critique pour une entité, qu'il s'agisse des services auxquels elle accède ou des services qu'elle héberge. L'entité doit donc prendre des mesures visant à garantir la disponibilité en phase avec ses objectifs de sécurité.

En premier lieu, il est recommandé de multiplier autant que possible les chemins de raccordement physique (généralement deux) pour éviter tout point unique de rupture.

Par ailleurs, les équipements d'accès (ex. : routeurs) peuvent être doublés et/ou double alimentés électriquement pour pallier une panne matérielle ou d'alimentation électrique.

Dans l'hypothèse de deux accès, le choix d'un FAI distinct par accès permet de pallier une interruption de service au niveau d'un cœur de réseau. Dans le cas des accès entrants, cela peut nécessiter un travail de gestion de routage dynamique (gestion d'AS, *Autonomous System*) au niveau de l'interconnexion pour garantir que l'acheminement des flux puisse s'effectuer correctement via l'un ou l'autre des réseaux opérateur.

R17

Garantir la disponibilité attendue grâce à la résilience des accès opérateurs

L'entité doit prendre les mesures nécessaires pour garantir la disponibilité attendue de l'accès à Internet :

- travaux de génie civil pour éviter tout point unique de rupture ;
- déploiement d'équipements supplémentaires pour assurer la redondance matérielle ;
- configuration logicielle pour garantir une résilience réseau protocolaire.

Il est aujourd'hui possible d'acheter en ligne des « prestations » de déni de service distribué (DDoS [10]). Ces prestations sont accessibles pour un coût modique (inférieur à une centaine d'euros) à des profils malveillants ne disposant pas nécessairement de compétences techniques avancées. Ce type d'attaque, s'il réussit, peut nuire fortement à la disponibilité de l'accès Internet de l'entité et donc à son image ou à sa performance. Des solutions techniques, généralement proposées par les FAI, peuvent permettre de contrer une telle attaque.

R18

Mettre en œuvre des contre-mesures aux attaques en déni de service

Qu'il s'agisse d'un service souscrit auprès d'un FAI ou géré en propre par l'entité, il est recommandé de déployer une solution de protection anti-DDoS.

Information

L'ANSSI publie un guide pour comprendre et anticiper les attaques en déni de service distribué [6].

La fonction de routage représente un élément critique de la passerelle Internet sécurisée. En effet, elle détermine l'ensemble des chemins possibles entre le SI de l'entité et Internet. Afin de se prémunir de l'apparition de chemins non souhaités, le routage statique doit être privilégié au sein de la passerelle Internet sécurisée.

R19

Utiliser un routage statique au sein de la passerelle Internet sécurisée

Au sein de la passerelle Internet sécurisée, il est recommandé de déclarer statiquement les routes IP dans les équipements réseau et de désactiver explicitement les protocoles de routage dynamique.

Attention

En particulier, dans le cas d'une éventuelle route par défaut configurée sur le pare-feu interne, il convient de s'assurer que celle-ci n'est pas configurée vers le pare-feu externe (donc vers Internet). En effet, une erreur de configuration avec l'ajout d'une règle de pare-feu interne trop permissive autorisant un flux vers une destination quelconque (*any*) créerait une faiblesse dans l'architecture.
Le cas échéant, il est recommandé de configurer la route par défaut du pare-feu interne vers le SI interne.

3.3 Confidentialité

Afin d'éviter toute fuite d'information sur les politiques de filtrage mises en place vis-à-vis d'Internet, il est recommandé de rendre « silencieux » les pare-feux externes, c'est-à-dire qu'un paquet accepté doit être routé (`ACCEPT`), un paquet refusé doit être ignoré (`DROP`) sans provoquer l'envoi d'une réponse ICMP (`REJECT`).

10. L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.

R20

Ignorer les paquets refusés par la politique des pare-feux externes

Il est recommandé que les connexions refusées par la politique d'un pare-feu externe ne génèrent pas de réponses (mode `DROP` et non `REJECT`).

Afin d'éviter toute fuite d'information technique permettant à un attaquant de reconstituer tout ou partie de l'infrastructure de l'entité, il peut être nécessaire d'anonymiser certains champs techniques (ex. : nom et adresse IP des serveurs relais de messagerie dans les en-têtes de courriels, champs *Referer* et *Origin* dans les en-têtes HTTP).

R21

Masquer l'architecture interne vis-à-vis d'Internet

Dès lors que c'est techniquement possible, il est recommandé d'anonymiser les champs techniques divulguant de l'information sur les infrastructures internes de l'entité.

Information

La recommandation R21 est bien à considérer comme complémentaire et moins prioritaire dans la mesure où la sécurité par l'obscurité n'est pas le principe directeur de sécurisation de l'architecture d'interconnexion à Internet.

4
Sécurisation de l'accès aux contenus hébergés sur le Web

L'accès aux contenus hébergés sur le Web (ex. : navigation Web des utilisateurs, récupération de sources logicielles pour le maintien en condition de sécurité, etc.) est un des besoins liés à Internet les plus courants pour une entité. Dans ce chapitre, des recommandations spécifiques à la passerelle Internet sécurisée sont d'abord présentées. Des compléments sur la configuration du poste de travail pour la navigation Web des utilisateurs sont ensuite proposés dans la section 4.6 (cf. page 34).

4.1 Mise en place d'un serveur mandataire

Il est essentiel d'éviter tout accès direct depuis un poste utilisateur ou un serveur vers le Web. Pour cela, un serveur mandataire (*proxy*) Web doit assurer le rôle de relais et mettre en œuvre des fonctions de sécurité : authentification, contrôle d'accès, analyse de contenus, journalisation, etc.

On convient de parler d'*un* serveur mandataire mais une grappe (ou *cluster*) de serveurs mandataires peut être déployée pour garantir la haute disponibilité ou séparer des chaînes d'accès (ex. : pour les postes de travail d'une part, pour les serveurs d'autre part). À défaut d'être unique, il est recommandé que les serveurs mandataires soient exploités de manière centralisée pour permettre une application simple et rapide des politiques de sécurité et faciliter la journalisation.

R22

Mettre en place un serveur mandataire pour l'accès aux contenus Web

Pour l'accès aux contenus hébergés sur le Web, un serveur mandataire doit être mis en place au sein de la zone de services relais de la passerelle Internet sécurisée.

Pour des raisons opérationnelles ou budgétaires, l'entité peut souhaiter, de manière alternative, souscrire à une offre SaaS de serveur mandataire. Le cas échéant et conformément à R15, il est recommandé que le service soit qualifié selon le référentiel d'exigences SecNumCloud [18] de l'ANSSI et que l'interconnexion avec le fournisseur soit réalisée à travers un tunnel VPN IPsec à l'état de l'art (cf. le guide IPSec [7] de l'ANSSI).

Attention

Il existe sur le marché de nombreuses solutions de serveurs mandataires, libres ou propriétaires. Ce sont généralement des produits complexes, embarquant de nombreuses fonctionnalités. Une bonne maîtrise de cet équipement est alors indispensable pour maîtriser la sécurité de l'accès aux contenus hébergés sur le Web.

Des précisions sur la configuration du serveur mandataire sur les postes de travail sont apportées dans la section 4.6.2 (cf. page 35).

4.2 Authentification

À des fins de contrôle d'accès et d'imputabilité des connexions, il est recommandé d'authentifier tous les accès aux contenus hébergés sur le Web : avec des comptes individuels pour les utilisateurs (exceptionnellement de comptes génériques si le suivi de leur utilisation peut être tracé), des comptes de service pour les applications.

En effet, l'absence d'authentification a plusieurs conséquences :

- il n'est pas possible de réaliser un filtrage spécifique selon les catégories d'utilisateurs (standards, privilégiés, restreints, etc.) ;
- l'accès sortant par un code malveillant s'exécutant sur une ressource interne est facilité ;
- la traçabilité des accès sortants est limitée à l'adresse IP d'origine de la requête (voire celle d'un équipement de routage en cas de traduction d'adresse), et n'intègre pas l'identité de l'utilisateur, ce qui complexifie les recherches en cas d'intrusion.

R23

Authentifier tous les accès aux contenus Web

Tous les accès aux contenus hébergés sur le Web doivent être authentifiés de manière individuelle pour les utilisateurs et non ambiguë pour les services.
À défaut, pour un compte générique, une traçabilité de son utilisation (relevé d'identité) doit être mise en place.

Pour des raisons techniques, il est possible que certains accès ne soient pas authentifiables (ex. : logiciel ne prenant pas en charge la saisie d'un identifiant et d'un mot de passe associés à la configuration d'un accès par serveur mandataire). Dans ce cas, une liste d'autorisations (aussi appelée liste blanche) peut être gérée sur la base de la source et/ou de la destination (ex. : une application hébergée sur un serveur avec une adresse IP fixe interne accédant au site de son éditeur pour réaliser ses mises à jour et ne supportant pas l'authentification). Il est recommandé que le serveur mandataire autorise explicitement les seules adresses IP source à accéder sans authentification au domaine DNS du site distant.

R24

Prévoir des restrictions pour les accès non authentifiables

Les exceptions à la recommandation R23 (typiquement les logiciels ne supportant pas l'authentification à un serveur mandataire) doivent être gérées grâce à une liste d'autorisations contenant les adresses IP ou domaines exemptés d'authentification.
Dans ce cas, il est recommandé d'être le plus proche possible du besoin opérationnel et d'éviter tout ajout à la liste d'autorisations d'un large masque de sous-réseau (ex. : supérieur à /24 en IPv4) ou d'un domaine DNS très étendu (ex. : `*.moncdn.fr`).

4.3 Inspection TLS

Le nombre de sites accessibles en HTTPS est en constante augmentation et constitue une avancée majeure dans la sécurisation des communications dans la mesure où la configuration TLS associée est à l'état de l'art (cf. le guide TLS de l'ANSSI [14]).

La contrepartie est que, s'il s'agit d'accès à des sites d'hameçonnage (*phishing*) ou d'hébergement de codes malveillants, il est théoriquement impossible de détecter le contenu suspect dans l'ensemble du trafic chiffré. Pour pallier cela, la mise en place d'inspection TLS est une possibilité. Celle-ci doit permettre *in fine* d'analyser le contenu et de s'assurer de la conformité protocolaire des échanges.

Attention

Tel que mentionné dans le guide de recommandations de sécurité concernant l'analyse des flux HTTPS [8], « *[...] la mise en place de mécanismes de déchiffrement HTTPS présente des risques dans la mesure où cette opération entraîne la rupture d'un canal sécurisé et expose des données en clair au niveau de l'équipement* [11] *en charge de l'opération. Lorsqu'un tel déchiffrement est nécessaire, sa mise en œuvre doit s'accompagner de beaucoup de précautions [...]* ».

L'inspection TLS répond donc au besoin de détection de codes malveillants et doit, le cas échéant, être mise en œuvre de façon sécurisée au sein de la zone de services relais. Le choix de l'équipement réalisant cette inspection est structurant ; celui-ci doit notamment permettre une configuration des paramètres cryptographiques à l'état de l'art (cf. l'annexe B1 du Référentiel général de sécurité [16]).

R25

Étudier la mise en place d'une inspection TLS maîtrisée

Afin de se prémunir de la diffusion de codes malveillants par le biais de sites accessibles en HTTPS, il est recommandé d'étudier la mise en place d'une inspection TLS permettant d'analyser le contenu échangé.
Le lecteur doit s'approprier au préalable les recommandations de sécurité concernant l'analyse des flux HTTPS dans le guide [8]. Entre autres, le choix de l'équipement d'inspection et la configuration de ses paramètres cryptographiques doivent être considérés avec la plus grande attention.
Enfin, en vertu du respect de la vie privée des collaborateurs, une liste de sites réputés de confiance et non inspectés doit être établie (ex. : sites bancaires) et partagée avec les utilisateurs.

Attention

La mise en œuvre d'inspection TLS pour détecter des codes malveillants est un complément et non une alternative aux mesures de détection propres aux équipements terminaux (ex. : antivirus sur les postes de travail ou serveurs accédant au Web).

11. N.D.R. : le serveur mandataire généralement.

4.4 Journalisation

Dans le contexte de la passerelle Internet sécurisée et de l'accès aux contenus hébergés sur le Web, il convient de distinguer deux types de journaux :

- les journaux d'événements techniques des équipements ;
- les journaux d'accès (utilisateurs ou services) aux contenus Web.

Si l'objectif de journalisation peut différer (supervision de sécurité ou investigation numérique *a posteriori* pour les premiers, obligation légale pour les seconds), il convient que ceux-ci soient centralisés et conservés intègres.

R26

Centraliser et sécuriser les journaux liés aux accès Web

L'ensemble des journaux (techniques et fonctionnels) générés par les serveurs mandataires doivent être centralisés, de préférence par l'intermédiaire d'un réseau d'administration dédié (cf. R16).
Il est recommandé de consulter les recommandations de sécurité de l'ANSSI pour la mise en œuvre d'un système de journalisation [4], en particulier le paragraphe C.3.1 sur la conservation des éléments de journalisation par les fournisseurs d'accès à Internet.

4.5 Déploiement de postes de rebond

Pour les entités ayant des objectifs élevés de sécurité, il peut être envisagé de déployer une infrastructure de postes de rebond sur lesquels les utilisateurs se connectent depuis leur poste bureautique par accès à distance. *In fine* ce sont les postes de rebond qui permettent de naviguer sur le Web. La rupture protocolaire permise par l'accès à distance renforce le cloisonnement du poste bureautique vis-à-vis d'Internet. De façon complémentaire, ces postes de rebond peuvent être des machines virtuelles temporaires, détruites après utilisation afin d'éviter toute persistance d'une attaque.

Même dans ce cas de figure et conformément à R22, les postes de rebond accèdent aux contenus Web à travers un serveur mandataire. De plus, il sont dédiés à cet usage et ne permettent pas d'autres utilisations (ex. : pas d'autres applications installées qu'un navigateur Web). Cette architecture est représentée sur la figure 4.1.

R27 +

Déployer des postes de rebond pour la navigation Web

Pour répondre à des objectifs de sécurité élevés, il est recommandé de déployer une infrastructure de postes de rebond dédiés à la navigation Web sur lesquels les utilisateurs se connectent par accès à distance depuis leur poste de travail bureautique.
Les postes de rebond doivent utiliser le serveur mandataire de la passerelle Internet sécurisée pour accéder aux contenus hébergés sur le Web.

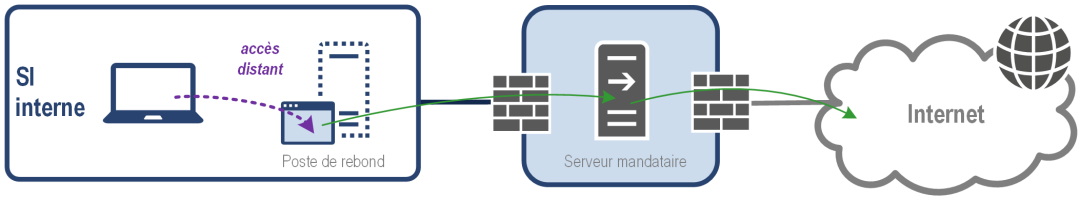


FIGURE 4.1 – Infrastructure de postes de rebond pour la navigation Web

4.6 Configuration des postes de travail pour la navigation Web

Avant tout, les postes de travail des utilisateurs sont supposés conformes aux pratiques d'hygiène informatique, dont entre autres :

- être à jour (système d'exploitation et logiciels) ;
- activer un pare-feu local ;
- disposer d'un anti-virus.

4.6.1 Maîtrise d'un ou plusieurs navigateurs Web

L'ANSSI ne se prononce pas en faveur de tel ou tel navigateur Web : Microsoft Edge, Google Chrome, Mozilla Firefox, Safari, etc. Chacun présente ses avantages et inconvénients fonctionnels et de sécurité.

L'utilisation d'un navigateur Web conforme aux standards du Web et maintenu à jour par son éditeur est indispensable. La maîtrise de son déploiement et de son exploitation (configuration centralisée, mises à jour, gestion des greffons ou *plugins*, etc.) constitue dès lors l'enjeu majeur du point de vue de la sécurité. Le déploiement maîtrisé d'une seule solution est préférable par rapport au déploiement de plusieurs solutions inégalement maîtrisées.

R28

Maîtriser le déploiement et l'exploitation du ou des navigateurs Web

En tant qu'interface d'accès des utilisateurs au Web, le ou les navigateurs Web déployés sur les postes de travail doivent être configurés et mis à jour selon des procédures strictes.
En particulier leur surface d'attaque doit être réduite au strict nécessaire par désactivation de tout module ou paramètre inutile.

Certaines entités font le choix de déployer un navigateur pour la navigation interne (ex. : sites intranet) et un navigateur pour la navigation Web. Cette solution peut constituer une bonne pratique dans la mesure où la recommandation R28 est respectée pour les deux navigateurs. En effet, si l'entité doit maintenir un navigateur interne obsolète pour des raisons fonctionnelles (ex. : une application métier historique non conforme aux standards Web), il n'est pas suffisant de considérer qu'il est « moins exposé » ; des mesures complémentaires doivent être prises, par exemple la conteneurisation du navigateur voire l'utilisation de postes de travail dédiés.

4.6.2 Configuration du serveur mandataire

Pour une meilleure maîtrise des flux sur le réseau de l'entité, le serveur mandataire doit être configuré en mode *explicite* et non *transparent* vis-à-vis des clients. Cela se justifie par deux raisons :

- éviter un routage d'adresses IP publiques sur le réseau privé de l'entité, voire un routage par défaut vers ce serveur mandataire – un serveur mandataire configuré en mode transparent sur les clients doit « attirer » le trafic à destination d'Internet ;
- pouvoir interdire les résolutions DNS publiques (ex. : adresse Web) depuis les postes de travail ; celles-ci sont alors inutiles localement car gérées par le serveur mandataire et le risque d'une exfiltration par le canal DNS depuis le poste est ainsi réduit (cf. paragraphe 2.4.6 page 21).

R29

Configurer le serveur mandataire en mode explicite

Du point de vue de la sécurité, le serveur mandataire doit être configuré en mode explicite sur les clients.

Afin de ne pas affaiblir le niveau global de sécurité du SI de l'entité, il est nécessaire que tous les postes de travail, y compris les postes nomades, ne puissent pas accéder directement à Internet. En situation de nomadisme, il est fortement recommandé que les postes de travail se connectent de manière sécurisée à travers un tunnel VPN au SI de l'entité puis accèdent à Internet à travers la passerelle Internet sécurisée (cf. figure 3.2 du guide de l'ANSSI sur le nomadisme numérique [13]).

R30

Empêcher le contournement du serveur mandataire

Il doit être techniquement impossible pour l'utilisateur de contourner les équipements de sécurité pour accéder à Internet.
En particulier, la configuration du serveur mandataire dans les navigateurs Web doit être non modifiable par l'utilisateur ou un logiciel tiers.
Dans un souci de défense en profondeur, le pare-feu local des postes de travail doit bloquer tout accès direct à Internet (sauf exception pour l'accès au concentrateur VPN de l'entité).
Cette recommandation est également valable pour toute autre ressource (ex. : serveur ou mobile multifonction [12] sous contrôle de l'entité) nécessitant d'accéder au Web à travers un navigateur ou les protocoles HTTP/HTTPS.

Attention

Si cette configuration est incompatible avec les technologies de portail captif, elle est le seul moyen de garantir que le poste sera protégé en toutes circonstances. Même temporaire, un accès à ce type de portail annihile la confiance dans un poste. L'utilisation de solutions d'accès alternatives est recommandée.

Le serveur mandataire peut être déclaré simplement par une politique de configuration (ex. : *Group Policy Object* sur Windows) permettant l'ajout d'un nom DNS ou d'une adresse IP dans les paramètres du navigateur Web.

12. Le terme anglais *smartphone* est plus couramment utilisé.

R31

Appliquer une politique de configuration locale du serveur mandataire

Il est recommandé de déclarer le serveur mandataire localement sur les postes accédant à Internet, idéalement grâce à une politique de configuration.
Cette recommandation est également valable pour toute autre ressource (ex. : serveur ou mobile multifonction [12] sous contrôle de l'entité) nécessitant d'accéder au Web à travers un navigateur ou les protocoles HTTP/HTTPS.

En complément, des plages d'adresses IP (ex. : plage privée 10.0.0.0/8) ou des noms de domaine locaux peuvent être déclarés en exception pour éviter l'envoi de trafic interne au SI vers le serveur mandataire de la passerelle Internet sécurisée.

Supporté par la plupart des navigateurs, le fichier .PAC (*proxy auto-config*) permet de définir finement la politique de configuration du serveur mandataire, en fonction de la destination notamment. Par exemple, les flux internes sont envoyés directement alors que les flux à destination d'Internet sont envoyés vers le serveur mandataire.

Un déploiement du fichier .PAC directement sur les postes de travail est possible. Toutefois, la mise à disposition sur un serveur Web interne est généralement préférée. En effet, cela permet une reconfiguration plus rapide au besoin, sans nécessité de redéployer le fichier unitairement par poste.

Le cas échéant, l'adresse cible du fichier PAC (ex. : `https://monserveur/proxy.pac`) est spécifiée dans la configuration des navigateurs. Ce fichier doit être récupéré via le protocole HTTPS et non HTTP. Le certificat du serveur Web doit être signé par une autorité de certification déclarée au niveau du navigateur.

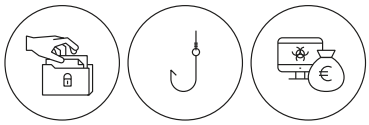
Cette solution alternative à la recommandation R31 présente des avantages fonctionnels mais induit un risque d'interception et d'altération du fichier de configuration pouvant mener à un détournement du trafic.

Attention

Le protocole *Web Proxy Autodiscovery Protocol* (WPAD) est une alternative au fichier .PAC ; il s'appuie sur DHCP et DNS pour la récupération d'un fichier de configuration `wpad.dat`. Même s'il est relativement simple à mettre en œuvre pour le déploiement d'une configuration automatique de serveur mandataire, plusieurs vulnérabilités affectent ce protocole. Son utilisation est donc à proscrire *absolument*.

5
Sécurisation du service de messagerie électronique

Un deuxième service très utilisé, et nécessitant généralement l'interconnexion à Internet, est la messagerie électronique. Son usage pour les besoins professionnels est très répandu, quels que soient la taille et le secteur d'activité de l'entité. Les boîtes aux lettres électroniques regorgent d'informations métier ou techniques qui, agrégées, en font des cibles de choix pour les attaquants. Dans le même temps, ce service est devenu un des principaux vecteurs d'attaque informatique : tentative d'hameçonnage [13] pour récupérer des données personnelles, envoi de pièces jointes malveillantes pour exploiter les vulnérabilités d'un poste de travail à des fins de rançonnage ou d'espionnage, etc.



Dès lors, la sécurisation de ce service est indispensable pour réduire le risque d'accès illégitimes et le risque de réception – voire d'envoi à l'insu de l'entité – de courriels à des fins malveillantes. Différentes mesures complémentaires peuvent être mises en œuvre comme :

- des mesures d'architecture (section 5.2) ;
- la protection en confidentialité et l'authentification des canaux de transport (section 5.3) ;
- la protection contre les courriels illégitimes (section 5.4).

La protection en disponibilité du service de messagerie (section 5.5) peut également être importante pour l'entité.

Information

Ce chapitre traite spécifiquement la sécurisation du *service de messagerie électronique* dans le cadre d'une passerelle Internet sécurisée, et non de la sécurisation des *messages électroniques* – qui est un sujet connexe tout aussi important. Ainsi les mécanismes cryptographiques, tels que la signature ou le chiffrement de bout en bout des courriels, ne sont pas abordés ici.
Par ailleurs, le lecteur doit disposer des connaissances minimales sur le fonctionnement d'un service de messagerie électronique pour appréhender ce chapitre.

13. Le terme anglais *phishing* est couramment utilisé.

5.1 Expression de besoin et analyse de risque

Conformément à la recommandation R1, la messagerie électronique est généralement identifiée comme un service nécessitant une interconnexion à Internet avec des flux entrants et sortants. Il convient toutefois de détailler ce besoin selon les activités de l'entité et de distinguer :

- la messagerie pour les échanges des collaborateurs, entre eux ou avec l'extérieur, dite *messagerie bureautique* ;
- la messagerie pour les activités métier, par exemple pour les échanges avec les clients dans le cadre d'un service après-vente ; celle-ci, dite *messagerie métier*, est potentiellement interconnectée à un progiciel de gestion de la relation client ;
- la messagerie pour les besoins techniques, de supervision ou d'alerte ; celle-ci, dite *messagerie technique*, est généralement interconnectée à des outils de supervision ou de suivi de tickets, et permet parfois des échanges machine à machine.

Il est important d'identifier les messageries qui nécessitent la réception ou l'envoi de courriels, lesquelles doivent être interconnectées entre elles, et lesquelles nécessitent une interconnexion à Internet. Par exemple, une messagerie technique peut être cloisonnée au sein du SI de l'entité sans interconnexion à Internet, alors qu'une messagerie métier peut nécessiter l'envoi et la réception de courriels sur Internet.

R32

Identifier les différents besoins liés à la messagerie électronique

Pour le service de messagerie électronique, l'entité doit identifier les différents besoins : réception ou envoi de courriels, interconnexion à Internet, rôles des expéditeurs (ex. : utilisateurs, services), noms de domaines associés, etc.

Une fois ces besoins identifiés, il convient de mener une analyse de risque spécifique au service de messagerie électronique, selon une méthodologie telle EBIOS *Risk manager* [10] ou, pour les entités moins matures, sur la base de questions simples, pour identifier les besoins de sécurité :

- quelle est l'indisponibilité acceptable de ce service ?
- quelles seraient les conséquences de la destruction de l'ensemble des courriels ?
- quelles seraient les conséquences de la récupération de l'ensemble des courriels par un tiers, éventuellement le fournisseur du service de messagerie ou un concurrent ?
- quelles seraient les conséquences d'une usurpation d'identité de l'expéditeur ?

Par ailleurs, les recommandations d'architecture proposées dans ce chapitre, même dérogatoires par rapport à l'état de l'art, nécessitent des moyens financiers potentiellement importants pour financer des ressources humaines compétentes, des investissements matériels et des coûts récurrents. Par conséquent, l'analyse de risque doit évaluer les différents scénarios faisant intervenir de l'externalisation (pas d'externalisation, externalisation de l'hébergement seul, externalisation de l'administration seule, externalisation du service dans son ensemble) tout en précisant les conditions et les moyens associés. Le lecteur peut se reporter au guide de l'ANSSI sur le sujet de l'externalisation [2], qui aborde entre autres la réversibilité.

Enfin, l'administration fonctionnelle du service, qu'elle soit internalisée ou externalisée, doit également être traitée avec attention dans l'analyse de risque. En effet, les administrateurs de messagerie ont des droits privilégiés leur donnant accès aux paramètres et aux contenus des boîtes aux lettres.

R33

Ne pas externaliser le service de messagerie électronique sans une analyse de risque

Le niveau d'externalisation du service de messagerie électronique doit faire l'objet d'un traitement rigoureux dans le cadre d'une analyse de risque.
Dans le cas d'une offre SaaS et conformément à R15, il est recommandé que le service soit qualifié selon le référentiel d'exigences SecNumCloud [18] de l'ANSSI.

Information

Dans la suite de ce chapitre, la section 5.2 traite des questions d'architecture au sein de la passerelle Internet sécurisée. Elle ne concerne donc que les entités faisant le choix de conserver en interne la maîtrise de l'architecture du service de messagerie électronique.
Les sections 5.3, 5.4 et 5.5 s'adressent à toute entité, quel que soit le positionnement dudit service. Dans le cas d'une externalisation, certains paramétrages nécessiteront potentiellement l'intervention du prestataire.

5.2 Architecture

5.2.1 Composants

Afin de produire, stocker et transmettre des courriels, il existe un nombre important de composants logiciels intervenant dans un système de messagerie électronique. Il ne s'agit pas ici d'expliquer en détail ces différents composants du point de vue fonctionnel, mais d'avoir un vocabulaire commun pour expliquer les concepts de sécurité à appliquer.

De façon simplifiée, on distingue dans les systèmes de messagerie électronique :

- les clients de messagerie (*Mail User Agent*) qui permettent de produire et consulter des courriels ;
- les serveurs de boîtes aux lettres (*mailboxes*) qui stockent des courriels ;
- les serveurs de transfert de courriels (*Mail Transfer Agent*) dits aussi serveurs relais, ou serveurs SMTP (*Server Mail Transfer Protocol*) – du nom du protocole qu'ils utilisent majoritairement pour la transmission des courriels à travers les réseaux. Le premier serveur relais, qui accepte les courriels des clients de messagerie, est appelé (*Mail Submission Agent*) et le dernier serveur relais, qui délivre les courriels dans les boîtes aux lettres, est appelé (*Mail Delivery Agent*).

Information

Certaines solutions de messagerie électronique peuvent utiliser des protocoles alternatifs à SMTP pour les transferts internes à l'infrastructure. C'est le cas de Microsoft Exchange par exemple et l'utilisation de MAPI (*Messaging application programming*

interface). Toutefois, le transfert de courriels en dehors de l'infrastructure interne repose quasi-systématiquement sur SMTP. Ainsi, dans la suite du chapitre, le terme de *serveur relais* sera utilisé de manière générique et celui de *serveur SMTP* dès lors qu'il s'agit d'un serveur relais exposé sur Internet.

5.2.2 Cloisonnement et filtrage

Sauf cas particulier, les serveurs de boîtes aux lettres, accessibles par les clients de messagerie, doivent être hébergés au sein du SI de l'entité. Ils peuvent communiquer avec des serveurs relais internes au SI de l'entité, ou des serveurs SMTP, au sein de la passerelle Internet sécurisée, pour les échanges sur Internet.

R34

Déployer les serveurs de boîtes aux lettres au sein du SI

Les serveurs de boîtes aux lettres et le stockage associé doivent être déployés au sein du SI de l'entité (et non au sein de la passerelle Internet sécurisée).

R35

Déployer les serveurs relais en fonction des stricts besoins

Pour les besoins de messagerie strictement internes à l'entité, au moins un serveur relais doit être positionné au sein du SI de l'entité, et dédié à cette fonction. Ce serveur ne doit pas être chaîné avec un serveur SMTP exposé sur Internet.
Pour les besoins de messagerie externes à l'entité (*i.e.* avec une interconnexion à Internet), au moins un serveur SMTP doit être positionné au sein de la passerelle Internet sécurisée.

En cohérence avec la recommandation R6, il est recommandé de cloisonner les serveurs SMTP d'envoi et de réception au sein de la passerelle Internet sécurisée.

R36

Cloisonner les serveurs SMTP d'envoi et de réception

Il est recommandé de cloisonner les serveurs SMTP d'envoi et de réception (ex. : deux machines virtuelles distinctes) au sein de la passerelle Internet sécurisée. Ils doivent être configurés en conséquence ; par exemple :

- un serveur SMTP d'envoi n'accepte les courriels que depuis une liste de serveurs autorisés (serveurs relais internes ou serveurs de boîtes aux lettres) et assure des fonctions de nettoyage des en-têtes (cf. recommandation R21) ;
- un serveur SMTP de réception applique les premières politiques de sécurité, assure des fonctions d'analyse protocolaire et de contenu, qualifie les courriels nécessitant une mise en quarantaine, transmet *in fine* les courriers à un autre serveur relais de l'entité ou à un serveur de boîtes aux lettres.

La figure 5.1 représente une architecture type. Les flux représentés ne sont pas nécessairement exhaustifs ; l'absence de flux entre le serveur relais sans interconnexion avec Internet, hébergé dans le SI de l'entité, et la passerelle Internet sécurisée est toutefois volontaire.

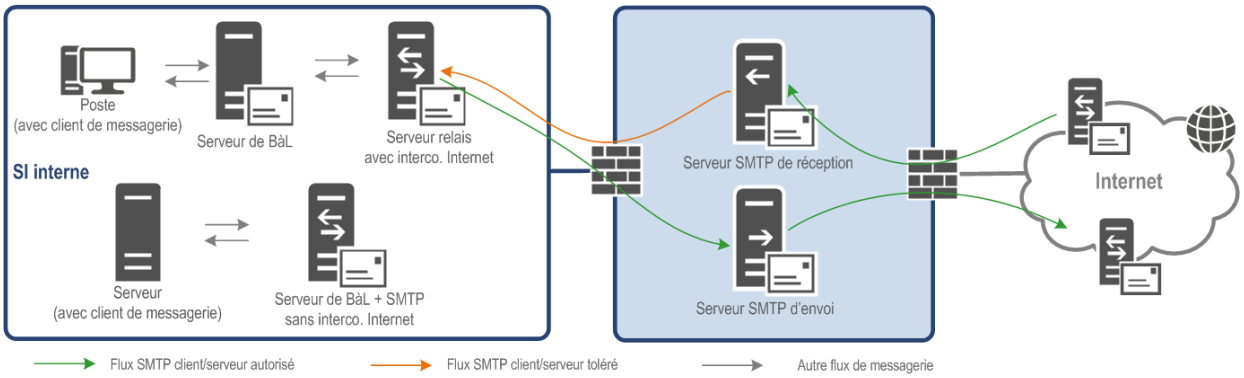


FIGURE 5.1 – Exemple d'architecture de messageries (interconnectées ou non à Internet)

Dès lors que les serveurs de boîtes aux lettres et les serveurs relais sont positionnés dans l'architecture, ils doivent être les seuls à pouvoir échanger grâce aux protocoles de messagerie (ex. : SMTP, MAPI). De plus, les clients de messagerie doivent se connecter exclusivement aux serveurs de boîtes aux lettres, avec les protocoles *ad hoc* (ex. : IMAPS, MAPI). Cela doit se traduire dans les matrices de flux internes, et propres à la passerelle Internet sécurisée, afin d'éviter l'envoi, ou la réception, de courriels par d'autres machines.

R37

N'autoriser les protocoles de messagerie qu'entre infrastructures légitimes

Afin d'éviter des usages détournés du service de messagerie électronique, les protocoles de messagerie doivent être autorisés selon le strict besoin opérationnel des infrastructures légitimes.
En particulier, l'utilisation illégitime des ports SMTP (TCP/25 sans chiffrement et TCP/465 avec chiffrement implicite) par un serveur autre qu'un serveur SMTP doit générer des journaux au niveau des pare-feux et une alerte de sécurité.

5.2.3 Mécanismes antispam et recherche de contenu malveillant

La messagerie électronique étant un vecteur de compromission, des mécanismes doivent être mis en œuvre pour tenter de détecter (et stopper dans la mesure du possible) au plus tôt les courriels indésirables (*spam*). Ces mécanismes doivent en particulier couvrir la recherche de contenu malveillant (ex. : une pièce jointe piégée ou un lien vers une page Web).

Le blocage des courriels indésirables, dont font partie les courriels d'hameçonnage (*phishing*), est généralement complexe à mettre en œuvre, d'un point de vue technique, pour être efficient. Il nécessite une attention particulière pour éviter les faux-positifs (un courriel bloqué qui ne serait en fait pas indésirable) ayant un impact direct pour les utilisateurs. Différents mécanismes d'analyse des en-têtes d'une part, et des corps de courriels d'autre part existent, par exemple :

- les listes d'autorisations, d'interdictions ou d'interdictions provisoires (aussi appelées listes blanche, noire et grise) d'adresses IP ou de noms de domaine permettant respectivement d'autoriser, de bloquer ou de bloquer temporairement les courriels en provenance de ces sources ;
- l'analyse heuristique du corps des courriels ;

- le test de Turing permettant d'identifier l'expéditeur comme un humain (ex. : reproduction d'un code affiché dans une image, ou calcul d'une opération lors de la réception du premier courriel d'un nouvel expéditeur).

L'activation de ces mécanismes complémentaires n'est pas nécessairement systématique pour chaque courriel reçu. Par exemple, un courriel reçu depuis un domaine présent dans une liste d'autorisations peut dispenser d'un test de Turing pour l'expéditeur. Ce test peut être activé en dernier recours pour un courriel dont le caractère indésirable n'a pas pu être déterminé par d'autres mécanismes.

R38

Mettre en œuvre des mécanismes antispam

Afin de limiter la réception des courriels indésirables dans les boîtes aux lettres, des mécanismes antispam doivent être mis en œuvre en amont, par exemple :

- l'utilisation de listes d'autorisations, d'interdictions ou d'interdictions provisoires d'adresses IP ou de noms de domaine ;
- l'analyse heuristique du corps des courriels ;
- le test de Turing pour les nouveaux expéditeurs.

Ces mécanismes antispam permettent d'éliminer une part importante de courriels indésirables mais ne sont pas des remparts infaillibles contre des courriels indésirables ciblés. En effet, un attaquant peut respecter les standards de rédaction d'un courriel, utiliser un serveur d'envoi légitime et valider un test de Turing.

De manière complémentaire, les pièces jointes d'un courriel doivent être analysées par un antivirus ; cette analyse préalable à la délivrance du courriel sur le client de messagerie ne se substitue pas à une analyse antivirus au niveau du poste de travail, préférentiellement avec une technologie distincte. De plus, une analyse des liens contenus dans le corps des courriels doit être menée afin de détecter ceux vers des pages Web malveillantes (ex. : site Web d'hameçonnage imitant un site légitime en vue de récupérer des données personnelles).

R39

Mettre en œuvre des mécanismes de détection de contenu malveillant

Des mécanismes de détection de contenu malveillant spécifiques à la messagerie électronique doivent être mis en œuvre, comme l'analyse antivirus des pièces jointes ou l'analyse des liens Web présents dans le corps des courriels.

Attention

La mise en œuvre de ces mécanismes de détection, pertinente sur du contenu en clair, ne remet pas en cause la prévalence du chiffrement du corps des courriels ou des pièces jointes qui le nécessitent. Toutefois, comme indiqué en introduction de ce chapitre, ce sujet n'est pas abordé ici.

Ces services de détection peuvent être spécifiquement externalisés. Ainsi, tous les courriels d'une entité peuvent être préalablement reçus par un service externalisé, souvent de type SaaS, avant d'être retransmis à l'entité. Les recommandations d'usage sur l'externalisation, en particulier dans le *cloud* s'appliquent ici encore (cf. recommandation R15).

Information

Tous les mécanismes de détection doivent être mis en œuvre dans le respect de la réglementation, et il est recommandé qu'ils fassent l'objet d'une information aux utilisateurs (ex. : mention dans la charte informatique).

5.2.4 Exposition des accès utilisateurs à la messagerie sur Internet

Afin de garder la maîtrise des courriels échangés et stockés, mais également de limiter la surface d'attaque du SI de l'entité, il est recommandé de ne pas exposer sur Internet les accès utilisateurs à la messagerie. Dans ce cas, conformément au guide ANSSI sur le nomadisme numérique [13], les utilisateurs nomades doivent accéder à leurs courriels exclusivement depuis un équipement (ordinateur, tablette, mobile multifonction) maîtrisé par l'entité, à travers un tunnel VPN établi jusqu'au SI de l'entité.

R40

Ne pas exposer les accès utilisateurs à la messagerie sur Internet

Le service de messagerie électronique ne doit pas être exposé sur Internet pour les accès des utilisateurs à leurs boîtes aux lettres. En particulier, aucun portail de type *Webmail* exposé sur Internet ne doit être déployé.

Des contraintes organisationnelles propres à l'entité peuvent aller à l'encontre de la recommandation R40 et nécessitent une solution alternative en acceptant un niveau de sécurité moindre.

Attention

Dès lors que l'entité accepte d'exposer sur Internet les accès utilisateurs à la messagerie, potentiellement depuis des équipements non maîtrisés, le risque résiduel d'interception ou d'exfiltration de l'ensemble des courriels échangés et stockés doit être accepté par une autorité (l'autorité d'homologation dans le cas où le service serait homologué).

R40 -

Sécuriser les accès utilisateurs à la messagerie sur Internet

Dans le cas où une autorité aurait accepté le risque d'exposition du service de messagerie électronique sur Internet, il est indispensable de prévoir une chaîne d'accès avec des ressources dédiées, des restrictions d'accès et une stratégie renforcée de détection, par exemple :

- un serveur d'exposition (ex. : portail *Webmail*) hébergé au sein de la zone de services exposés ;
- la protection du serveur d'exposition par un serveur mandataire inverse (*reverse proxy*), voire un pare-feu applicatif, hébergés en zone de services relais ;
- la mise en œuvre d'une authentification double facteur pour les utilisateurs, éventuellement avec la fourniture d'un certificat électronique ;
- la définition d'une stratégie renforcée de détection (géolocalisation des connexions, nombre d'authentifications échouées, volumes de courriels échangés).

5.3 Sécurisation des canaux de transport

Afin de réduire le risque d'usurpation d'identité (et donc de réception d'une certaine part de courriels malveillants), des mécanismes d'authentification doivent être mis en œuvre sur les canaux de transport entre l'expéditeur et les destinataires. Les protocoles sécurisés standards permettent en outre une protection des données échangées, en confidentialité (pour réduire le risque d'interception en clair) et en intégrité (pour détecter d'éventuelles modifications). En effet, par défaut, les courriels sont comme de simples cartes postales, sans protection des adresses d'expédition ni des adresses de destination ni du contenu.

En premier lieu, sur un réseau local maîtrisé, le canal de transport entre les clients de messagerie et les serveurs de boîtes aux lettres doit être sécurisé au niveau applicatif.

R41

Sécuriser le canal de transport entre clients de messagerie et serveurs de boîtes aux lettres

Quel que soit le protocole utilisé, les flux de messagerie entre les clients de messagerie et les serveurs de boîtes aux lettres doivent être chiffrés et authentifiés. Cette authentification des flux est complémentaire à l'authentification applicative des utilisateurs.
Ainsi, l'utilisation des protocoles sécurisés de messagerie, désormais standards (ex. : SMTPS, POPS, IMAPS ou HTTPS) est recommandée.

Entre les infrastructures de messagerie (internes ou externalisées) de deux domaines distincts (celui de l'expéditeur et celui d'un destinataire), les courriels transitent à travers un ou plusieurs serveurs SMTP, sur des réseaux potentiellement non maîtrisés (ex. : Internet, réseaux « privés » d'opérateur). La sécurité de bout en bout du canal de transport dépend de la configuration de chacun des serveurs SMTP, dont la plupart ne sont pas sous la maîtrise de l'entité.

Ainsi, l'entité doit supporter l'établissement d'un canal de transport sécurisé à l'état de l'art, tout en assurant l'interopérabilité avec des serveurs SMTP d'un plus faible niveau de sécurité, d'où le recours à l'option `STARTTLS`, dit TLS opportuniste. Dans ce cas, les communications avec les serveurs SMTP externes à l'entité sont chiffrées et authentifiées si le serveur SMTP externe le supporte également. Sinon la communication continue en clair. En d'autres termes, l'activation de cette option sur les serveurs SMTP de l'entité est une condition nécessaire mais non suffisante à l'utilisation effective de TLS.

De plus, la configuration de TLS doit être assez tolérante, c'est-à-dire accepter non seulement des versions récentes du protocole et des suites cryptographiques robustes (cf. le guide TLS de l'ANSSI [14]) pour l'établissement d'un canal sécurisé à l'état de l'art, mais aussi des versions plus anciennes du protocole et des suites cryptographiques plus faibles. En effet, les paramètres finalement négociés dépendent des configurations des serveurs SMTP de part et d'autre. En cas de configuration trop stricte, non supportée par le serveur SMTP externe, l'établissement du canal TLS serait impossible et la communication continuerait en clair, ce qui n'est pas souhaitable.

R42

Activer l'option `STARTTLS` sur les serveurs SMTP

Sur les serveurs SMTP, l'option `STARTTLS` doit être activée avec une configuration TLS supportant l'état de l'art et tolérant des paramètres d'un niveau de sécurité moindre. Le cycle de vie des certificats doit être traité avec attention.
De plus, il est recommandé dans ce cas de désactiver sur les serveurs SMTP, et de bloquer sur les briques de filtrage, le service SMTP avec chiffrement implicite (TCP/465).

Pour les entités matures, une option de sécurité plus stricte, `REQUIRETLS`, permet de forcer la totalité de l'échange à travers un canal TLS. En cas d'échec de la négociation entre deux parties, la communication échoue et un message de non-distribution est émis.

R42 +

Activer l'option `REQUIRETLS` sur les serveurs SMTP

Pour forcer les échanges à travers un canal TLS avec une entité destinataire qui le supporte, il est recommandé d'activer l'option `REQUIRETLS`.

Attention

L'activation de l'option `REQUIRETLS`, plus efficace pour la sécurité mais plus contraignante d'un point de vue opérationnel, nécessite des tests et de la supervision, dans la mesure où des courriels pourraient ne pas être transmis en cas d'incompatibilité des paramétrages TLS expéditeur et destinataire.

5.4 Protection contre les courriels illégitimes

Certaines attaques commencent par des campagnes de courriels usurpant l'identité d'expéditeurs légitimes. Il s'agit d'un cas particulier de courriels indésirables, pour lesquels des recommandations générales ont été proposées dans le paragraphe 5.2.3. Pour limiter la nuisance de ces courriels, en amont de leur réception par les utilisateurs, certains protocoles ont pour rôle de vérifier l'authenticité et l'intégrité des courriels. Ils nécessitent une configuration, non seulement par l'entité expéditrice sur les enregistrements DNS de ses noms de domaine, mais aussi par l'entité destinataire sur ses serveurs SMTP de réception. Ces protocoles sont :

- *Sender Policy Framework* (SPF) qui permet de spécifier les adresses IP des serveurs autorisés à émettre les courriels d'un domaine (paragraphe 5.4.1) ;
- *DomainKeys Identified Mail* (DKIM) qui permet l'authentification du domaine de messagerie d'un courriel à l'aide d'une signature cryptographique (paragraphe 5.4.2) ;
- *Domain-based Message Authentication, Reporting and Conformance* (DMARC) qui permet notamment à une entité de définir une politique de traitement de ses courriels envoyés en fonction des résultats de conformité SPF et DKIM (paragraphe 5.4.3).

Ces protocoles ont un intérêt double pour l'entité :

- en tant que destinataire, ils renforcent la vérification de la légitimité des courriels reçus ;
- en tant qu'expéditrice :

- ils fournissent, aux destinataires des courriels qu'elle envoie, des informations techniques pour s'assurer de la légitimité des courriels envoyés,
- ils lui permettent de recevoir des statistiques sur l'utilisation de son ou ses domaines de messagerie.

La figure 5.2 propose une cinématique simplifiée du fonctionnement de ces protocoles pour l'entité en tant que destinataire (les numéros de cette liste sont reportés sous la forme ① à ④) :

1. l'envoi d'un courriel comportant une signature DKIM (dit courriel signé) depuis le domaine `monpartenaire.fr` et sa réception par le serveur SMTP de l'entité ;
2. la vérification des paramètres SPF, DKIM et DMARC du courriel…
3. … nécessitant le recours aux enregistrements DNS publics de l'expéditeur ;
4. enfin, l'envoi d'un rapport DMARC à l'expéditeur selon la politique qu'il a définie.

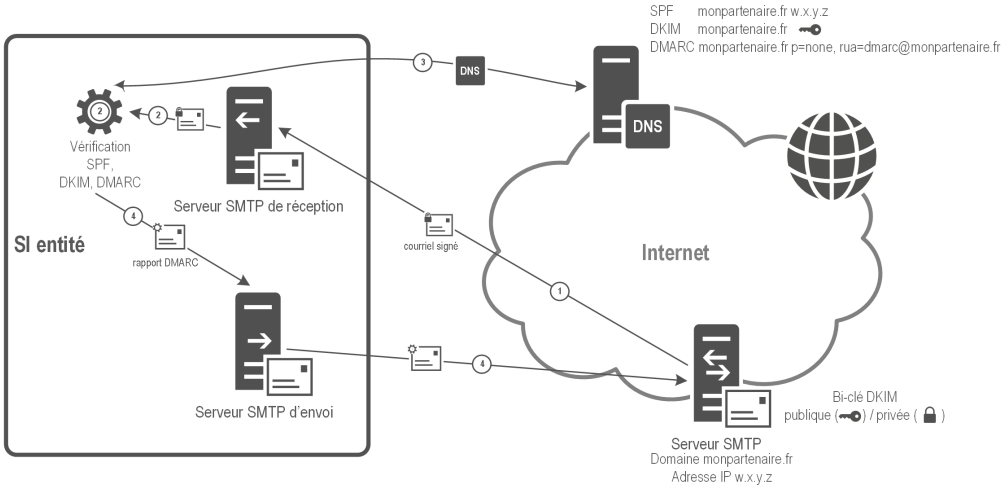


FIGURE 5.2 – Cinématique simplifiée du fonctionnement de SPF, DKIM et DMARC pour une entité destinataire de courriels

Attention

Ces mécanismes ne permettent pas de se protéger contre certaines attaques utilisant la messagerie comme vecteur d'attaque, par exemple :

- le « typosquattage » d'un nom de domaine proche de celui de l'entité ;
- l'usurpation de l'identité de l'émetteur du courriel en amont du serveur SMTP d'envoi ;
- un courriel dont le contenu est piégé.

5.4.1 Sender Policy Framework (SPF)

L'adresse source d'un courriel (champ `From:`) est laissée à la discrétion de l'expéditeur ou de son serveur de messagerie. Ainsi, le protocole SMTP permet par construction de modifier l'adresse source pour envoyer des courriels en usurpant des domaines de messagerie. Afin de réduire le nombre de ces courriels illégitimes, une entité peut déclarer la liste des adresses IP des serveurs SMTP autorisés à envoyer des courriels en utilisant les noms de domaine qu'elle détient, et éventuellement

les adresses IP de ceux qui ne sont pas autorisés. Cette déclaration est stockée dans un enregistrement DNS du domaine de type *Text Resource Record* (TXT RR).

Les serveurs SMTP de réception peuvent alors vérifier que l'adresse IP du serveur SMTP d'envoi d'un courriel est bien listée dans celles autorisées pour le domaine. Cette solution est simple à mettre à œuvre pour un coût limité, dès lors que l'inventaire des serveurs est rigoureux, notamment s'il existe de multiples serveurs SMTP d'envoi, et d'externalisation d'envois de courriels au nom de l'entité.

R43

Supporter SPF sur les serveurs SMTP de réception

Le protocole SPF (ou le service Sender ID dans les infrastructures Microsoft Exchange) doit être supporté sur les serveurs SMTP de réception de l'entité.

R44

Configurer SPF pour les domaines de messagerie électronique de l'entité

Il est recommandé de configurer SPF pour les domaines de messagerie électronique de l'entité, en étant particulièrement attentif, d'une part à l'inventaire des serveurs SMTP d'envoi, qu'ils soient internes ou externes, et d'autre part aux usages spécifiques (ex. : utilisation d'alias).

Le protocole SPF n'est toutefois pas infaillible pour détecter une usurpation. Par exemple :

- si une adresse IP est attribuée à des instances de serveurs SMTP de différents domaines, un utilisateur d'un domaine peut émettre un courriel en usurpant un autre domaine tout en utilisant une adresse IP autorisée ;
- si un attaquant a pris le contrôle d'un serveur SMTP, ou usurpe l'adresse IP d'un serveur SMTP légitime, SPF ne peut pas distinguer la fraude.

Information

Des détails concernant le protocole SPF et sa configuration sont disponibles sur le Web, par exemple sur le site `https://www.open-spf.org`, ou en consultant la RFC 7208.

5.4.2 DomainKeys Identified Mail (DKIM)

L'adresse IP source du serveur SMTP d'envoi n'est pas un gage infaillible d'authenticité de l'expéditeur. Il est également possible de vérifier la légitimité d'un serveur SMTP en recourant à la cryptographie asymétrique avec l'usage d'une bi-clé (clé privée et clé publique) et d'un mécanisme de signature. Pour cela, le protocole DKIM peut être utilisé : le serveur SMTP d'envoi signe cryptographiquement certains champs de l'en-tête et/ou le corps des courriels. La clé publique est stockée dans un champ texte de l'enregistrement DNS du domaine appelé sélecteur DKIM. La clé privée utilisée pour la signature est donc unique pour un nom de domaine et un sélecteur. Le serveur SMTP de réception peut alors vérifier l'authenticité des champs grâce à la clé publique contenue dans l'enregistrement DNS du domaine.

Lorsqu'un courriel est reçu, le comportement attendu du serveur SMTP de réception est de vérifier les signatures présentes (ou leur absence). Il a ensuite pour tâche de vérifier la politique de signature du serveur SMTP d'envoi, avant de le transférer au moteur de filtrage (se référer à la figure 1 de la RFC 5585). L'échec de la vérification de la signature d'un ou plusieurs champs ne signifie pas que le courriel est illégitime. En effet, les signatures peuvent être altérées accidentellement lors de leur transport. Un tel courriel ne devrait donc pas être considéré différemment d'un courriel non signé.

De plus, chaque bi-clé utilisé pour DKIM est associé à un sélecteur dans l'enregistrement DNS. Ce champ permet d'identifier la clé utilisée si le serveur en possède plusieurs, ou si plusieurs serveurs exploitent le même nom de domaine. Dans ce dernier cas, il peut alors s'agir de serveur externes au SI et ayant une délégation de droit d'utilisation du nom de domaine.

R45

Supporter DKIM sur les serveurs SMTP de réception

Le protocole DKIM doit être supporté sur les serveurs SMTP de réception de l'entité.

R46 +

Configurer DKIM pour les domaines de messagerie électronique de l'entité

Il est recommandé de configurer DKIM pour les domaines de messagerie électronique de l'entité. Le cas échéant, la clé privée utilisée pour la signature doit être protégée.

Cependant, plusieurs limites sont identifiées pour le protocole DKIM :

- il est possible pour un serveur illégitime de rejouer un courriel légitime ;
- la modification de champs non signés du courriel ne peut pas être détectée ;
- le choix des paramètres cryptographiques (taille et rotation de clés) doit être traité avec attention, en conformité avec l'annexe B1 du Référentiel général de sécurité [16] afin d'éviter l'utilisation de clés de taille faible pouvant être cassées.

Information

Des détails concernant le protocole DKIM et sa configuration sont disponibles sur le Web, par exemple sur le site `https://dkim.org`, ou en consultant la RFC 5585.

5.4.3 Domain-based Message Authentication, Reporting and Conformance (DMARC)

DMARC est un protocole complémentaire de SPF et DKIM. En effet, la déclaration d'une politique DMARC, par l'entité propriétaire d'un domaine, est l'ajout, dans l'enregistrement DNS idoine, du comportement attendu de la part d'un serveur SMTP à la réception d'un courriel émis depuis ce domaine. Ce propriétaire y annonce quel traitement (vérification DKIM et/ou SPF) doit être appliqué sur les courriels utilisant son nom de domaine, ainsi que la politique à appliquer en cas d'échec lors de la vérification : accepter le courriel (*p=none*, où *p* signifie ici *policy* – politique en anglais), le catégoriser comme indésirable (*p=quarantine*), ou le supprimer (*p=reject*).

La politique DMARC contient également une ou plusieurs adresses de messagerie pour recevoir les statistiques d'application. Ces rapports peuvent être détaillés (ex. : pour chaque courriel ayant échoué la vérification de l'authentification SPF ou DKIM) ou agrégés (statistiques régulières sur l'ensemble des courriels utilisant le domaine).

R47 +

Supporter DMARC sur les serveurs SMTP de réception

Il est recommandé de supporter le protocole DMARC sur les serveurs SMTP de réception de l'entité.

R48 +

Configurer DMARC pour les domaines de messagerie électronique de l'entité

Il est recommandé de configurer DMARC pour les domaines de messagerie électronique de l'entité.
Dans un premier temps, il est recommandé d'analyser les statistiques d'utilisation sur la base d'une politique d'acceptation de tous les courriels (*p=none*), avant d'activer une politique plus stricte.

Information

Des détails concernant le protocole DMARC et sa configuration sont disponibles sur le Web, par exemple sur le site `https://dmarc.org`, ou en consultant la RFC 7489.

5.4.4 DNSSEC

Les protocoles décrits précédemment dans cette section s'appuient sur les enregistrements DNS des domaines à protéger. S'il n'est pas possible de garantir la fiabilité du serveur DNS lui-même, il convient de garantir la fiabilité des données, par exemple avec l'utilisation de DNSSEC.

R49

Supporter DNSSEC pour les résolutions publiques

Afin de fiabiliser le support de SPF, DKIM et DMARC, reposant sur les enregistrements DNS des domaines d'expédition, il est recommandé que les résolutions DNSSEC soient supportées sur les serveurs DNS de résolution publique de l'entité.

R50 +

Configurer DNSSEC pour les domaines de messagerie électronique de l'entité

Afin de fiabiliser l'utilisation de SPF, DKIM et DMARC, pour les domaines de messagerie électronique de l'entité, il est recommandé de configurer DNSSEC pour ces domaines.

5.5 Disponibilité

Le sujet de la disponibilité doit être intégré à l'analyse de risque.

Pour couvrir les cas de panne sur les infrastructures internes de l'entité, au-delà des mesures génériques de sauvegarde, la redondance des serveurs SMTP et des enregistrements MX associés est recommandée.

Pour couvrir les attaques en déni de service distribué, les mesures génériques anti-DDoS de la passerelle Internet sécurisée (recommandation R18) peuvent protéger le service de messagerie électronique des attaques en disponibilité les plus courantes. Des attaques plus évoluées de type « bombardement de courriels » (*email bombing*), peuvent également mettre en défaut le service, en saturant les serveurs SMTP de réception, voire les boîtes aux lettres des utilisateurs. Les mesures techniques en cas d'attaque sont généralement spécifiques et réactives (ex. : blocage d'adresses IP source, de domaines d'expédition).

R51

Prévoir des mesures de protection en disponibilité du service de messagerie électronique

Suivant les besoins de sécurité et les moyens de l'entité, il est recommandé de mettre en œuvre ou d'anticiper des mesures de protection en disponibilité du service de messagerie électronique, pour couvrir les cas de panne et les attaques.

Liste des recommandations

Bibliographie

[1] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://www.ssi.gouv.fr/nt-commutateurs.

[2] *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information*.
Guide Version 1.0, ANSSI, décembre 2010.
https://www.ssi.gouv.fr/infogerance.

[3] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/hygiene-informatique.

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

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

[6] *Comprendre et anticiper les attaques DDoS*.
Guide Version 1.0, ANSSI, mars 2015.
https://www.ssi.gouv.fr/guide-ddos.

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

[8] *Recommandations de securité concernant l'analyse des flux HTTPS*.
Note technique DAT-NT-019/ANSSI/SDE/NP v1.2, ANSSI, février 2016.
https://www.ssi.gouv.fr/analyse-https.

[9] *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.
https://www.ssi.gouv.fr/nettoyage-politique-fw.

[10] *La méthode EBIOS Risk Manager - Le Guide*.
Guide Version 1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide.

[11] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet*.
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.
https://www.ssi.gouv.fr/guide-pare-feux-internet.

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

[13] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v1.0, ANSSI, octobre 2018.
https://ssi.gouv.fr/nomadisme-numerique.

[14] *Recommandations de sécurité relatives à TLS*.
Guide SDE-NT-035 v1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[15] *Instruction générale interministérielle n°1300*.
Référentiel Version 1.0, ANSSI, novembre 2011.
https://www.ssi.gouv.fr/igi1300.

[16] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[17] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://www.ssi.gouv.fr/ii901.

[18] *Prestataires de services d'informatique en nuage (SecNumCloud). Référentiel d'exigences*.
Référentiel 3.1, ANSSI, juin 2018.
https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf.

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

ANSSI-PA-066
Version 3.0 - 19/06/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN