RECOMMANDATIONS POUR CHOISIR DES PARE-FEUX MAÎTRISÉS DANS LES ZONES EXPOSÉES À INTERNET

GUIDE ANSSI

ANSSI-PA-044
22/01/2018

PUBLIC VISÉ :

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

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

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

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	22/01/2018	Version initiale

Table des matières

1
Introduction

Au regard des menaces pesant sur les systèmes d'information (SI) connectés à Internet, les organisations doivent mettre en place les moyens permettant de protéger au mieux les informations dont elles ont la responsabilité. Cela passe par une maîtrise de tous les flux de données entrants et sortants de ces systèmes d'information et donc par la mise en œuvre raisonnée de passerelles sécurisées *incontournables* par lesquelles transitent les flux de données vers ou en provenance d'Internet.

La figure 1.1 donne une représentation simplifiée d'une passerelle Internet sécurisée destinée à traiter les flux entrants aussi bien que les flux sortants.

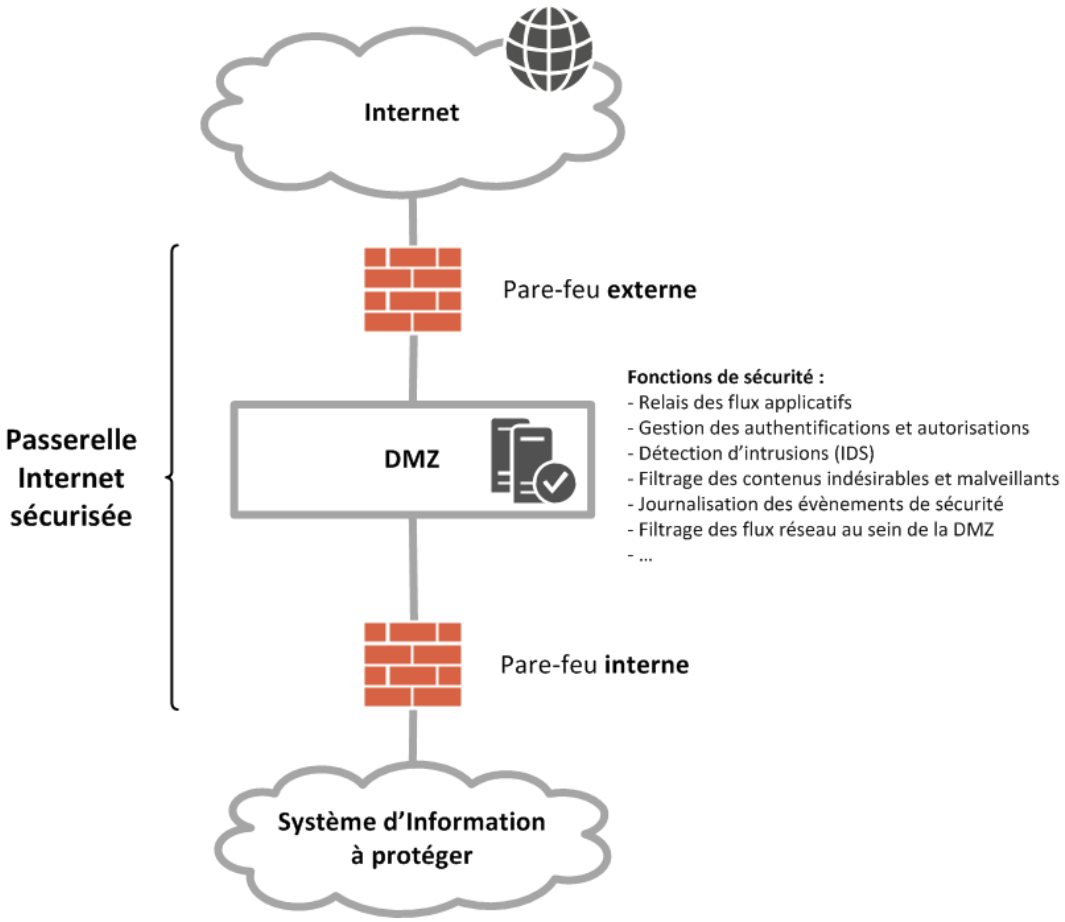

FIGURE 1.1 – Représentation simplifiée d'une passerelle Internet sécurisée

Dans la suite de ce document, le pare-feu connecté directement à Internet est désigné « Pare-feu externe » et le pare-feu connecté au SI à protéger est désigné « Pare-feu interne ». La zone située entre ces deux pare-feux est appelée DMZ [1].

Les passerelles Internet sécurisées portent différentes fonctions de sécurité parmi lesquelles on peut citer :

- le relais des flux applicatifs ;
- la gestion des authentifications et des autorisations ;
- la détection d'intrusions (IDS [2]) ;
- le filtrage des contenus indésirables et malveillants ;
- la journalisation des évènements de sécurité ;
- le filtrage des flux réseau au sein de la DMZ [3].

Il est recommandé que ces fonctions de sécurité soient préférentiellement mises en œuvre au sein de la DMZ en privilégiant, autant que possible, la mise en place de solutions dédiées par fonction de sécurité.

Ce guide donne des recommandations d'architecture spécifiquement pour la fonction de filtrage des flux réseau mise en œuvre par des pare-feux et n'a pas pour vocation de répondre aux problématiques d'urbanisation concernant les autres fonctions de sécurité.

Information

Même si la fonction de terminaison des réseaux privés virtuels (VPN [4]) fait classiquement partie des fonctions de sécurité rencontrées dans une passerelle Internet et qu'elle peut être portée par des pare-feux, elle n'est toutefois pas prise en compte dans le contexte de ce guide. Si présente dans une passerelle Internet sécurisée, cette fonction de sécurité est en effet plutôt mise en œuvre pour l'interconnexion d'entités ayant le même niveau de sensibilité [5], alors que ce guide ne traite que du cas de l'interconnexion du SI avec Internet.

Les architectures ne mettant en œuvre qu'un seul pare-feu sont exclues du périmètre de ce document car elles ne présentent pas un niveau de sécurité satisfaisant. Plus d'informations concernant les topologies de passerelles sécurisées sont disponibles dans le document publié par l'ANSSI [9].

R1

Mettre en œuvre au moins deux pare-feux en cascade

Une passerelle Internet sécurisée doit mettre en œuvre au moins deux pare-feux en cascade car une architecture basée sur un seul pare-feu, créé un point de défaillance dont la compromission expose l'ensemble des ressources du SI à protéger.

1. *DeMilitarized Zone*, zone démilitarisée en français. Ce guide n'étant pas un guide d'urbanisation, la représentation de la DMZ sur les différentes figures d'illustration est volontairement simplifiée, sans cloisonnement des fonctions.
2. *Intrusion Detection System*.
3. Le filtrage des flux réseau sera réalisé au minimum par les pare-feux interne et externe mais pourra également être mis en œuvre au niveau de pare-feux additionnels placés au sein de la DMZ.
4. *Virtual Private Network*.
5. À titre d'exemple, il peut s'agir de l'interconnexion de systèmes d'information ayant le même niveau de sensibilité (interconnexion dite « site-à-site ») ou encore de la connexion de postes nomades à leur SI d'appartenance.

Ce guide apporte les réponses aux questions suivantes :

- Est-il préférable d'utiliser des pare-feux de technologies différentes ?
- La virtualisation des pare-feux peut-elle être envisagée ?
- Doit-on mettre en œuvre des pare-feux qualifiés ou certifiés ? Dans l'affirmative, quel doit être le niveau du visa de sécurité (qualification ANSSI [6], certification critères communs [7], certification CSPN [8]) ?

Ces questions s'entendent pour des SI de niveau :

- Diffusion Restreinte [9] (DR) ;
- sensible [10] ;
- non protégé (NP).

Information

Les SI classifiés de défense sont exclus du périmètre de ce guide.

6. Se reporter à https ://www.ssi.gouv.fr/qualification/.
7. Se reporter à https ://www.ssi.gouv.fr/certification/.
8. Certification de Sécurité de Premier Niveau, se reporter à https ://www.ssi.gouv.fr/cspn/.
9. *Les systèmes d'information* Diffusion Restreinte *sont les systèmes d'information sensibles qui traitent d'informations portant la mention* Diffusion Restreinte *ou ses équivalentes européennes ou internationales*, II 901 [8], Titre 1, Article 1.
10. *Les systèmes d'information sensibles sont ceux qui traitent d'informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre*, II 901 [8], Titre 1, Article 1.

2
Diversification technologique des pare-feux

Une approche « mono-éditeur » consiste à déployer la même solution technologique (matérielle et logicielle) pour le pare-feu externe et le pare-feu interne tandis qu'une approche « multi-éditeurs » privilégie la diversification technologique.

L'approche « mono-éditeur » permet de simplifier les tâches d'administration et d'exploitation. À titre d'exemple, elle autorise à mettre en œuvre une solution de gestion intégrée d'un ensemble de pare-feux, et facilite ainsi les tâches d'administration (unicité de déclaration des objets, unicité de configuration des règles de flux et propagation automatisée de celles-ci vers les différents pare-feux, etc.). Les coûts d'exploitation et de formation des administrateurs s'en trouvent réduits.

Néanmoins, l'approche « mono-éditeur » est moins satisfaisante du point de vue de la sécurité des systèmes d'information que l'approche « multi-éditeurs ». L'exploitation réussie par un attaquant d'une vulnérabilité affectant un pare-feu peut être répétée trivialement sur d'autres pare-feux de même technologie.

En outre, au-delà de la présence d'une vulnérabilité intrinsèque au pare-feu, la probabilité qu'une erreur de configuration soit reproduite par un exploitant est plus forte si les pare-feux sont identiques, *a fortiori* en cas de gestion centralisée d'un ensemble de pare-feu.

Par conséquent, la mise en œuvre de pare-feux de technologies différentes doit être préférée. Cette mesure est conforme au principe de défense en profondeur [3], concept clé des architectures et des systèmes sécurisés. Cette diversification technologique est d'autant plus efficace si les différents composants des deux pare-feux (matériel, système d'exploitation, moteur de filtrage et interface homme-machine) sont réellement différents.

R2

Privilégier la diversification technologique des pare-feux

Dans une passerelle Internet sécurisée, il est recommandé de déployer des pare-feux présentant des différences technologiques à tous les niveaux : matériel, système d'exploitation, moteur de filtrage et IHM.

Par ailleurs, la diversification technologique apporte une complémentarité des fonctionnalités proposées par les éditeurs. Cette complémentarité peut être mise à profit par le client pour répondre à ses différents besoins.

Enfin, la diversification technologique permet de réduire la dépendance à un seul fournisseur ; dépendance qui n'est jamais souhaitée pour des raisons variées (changement de statégie unilatérale qui serait subie par le client, abus de position dominante du fournisseur…).

Cependant, la diversification technologique n'est pertinente que si la maîtrise des différents pare-feux par les exploitants est démontrée. Cette maîtrise passe par la formation continue des personnels concernés et l'application par ces derniers des bonnes pratiques d'administration. L'ANSSI a formulé dans les documents [5] et [7] certaines pratiques recommandées pour la définition d'une politique de filtrage réseau.

Dans le cas où l'exploitation des pare-feux est confiée à un prestataire externe, il convient d'encadrer cette démarche en suivant les recommandations [2] visant à réduire les risques associés à cette pratique.

R3

Maîtriser les technologies des pare-feux déployés

Il appartient à chaque entité de veiller à la diversification technologique des pare-feux, tout en garantissant la maîtrise des différentes technologies par les équipes d'exploitation.

Information

Si l'entité opère de multiples technologies de pare-feux résultant de son historique (acquisitions multiples par exemple), il est préférable de rationaliser ces technologies pour n'en conserver qu'un nombre limité bien maîtrisé par les exploitants.

3
Pare-feux physiques et pare-feux virtualisés

Le filtrage réseau étant une fonction importante pour la sécurité d'un SI, particulièrement dans le cas des passerelles Internet sécurisées, il est recommandé de ne pas cumuler sur la même instance de pare-feu les fonctions de filtrage réseau avec d'autres fonctions de sécurité. À titre d'exemple, il est préférable de ne pas configurer un pare-feu interne ou un pare-feu externe comme point de terminaison VPN IPsec. De la même manière, il est déconseillé de faire porter par un pare-feu externe ou par un pare-feu interne des fonctionalités de détection d'intrusions. Ces fonctions de sécurité sont préférentiellement à mettre en œuvre au sein de la DMZ. Cette séparation stricte des fonctions permet de réduire la surface d'attaque des pare-feux, de diminuer le risque d'erreur de configuration et, de façon plus générale, est de nature à améliorer la disponibilité de l'ensemble des fonctions de sécurité de la passerelle Internet sécurisée.

R4

Dédier les pare-feux externe et interne à la fonction de filtrage réseau

La fonction de filtrage réseau d'une passerelle Internet sécurisée doit être portée par des pare-feux dédiés à cet usage (qu'ils soient physiques ou éventuellement virtuels). Cette fonction de filtrage ne doit pas coexister avec d'autres fonctions, notamment de sécurité, lesquelles doivent préférentiellement être mises en œuvre au sein de la DMZ.

Définition d'un pare-feu physique

Le terme « pare-feu physique » peut désigner différents types d'équipements de filtrage réseau. Il peut s'agir :

- d'une « *appliance* physique » : un pare-feu physique prêt-à-l'emploi fourni par un éditeur [11] ;
- d'un socle matériel fortement durci portant une fonction de filtrage réseau [12].

11. Exemples : Stormshield gamme SNxxxx, Cisco ASA, Check Point Security Appliance, Forcepoint NGFW appliance…
12. Exemples : Netfilter/iptable, Packet Filter (pf), ipfirewall (ipfw),IPFilter (ipf)…

Définition d'un pare-feu virtualisé

Le terme « pare-feu virtualisé » (ou « pare-feu virtuel ») peut désigner différents types d'équipements de filtrage réseau. Il peut s'agir :

- d'une instance de filtrage réseau hébergée sur une *appliance* physique de pare-feu mettant en œuvre des fonctions de virtualisation (notions de « contexte » ou de « domaine ») [13] ;
- d'une « *appliance* virtuelle » : un pare-feu virtualisé prêt-à-l'emploi fourni par un éditeur [14] et hébergé sur un hyperviseur de type 1 générique ou « *bare metal* » [15] dont la configuration aura été durcie.

Information

D'autres technologies de virtualisation visent à virtualiser les services réseau (NFV [16]) et à rendre le réseau programmable (SDN [17]). Ces technologies mettent en œuvre un logiciel interne [18] à un hyperviseur et permettent un filtrage, de niveau 2 ou supérieur, entre les machines virtuelles qu'il héberge. Ce type de virtualisation est hors du périmètre de ce guide.

La virtualisation des systèmes augmente le nombre des risques pesant sur ceux-ci :

- la fuite d'information par manque de cloisonnement ou du fait d'une vulnérabilité inhérente au mécanisme de cloisonnement mis en œuvre par l'hyperviseur ;
- la compromission du pare-feu virtualisé ou de l'hyperviseur sous-jacent ;
- l'atteinte plus aisée à la disponibilité en cas de compromission, mais aussi du fait d'une erreur d'administration inhérente à la complexité accrue des tâches d'administration.

L'ANSSI a publié un guide relatif à la virtualisation détaillant ces risques [4].

La confiance pouvant être accordée aux mécanismes de cloisonnement est très difficile à démontrer car, en pratique, l'isolation entre des systèmes virtualisés n'est jamais complète, particulièrement du fait des ressources partagées de bas niveau. Par conséquent, le principe de précaution doit s'appliquer et la virtualisation ne doit être envisagée que dans le cas d'une mutualisation de ressources entre des données, flux ou traitements qui relèvent d'un même niveau de criticité. Ainsi, les technologies de pare-feux virtualisés utilisées dans le cadre des passerelles sécurisées avec Internet sont déconseillées.

R5

Préférer la mise en œuvre de pare-feux physiques aux pare-feux virtualisés

De façon générale, la virtualisation des pare-feux des passerelles Internet sécurisées est déconseillée, à plus forte raison si ces passerelles protègent des systèmes d'information Diffusion Restreinte ou sensibles.

13. Exemples : Fortinet Virtual Domains, Forcepoint NGFW Virtual Contexts, Check Point Multi-Domain Security Management…
14. Exemples : Stormshield gamme Vxxx, Palo Alto Networks VM-Series, Cisco ASAv, Check Point vSEC Virtual Edition…
15. Exemples : Xen Project, VMware ESXi, Microsoft Hyper-V…
16. *Network Functions Virtualization*.
17. *Software Defined Network*.
18. Exemples : VMware NSX Distributed Firewall, Openstack Neutron Firewall-as-a-Service (FWaaS), Juniper vSRX…

Information

L'annexe 1 en page 20 de ce guide présente un argumentaire détaillant les raisons techniques pour lesquelles la virtualisation des pare-feux est déconseillée.

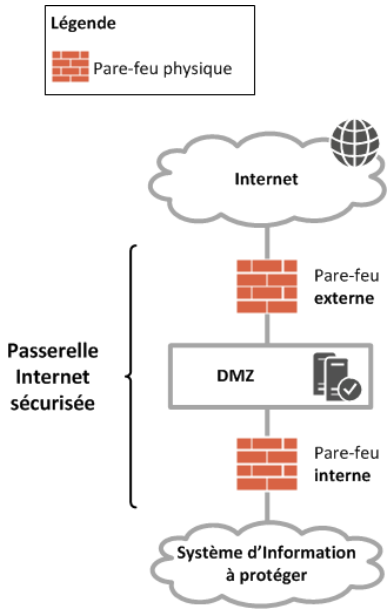

FIGURE 3.1 – Architecture de passerelle Internet sécurisée recommandée : les pare-feux interne et externe sont des pare-feux physiques

Dans une passerelle Internet sécurisée, il est néanmoins possible d'envisager de virtualiser plusieurs instances de filtrage réseau. En particulier, dans le cas d'infrastructures complexes, l'utilisation d'instances de filtrage distinctes virtualisées peut permettre de répartir des règles de flux par besoins fonctionels pour en faciliter l'exploitation (lecture des règles plus facile, gestion des règles par des équipes exploitantes distinctes…). Mais dans ce cas, une attention particulière doit être apportée au durcissement du socle matériel et logiciel. A cet égard, les *appliances* physiques de pare-feux telles que définies au début de ce chapitre sont sans doute plus adaptées, notamment si l'entité ne dispose pas de l'expertise nécessaire pour appliquer des actions de durcissement.

En outre, dans l'hypothèse où la virtualisation est mise en œuvre pour les pare-feux interne et/ou externe, les différentes instances virtuelles constituant le pare-feu interne, d'une part, et le pare-feu externe, d'autre part, ne doivent pas être mutualisées mais portées par des socles physiquement séparés.

R5 -

Séparer physiquement le pare-feu externe et le pare-feu interne si des solutions de virtualisation sont utilisées pour les pare-feux externe et/ou interne

En cas de besoin de virtualisation des instances de filtrage du pare-feu externe ou du pare-feu interne, celles-ci doivent être portées par des socles distincts, physiquement séparés. En outre, conformément à la recommandation R4 , les fonctionalités de sécurité de la DMZ ne doivent être mises en œuvre ni sur le pare-feu externe ni sur le pare-feu interne, que ceux-ci soient physiques ou virtualisés.

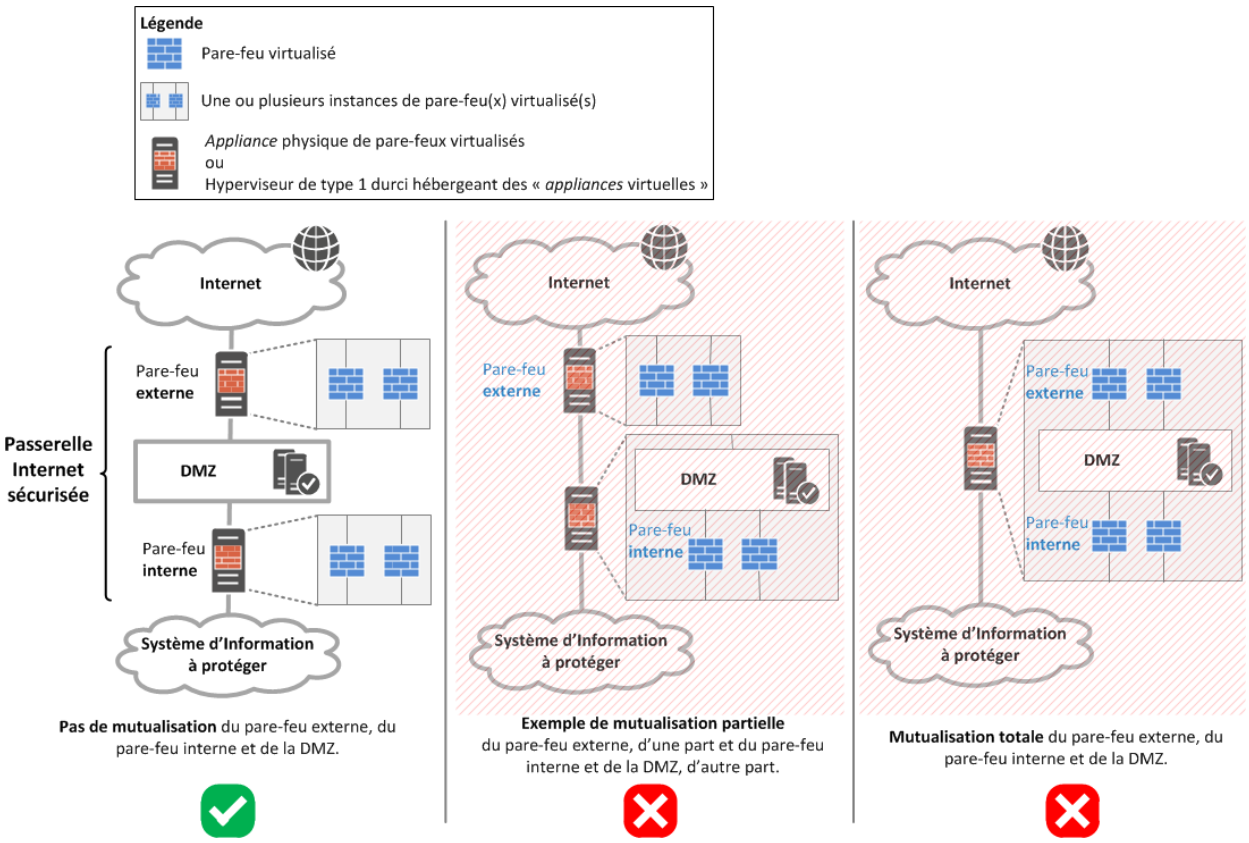

FIGURE 3.2 – Virtualisation des pare-feux interne et externe : architectures possibles et architectures proscrites

4
Positionnement des pare-feux qualifiés et certifiés

4.1 Terminologie

4.1.1 Pare-feux qualifiés

Définition d'un pare-feu qualifié

Un pare-feu qualifié est un produit de filtrage des flux réseau, certifié (cf. 4.1.2) au sens des critères communs [19] ou de la certification de sécurité de premier niveau (CSPN [20]), pour lequel l'éditeur a suivi par ailleurs, avec succès, le processus de qualification des produits établi par l'ANSSI [10]. En ce sens, la qualification d'un pare-feu va au-delà de sa certification car elle traduit la recommandation par l'État d'un produit de filtrage réseau.

Un certificat de qualification délivré par l'ANSSI atteste de la qualité du pare-feu sur le plan de sa robustesse aux attaques informatiques. Le contenu de la cible de sécurité est validé par l'ANSSI et reflète ainsi bien ce qui est attendu du produit d'un point de vue de la sécurité. En outre, la qualification atteste de la confiance qu'a l'État envers l'éditeur de la solution par l'analyse d'informations organisationnelles concernant celui-ci (informations sur la personne morale, la chaîne d'approvisionnement, les procédures opérationnelles, la stratégie produit…).

R6

Mettre en œuvre des pare-feux qualifiés

De manière générale, il est recommandé de mettre en œuvre des pare-feux qualifiés, quel que soit le niveau de sensibilité du SI protégé [21].

La qualification de sécurité est graduée en trois niveaux :

- **élémentaire**, normalement délivrée à l'issue d'une certification CSPN ;
- **standard**, normalement délivrée à l'issue d'une certification critères communs EAL 3+ [22] ;
- **renforcée**, normalement délivrée à l'issue d'une certification critères communs EAL 4+ [23].

La liste actualisée des pare-feux qualifiés par l'ANSSI est disponible sur le site web de l'ANSSI [24].

19. Se reporter à https ://www.ssi.gouv.fr/certification/.
20. Se reporter à https ://www.ssi.gouv.fr/cspn/.
21. Au moment de la rédaction de ce document, un seul pare-feu est qualifié au niveau standard. Il s'agit du produit *Stormshield Network Security*. Un guide de recommandations pour la configuration de ce pare-feu est disponible sur le site de l'ANSSI [1].
22. Niveau d'assurance EAL 3 augmenté des familles d'assurance ALC_FLR 3 et AVA_VAN 3.
23. Niveau d'assurance EAL 4 augmenté des familles d'assurance ALC_FLR 3, AVA_VAN 5 et ALC_DVS 2.
24. Liste des produits qualifiés : https ://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/.

4.1.2 Pare-feux certifiés

Définition d'un pare-feu certifié

Un pare-feu certifié est un produit de filtrage des flux réseau dont la robustesse a été évaluée par un tiers. Les évaluations de sécurité faites au titre de la certification de sécurité sont réalisées par des laboratoires indépendants appelés centres d'évaluation de la sécurité des technologies de l'information (CESTI) [25]. La certification d'un pare-feu est établie sur la base d'un contexte d'usage et d'objectifs de sécurité définis par un commanditaire qui n'est pas nécessairement l'ANSSI.

Le CESTI vérifie la résistance du produit à un niveau d'attaques donné. À chaque certification de sécurité est associé un niveau d'assurance qui traduit le niveau de profondeur de l'analyse effectuée par le CESTI. Le niveau de sécurité est évalué sur la base de référentiels normatifs ou standardisés (critères communs [26] ou CSPN [27]) lesquels impliquent la définition d'une cible de sécurité décrivant les fonctions de sécurité attendues pour la fonction de filtrage réseau.

Attention

Contrairement à la procédure de qualification, l'ANSSI n'intervient pas [28] dans la définition de la cible de sécurité d'un produit certifié. Celle-ci est définie uniquement par l'éditeur du produit de sécurité. L'éditeur peut choisir de laisser certaines fonctions hors du périmètre d'évaluation ou de faire porter une partie plus importante de la sécurité sur l'environnement opérationnel du pare-feu. Il est par conséquent recommandé d'être toujours attentif au contenu de la cible de sécurité d'un pare-feu certifié avant d'envisager une acquisition. Il est également conseillé d'être vigilant aux versions de logiciel auxquelles s'appliquent les certificats ainsi qu'aux éventuelles restrictions ou recommandations d'emploi accompagnant les rapports de certification.

La recommandation R2 évoque la diversification technologique. Néanmoins, si le marché des pare-feux ne propose qu'un pare-feu qualifié, il est envisageable de mettre en œuvre des pare-feux certifiés. Dans ce cas de figure particulier, il est recommandé de s'assurer que la cible de sécurité du pare-feu certifié est en adéquation avec les besoins de sécurité recherchés [29]. Typiquement, en tant que deuxième pare-feu mis en œuvre dans une passerelle Internet sécurisée, il est possible de choisir un pare-feu :

- soit certifié au niveau d'assurance EAL 3 augmenté des familles d'assurance ALC_FLR 3 et AVA_VAN 3 (ou supérieur), dont le certificat est reconnu par la France ;
- soit certifié CSPN.

25. En france, ces laboratoires indépendants sont accrédités par le comité français d'accréditation (COFRAC) et sont agréés par l'ANSSI, laquelle est également en charge de la délivrance des certificats. Dans le cas d'une CSPN, l'ANSSI est la seule entité nationale habilitée à émettre les certificats de sécurité.
26. Se reporter à https ://www.ssi.gouv.fr/certification/.
27. Se reporter à https ://www.ssi.gouv.fr/cspn/.
28. Plus exactement, l'ANSSI ne se prononce que si la cible définie par l'éditeur est mensongère.
29. Filtrage des flux réseau, traçabilité de l'initialisation des flux, protection contre la saturation des journaux, etc.

R7

Mettre en œuvre des pare-feux certifiés quand un seul pare-feu qualifié est disponible sur le marché

Dans le cas où le marché ne propose qu'un seul pare-feu qualifié, il est envisageable de mettre en œuvre des pare-feux certifiés selon les critères communs ou la CSPN. Il est impératif d'analyser leurs cibles de sécurité et leurs rapports de certification. Les guides d'utilisation associés à ces certifications doivent être respectés de manière à en faire un usage dans les conditions sûres identifiées à l'issue de la démarche de certification.

La liste actualisée des pare-feux pour lesquels la sécurité a été évaluée par des CESTI agréés par l'ANSSI (certifications critères communs ou CSPN) est disponible sur le site web de l'ANSSI [30].

Information

L'ANSSI délivre par ailleurs des agréments pour des produits de sécurité et notamment pour des pare-feux ayant vocation à protéger des systèmes d'informations Diffusion Restreinte. Ces agréments portent généralement sur la fonction de sécurité VPN (pare-feu utilisé en tant que chiffreur) et non sur la fonction de filtrage réseau.

4.2 Cas des systèmes d'information Diffusion Restreinte (DR)

L'annexe 2 de l'II 901 [8] définit le terme *réseau de classe 0* comme étant un réseau public ou tout réseau connecté à un réseau public qui n'est pas sécurisé au moyen de dispositifs de filtrage et de rupture de flux qualifiés. En particulier, il est stipulé que pour un système d'information Diffusion Restreinte, *au moins un dispositif de filtrage qualifié au niveau standard est mis en coupure de tous les flux depuis et vers le réseau de classe 0*. Cette exigence indique qu'au moins un pare-feu qualifié au niveau standard doit nécessairement être intégré à la passerelle Internet sécurisée.

R8

SI DR : Mettre en œuvre un pare-feu qualifié au niveau standard

Si la passerelle Internet sécurisée protège un SI Diffusion Restreinte, au moins un des deux pare-feux de cette passerelle (pare-feu externe ou pare-feu interne) est *obligatoirement* qualifié au niveau standard (ou supérieur).

Compte-tenu de la recommandation R2 relative à la diversification technologique des pare-feux, les pare-feux externe et interne doivent être technologiquement différents. Le deuxième pare-feu est préférentiellement, comme le premier pare-feu, un pare-feu qualifié. En l'absence d'un deuxième pare-feu qualifié disponible sur le marché, il est recommandé d'opter pour des pare-feux certifiés présentant un niveau d'assurance satisfaisant (voir recommandation R7). Il appartient à l'entité de faire le choix des pare-feux en fonction de ses besoins, des fonctionalités recherchées et des

30. Liste des produits certifiés critères communs (uniquement ceux pour lesquels l'ANSSI a délivré un certificat) : https ://www.ssi.gouv.fr/certification/ ; Liste exhaustive des produits certifiés critères communs et niveaux d'assurance associés : https ://www.commoncriteriaportal.org/products/ ; Liste des produits certifiés CSPN : https ://www.ssi.gouv.fr/cspn/.

compétences de ses exploitants mais en gardant à l'esprit qu'à niveau fonctionnel équivalent, c'est l'ordre de préférence défini ci-dessous qui doit guider la décision finale.

R9

SI DR : Privilégier de mettre en œuvre un second pare-feu qualifié de technologie différente du premier

Conformément à la recommandation R2, il est fortement recommandé que le deuxième pare-feu soit technologiquement différent du premier pare-feu. En outre, par ordre décroissant de préférence d'un point de vue sécurité des SI et en fonction de l'offre commerciale disponible, ce deuxième pare-feu de la passerelle est :

1. soit un pare-feu qualifié au niveau standard ;
2. soit un pare-feu qualifié au niveau élémentaire ;
3. soit un pare-feu non qualifié mais certifié (critères communs ou CSPN, voir section 4.1.2).

La recommandation R8 vise à insérer au minimum un pare-feu qualifié au niveau standard dans une passerelle Internet sécurisée qui protège un SI de niveau DR. Si ce pare-feu est le seul pare-feu qualifié mis en œuvre au sein de la passerelle Internet sécurisée il est recommandé de le positionner préférentiellement au contact du réseau de moindre confiance, c'est-à-dire du *réseau de classe 0* tel qu'il est défini en annexe 2 de l'II 901 [8].

R10

SI DR : Positionner préférentiellement le pare-feu qualifié au niveau standard au contact du réseau de moindre confiance

Si un seul pare-feu qualifié au niveau standard est mis en œuvre au sein de la passerelle Internet sécurisée, alors ce pare-feux doit *préférentiellement* être le pare-feu externe, c'est-à-dire le pare-feu connecté au *réseau de classe 0* tel que celui-ci est défini en annexe 2 de l'II 901 [8].

La figure 4.1 illustre une architecture recommandée de pare-feux dans le cas d'une passerelle Internet sécurisée protégeant un SI de niveau DR en précisant les positionnements des différents types de pare-feux ainsi que leurs niveaux de qualification ou certification.

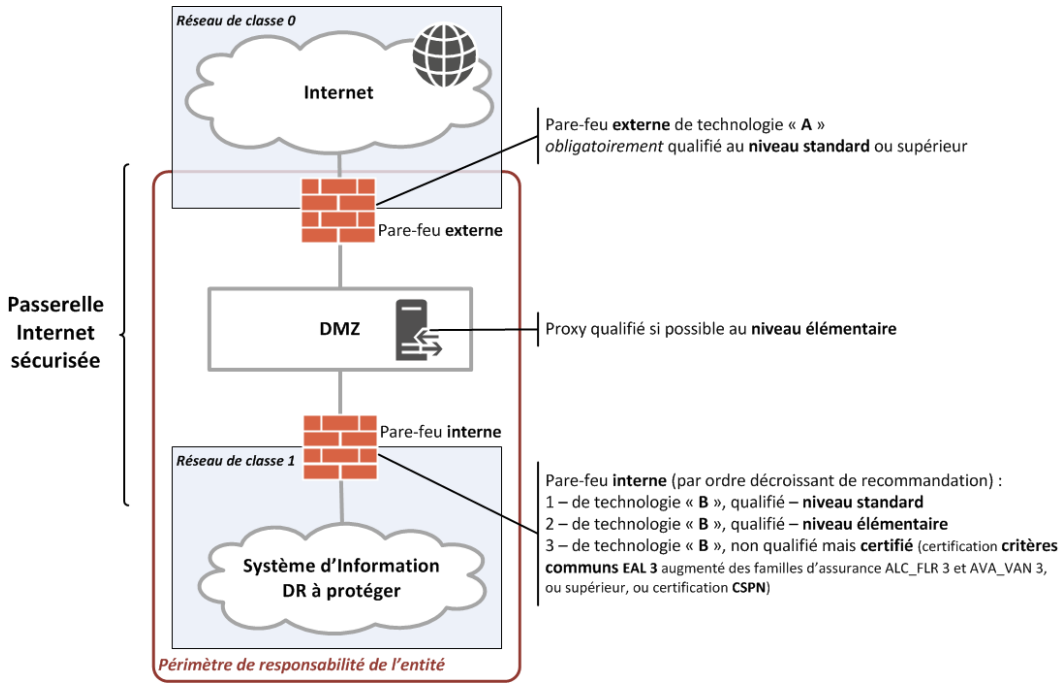

FIGURE 4.1 – Passerelle Internet sécurisée pour un SI Diffusion Restreinte

Cette dernière recommandation (R10) donne un orientation préférentielle. L'unique pare-feu qualifié au niveau standard (ou supérieur) peut éventuellement ne pas être le pare-feu externe mais le pare-feu interne. Ce choix est déterminé à l'issue d'une analyse menée par l'entité souhaitant mettre en œuvre une passerelle sécurisée avec Internet et prend en compte le contexte du SI considéré.

Cette analyse intègre notamment les éléments de réflexion suivants :

- la nature des données stockées ou transitant au sein de la passerelle : celles-ci sont-elles exclusivement des données non protégées ? S'il s'agit de données DR, celles-ci sont-elles chiffrées par des moyens adaptés ?
- la criticité métier et l'exposition des services et informations hébergés dans la DMZ : quelles sont les conséquences pour l'entité d'une atteinte en confidentialité, intégrité et/ou disponibilité de ces services et informations par un attaquant ? Ces services ont-il plutôt vocation à être tournés largement vers Internet ou bien plutôt à être utilisés par des utilisateurs du SI à protéger ?

R11

SI DR : Justifier le fait que le pare-feu qualifié au niveau standard ne soit pas le pare-feu externe

Si la passerelle Internet sécurisée protège un SI DR, alors le pare-feu qualifié au niveau standard doit *préférentiellement* être le pare-feu externe. Si le choix de l'entité est différent, une justification et une acceptation du risque résiduel doivent être formalisées. Un SI DR étant soumis à homologation [6], cette formalisation pourra par exemple être ajoutée à la liste des risques résiduels du dossier d'homologation.

4.3 Cas des systèmes d'information sensibles

L'application de l'II 901 [8] est obligatoire pour les SI sensibles des administrations de l'État et des entités publiques ou privées soumises à la réglementation relative à la protection du potentiel scientifique et technique de la nation (PPST). Elle a valeur de recommandation pour toute autre entité publique ou privée qui met en œuvre des systèmes d'informations sensibles [31].

Ce texte réglementaire prévoit notamment la mise en œuvre de produits ayant fait l'objet d'un visa de sécurité [32] tel que défini dans le chapitre d'introduction de ce guide.

Par conséquent, si la passerelle Internet sécurisée protège un SI sensible, il est obligatoire de mettre en œuvre des pare-feux qualifiés par l'ANSSI dans les administrations de l'État et dans les entités publiques ou privées soumises à la réglementation relative à la protection du potentiel scientifique et technique de la nation (PPST). Sur les SI sensibles des autres entités publiques ou privées, il est également *recommandé* de mettre en œuvre des pare-feux qualifiés par l'ANSSI.

R12

SI sensibles : Appliquer les mêmes recommandations que celles mises en œuvre dans le cas des SI DR

De manière générale, et par souci de simplification, il est recommandé d'appliquer pour les systèmes d'information sensibles, les mêmes principes d'architecture que pour la protection des systèmes d'information Diffusion Restreinte décrits à la section 4.2. Il est en particulier recommandé de mettre en œuvre des pare-feux qualifiés par l'ANSSI.

4.4 Cas des systèmes d'information non protégés (NP)

Pour les architectures non soumises à réglementation, la recommandation de diversification technologique s'applique. De même, les solutions de filtrage qualifiées sont recommandées.

4.5 Passerelles sécurisées mettant en œuvre plus de deux pare-feux

Dans ce guide, il a été pris pour hypothèse que la passerelle sécurisée avec Internet mettait en œuvre deux pare-feux en cascade : un pare-feu externe et un pare-feu interne. En pratique, il est fréquent de concevoir des architectures de passerelles sécurisées avec Internet mettant en œuvre

31. II 901 [8], Titre 1, Article 2.
32. II 901 [8], Annexe 1, Objectif 7.

plus de deux pare-feux successifs [9].

R13

Généraliser les recommandations de ce guide pour les passerelles constituées de plus de deux pare-feux en cascade

Dans le cas de passerelles Internet sécurisées comportant plus de deux pare-feux en cascade, il est recommandé de généraliser les recommandations formulées précédemment dans ce guide, c'est-à-dire :

- de diversifier les technologies de filtrage (R2) ;
- de bien faire porter uniquement les fonctions de filtrage par ces pare-feux (R4) ;
- de mettre en œuvre des pare-feux qualifiés (R6) ou, à défaut, certifiés (R7).

La figure 4.2 montre des exemples acceptables d'architectures de passerelles Internet sécurisées mettant en œuvre trois pare-feux en cascade.

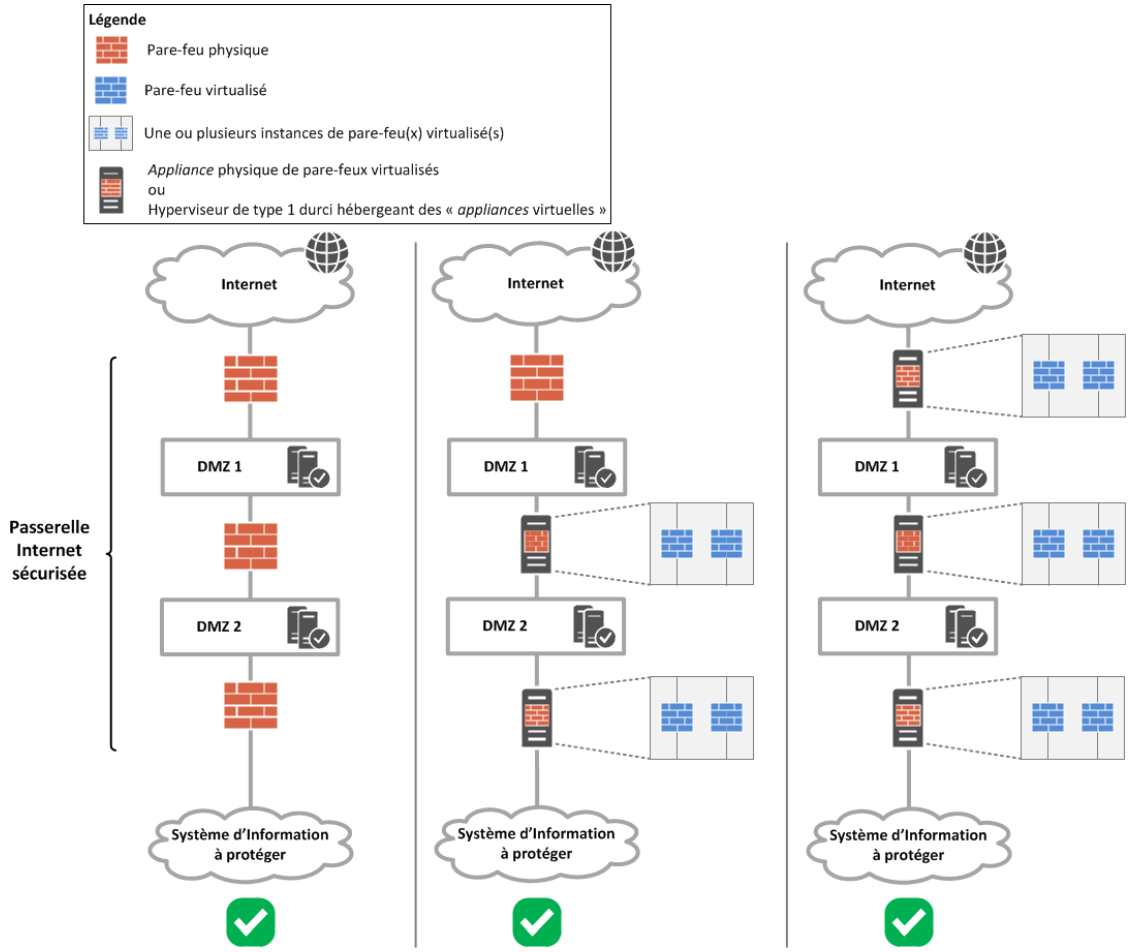

FIGURE 4.2 – Passerelles sécurisées complexes : exemples d'architectures possibles

Dans le cas des passerelles Internet sécurisées protégeant des SI DR ou sensibles, la recommandation R10 invite à positionner préférentiellement le pare-feu qualifié au niveau standard au contact du réseau de moindre confiance. Cette zone de moindre de confiance ou *réseau de classe 0* (tel qu'il est défini en annexe 2 de l'II 901 [8]) n'est pas nécessairement Internet : il peut exister, entre Internet et le pare-feu qualifié, des équipements et des informations ayant un moindre niveau de

criticité pour l'entité. Une telle zone pourra elle-même être protégée par un pare-feu qui ne sera pas nécessairement un pare-feu qualifié.

Par ailleurs, des raisons technologiques peuvent aussi justifier que ce soit un pare-feu non qualifié qui soit connecté en frontal d'Internet. Par exemple, considérons une entité à la recherche d'une fonction de pare-feu permettant de réduire l'impact d'une attaque en déni de Service de type DDoS [33]. Si cette fonction n'est pas disponible sur des pare-feux qualifiés, alors l'entité recherche cette fonction prioritairement sur un pare-feu certifié.

La figure 4.2 donne un exemple d'architecture de ce type et montre les contours des réseaux de classe 0 et de classe 1 tels qu'ils sont définis dans l'II 901.

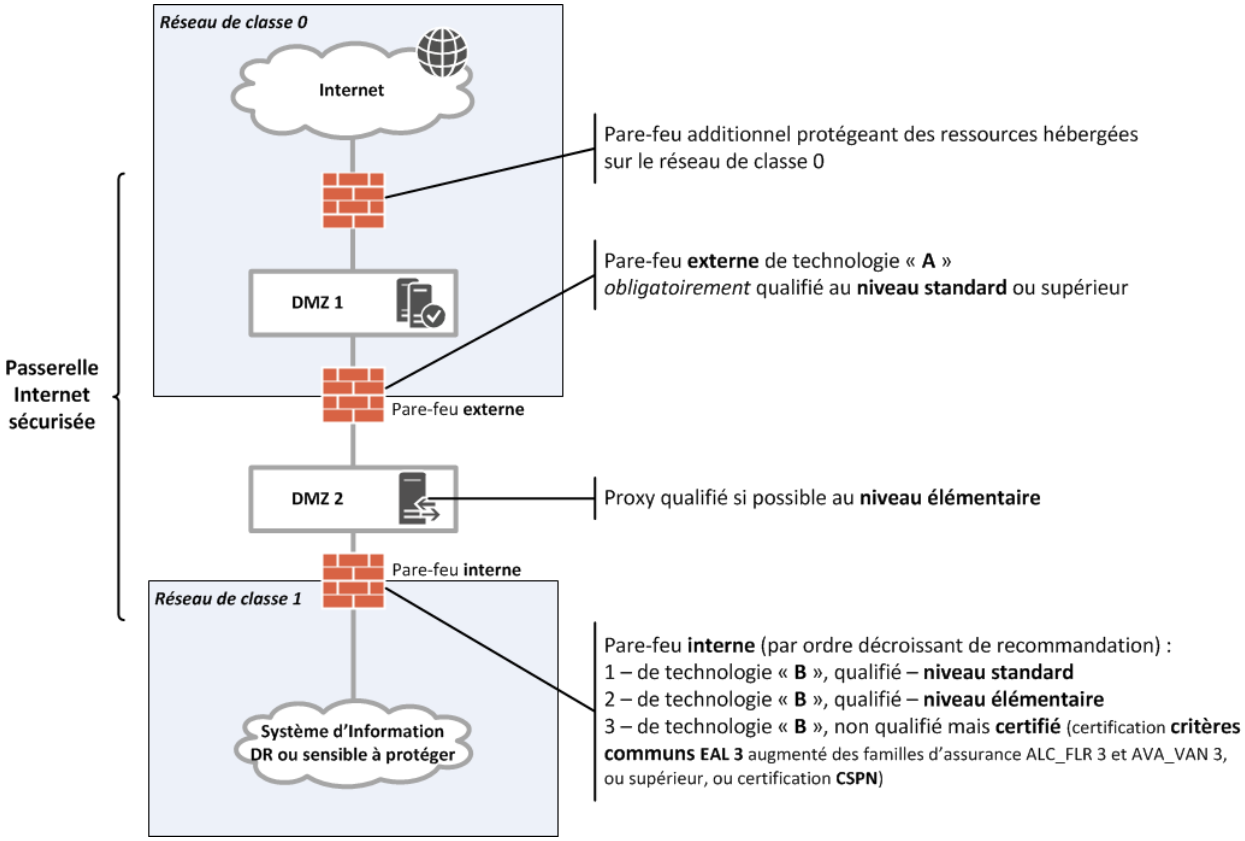

FIGURE 4.3 – Passerelles sécurisées complexes : exemples d'architecture dans le cas de systèmes d'information à protéger DR ou sensibles

Attention

La multiplication des pare-feux au sein des SI d'une entité ne doit pas être faite au détriment de la recommandation R3 relative à la maîtrise des technologies par l'exploitant des pare-feux.

33. *Distributed Denial of Service*.

5
Annexe 1

Cette annexe détaille les raisons techniques pour lesquelles la virtualisation des pare-feux est déconseillée.

- Contrairement à un pare-feu physique, un équipement virtuel ne peut pas reposer sur une pile réseau maîtrisée : une part plus ou moins importante de la couche d'abstraction issue de la virtualisation sera sollicitée, et celle-ci n'aura pas été évaluée comme peut l'être un pare-feu.
- Les privilèges élevés de l'hyperviseur par rapport aux VM permettent à un attaquant qui aurait réussi à obtenir certains droits sur le système de virtualisation de porter atteinte aux fonctions du pare-feu, par exemple en contournant la politique de sécurité ou en faussant les fonctions cryptographiques. Une partie de l'intérêt d'un pare-feu repose généralement dans la confiance en sa faculté d'autoprotection, qui est ici compromise.
- Dans la mesure où les privilèges d'administrateur de l'hyperviseur permettent assez facilement d'accéder aux privilèges d'administrateur d'un système invité, que ce soit un serveur ou un pare-feu, il n'est plus possible d'appliquer strictement la bonne pratique consistant à séparer les rôles d'administrateur système et d'administrateur réseau. En pratique, un compte d'administrateur de l'hyperviseur suffirait en effet à modifier la configuration des serveurs et des pare-feux.
- Pour les solutions offrant des fonctions de filtrage de flux et de chiffrement, l'effet de la couche de virtualisation sur la qualité des générateurs d'aléa des systèmes invités est difficile à évaluer (certains éléments utilisés comme source d'aléa peuvent être émulés et donc avoir un comportement plus déterministe). On ne peut pas exclure que les opérations cryptographiques d'un pare-feu virtualisé soit de ce fait affaiblies dans certains cas.
- Certains pare-feux proposent des fonctions avancées basées sur des composants matériels dédiés. Ces composants n'existant pas en environnement virtualisé, il est possible que les fonctions associées soient indisponibles, ou moins efficaces ou encore aient un fonctionnement différent (et potentiellement moins mature et moins testé) que dans la déclinaison matérielle.
- Le taux de disponibilité d'un pare-feu virtualisé pourrait être moindre que celui d'un pare-feu physique doté d'un mécanisme de haute disponibilité.

Liste des recommandations

Bibliographie

[1] *Recommandations de sécurisation d'un pare-feu Stormshield Network Security (SNS) - Version 2.7.2*.
Guide ANSSI-BP-031 v2.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/guide-sns/.

[2] *Externalisation et sécurité des systèmes d'information - Un guide pour maitriser les risques*.
Guide Version 1.0, ANSSI, janvier 2013.
https://www.ssi.gouv.fr/infogerance.

[3] *La défense en profondeur appliquée aux systèmes d'information*.
Guide Version 1.1, ANSSI, juillet 2004.
https://www.ssi.gouv.fr/defense-profondeur.

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

[5] *Recommandations 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] *L'homologation de sécurité en neuf étapes simples*.
Guide Version 1.2, ANSSI, février 2015.
https://www.ssi.gouv.fr/guide-homologation-securite.

[7] *Nettoyage d'une politique de pare-feu*.
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.
https://www.ssi.gouv.fr/nettoyage-politique-fw/.

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

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

[10] *Qualification*.
Page Web Version 1.0, ANSSI, mars 2016.
https://www.ssi.gouv.fr/qualification/.

ANSSI-PA-044
Version 1.0 - 22/01/2018

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN