Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

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

Paris, le 08 décembre 2011

N° 3248/ANSSI/ACE

GUIDE DE DEFINITION D'UNE ARCHITECTURE DE PASSERELLE D'INTERCONNEXION SECURISEE

Ce guide présente les différents principes permettant de définir l'architecture d'une passerelle d'interconnexion sécurisée. Ne seront considérées ici que les interconnexions entre un réseau privé (un *LAN*) hébergeant des informations sensibles mais non classifiées de défense[1] et un réseau ouvert (typiquement Internet).

On prendra pour illustrer notre propos le cas d'école d'une petite entreprise disposant d'un réseau interne et qui souhaite interconnecter ce réseau avec Internet pour permettre :

- d'une part à ses utilisateurs d'accéder à internet depuis leur poste de travail;
- d'autre part aux internautes d'accéder au site web de l'entreprise.

Ce document s'adresse en priorité aux architectes et administrateurs réseau de petites et moyennes entreprises ou de services de l'État. Des connaissances basiques en matière d'architectures réseau sont par ailleurs nécessaires pour appréhender certains des concepts présentés ci-après. Ce document se veut un guide en matière d'interconnexion, il n'édicte pas de règle impérative, mais décrit un ensemble de concepts ou de recommandations que chacun pourra adapter en fonction de ses contraintes et de ses enjeux.

1 Introduction

1.1 Analyse succincte des menaces

Les menaces principales considérées ici sont les suivantes :

- compromission (fuite) de données sensibles depuis le réseau de l'entreprise vers Internet ;
- *défiguration* du serveur web. Un attaquant peut en effet chercher à modifier le contenu du serveur web à des fins de désinformation, d'atteinte à l'image de marque de l'entreprise ou de revendication.

Bien que le présent document ne se focalise que sur la passerelle d'interconnexion, l'attention du lecteur est attirée sur le fait que la prise en compte de la sécurité sur le réseau interne (postes clients du réseau interne, serveurs, postes d'administration) est un **prérequis primordial**. En effet, sauf à

[1] Les questions de protection des informations classifiées de défense et les contraintes légales ne sont pas abordées ici.

utiliser des mécanismes extrêmement robustes et complexes (labellisation cryptographique de l'information notamment), il sera en règle générale impossible pour une passerelle d'empêcher seule la fuite d'information depuis un poste du réseau interne compromis par un attaquant. La passerelle ne pourra pas non plus empêcher un utilisateur légitime du système de faire fuir volontairement des informations (via la passerelle elle-même ou par support amovible). Les règles élémentaires de sécurité des postes utilisateurs sont donc impérativement à respecter avant toute interconnexion du réseau interne avec Internet. Pour mémoire, on s'attachera notamment à :

- maintenir à jour l'intégralité du parc des équipements ;
- n'octroyer aux utilisateurs que les privilèges et les droits nécessaires à leur activité (et dans tous les cas ne pas donner aux utilisateurs d'accès de niveau « administrateur » sur leur machine) ;
- désactiver les services inutiles ;
- activer et configurer finement un pare-feu personnel sur chaque machine ;
- définir une politique de sécurité pour le réseau qui définisse notamment une politique en matière de gestion de supports amovibles ;
- superviser le réseau, journaliser et définir une organisation de gestion d'incidents ;
- sensibiliser les utilisateurs à la menace.

1.2 Principes généraux et démarche

La conception d'une passerelle d'interconnexion ne se limite pas au choix d'une « *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 propre robustesse ;
- la capacité pour l'équipe technique chargée de le mettre en œuvre de le maîtriser et de le maintenir dans un état sécurisé.

a Apport pour la sécurité

L'apport sur le plan de la sécurité d'un produit correspond à sa fonction de sécurité principale, c'est à dire celle pour laquelle on met en œuvre le produit. Ainsi, par exemple, la fonction principale d'un pare-feu est de bloquer les flux réseau non autorisés. Toute autre service que le pare-feu est également capable de rendre (détection d'intrusion, routage avancé, traduction d'adresse) doit être considéré comme une fonction secondaire de l'équipement.

L'efficacité de la fonction de sécurité principale vis-à-vis des objectifs de sécurité du produit peut être vérifiée par une évaluation. C'est la raison d'être d'un certain nombre des labels de l'ANSSI (certification, qualification). Les produits bénéficiant de tels labels font l'objet d'une évaluation de sécurité indépendante dans un centre agréé par l'ANSSI. Le schéma de qualification permet par ailleurs de garantir que les produits ont été évalués spécifiquement en vue d'être mis en œuvre au sein d'une administration ou d'une entreprise. L'ANSSI recommande donc vivement l'emploi de produits qualifiés[2].

[2] http://www.ssi.gouv.fr/fr/produits.

b *Robustesse*

La robustesse d'un produit est sa propre résistance aux attaques. Un équipement réseau ne doit pas lui-même affaiblir la sécurité de la passerelle à laquelle il appartient. Certains équipements peuvent en effet disposer de fonctions auxiliaires (administration, mises à jour) particulièrement vulnérables et exploitables facilement par d'éventuels attaquants.

La robustesse d'un produit peut être estimée notamment en suivant les alertes et les avis des différents CERT[3] et notamment du CERTA[4]. L'utilisation d'un produit suivi par le CERTA et pour lequel des correctifs de sécurité sont systématiquement émis pour corriger les vulnérabilités mises en évidence sera bien sûr préférable à l'utilisation d'un produit inconnu ou non suivi par le réseau des CERT.

c *Maîtrise par les administrateurs et maintenabilité*

L'absence de maîtrise d'un produit, quelles que soit ses qualités intrinsèques, peut conduire à remettre en cause sa sécurité, par exemple suite à une erreur d'administration, ou à l'absence d'application des mises à jour par crainte des pannes. La bonne maîtrise dans le temps d'un produit repose naturellement sur l'adéquation entre son niveau de complexité (fonctionnalités, architecture) et les capacités (effectifs et compétences techniques) de l'équipe chargée de le mettre en œuvre. Elle est de plus facilitée par un certain nombre de facteurs intrinsèques au produit, notamment la qualité de sa documentation et de ses interfaces de paramétrage (qui, idéalement, ne doivent pas permettre la définition d'une configuration non sécurisée), la disponibilité d'un mécanisme de mise à jour robuste et documenté, et celle d'outils pertinents d'aide à la résolution de problèmes (journaux, validation de configuration, etc.).

d *Démarche*

La démarche retenue ici est de proposer une démarche de construction d'une passerelle d'interconnexion en partant d'une architecture très simple (mais peu résistante aux attaques) pour aller vers une architecture plus robuste (mais plus complexe). Il est important de noter que les éléments fournis ici n'ont aucun caractère impératif et doivent être interprétés comme un ensemble de conseils à appliquer (ou non) au cas par cas. Les choix relatifs à l'architecture finalement mise en place doivent être faits en prenant en compte :

- la sécurité de la passerelle ;
- sa maintenabilité ;
- les éventuelles contraintes opérationnelles et budgétaires.

e *Légende des schémas*

On retiendra la légende suivante pour les schémas:

- LAN: il s'agit du réseau interne de l'entreprise, celui sur lequel se trouvent les données sensibles, que l'on cherche à protéger, mais aussi celui sur lequel on peut mettre en place des mécanismes de sécurité ;
- WAN: il s'agit du réseau externe (typiquement Internet). C'est ici que se trouvent la majeure partie des attaquants (hors compromission d'un poste interne ou attaque interne). Il s'agit par ailleurs d'un réseau non-maîtrisé sur lequel il n'est pas possible *a priori* de mettre en place le moindre mécanisme de sécurité ;

3 Computer Emergency Response Team.
4 http://www.certa.ssi.gouv.fr.

- FW: il s'agit d'un filtre de paquet (pare-feu) en couches réseau et transport (couches 3, typiquement IP, et 4, typiquement TCP/UDP). Ce type d'équipement ne fait aucun traitement de niveau applicatif, et ne porte un jugement sur les paquets que sur la base des informations de ses couches basses (adresses IP de source et de destination, ports TCP et UDP). Il effectue par ailleurs le routage de paquets entre ses interfaces ;
- DMZ: Zone démilitarisée. Il s'agit d'une zone de service. Il peut s'agir de services applicatifs (serveur web, serveur de messagerie) ou de services de sécurité (serveurs mandataires - *proxy* - ou *reverse proxy)*. Cette zone tient son nom de sa position classique dans l'architecture d'une passerelle (voir plus bas).

On pourra noter que les équipements de niveau 2, c'est à dire les concentrateurs (*hub*) et les commutateurs réseau (*switch*), ne sont pas, de manière systématique, représentés sur les schémas. En effet, il n'existe à l'heure actuelle aucun équipement réseau de ce type qualifié par l'ANSSI. Il n'est donc pas possible de porter un jugement objectif sur le niveau et l'efficacité des mécanismes de sécurité que peut proposer un tel équipement. Les mécanismes de sécurité proposés peuvent toutefois être mis en œuvre au titre de la *défense en profondeur*. Une fois l'architecture de la passerelle définie proprement au niveau IP et transport (TCP, UDP), il est possible d'activer, en plus, les mécanismes de sécurité des niveaux inférieurs. En particulier, on préférera, sauf cas très spécifique, la mise en œuvre d'un commutateur (*switch*) à la place d'un concentrateur (*hub*). Par ailleurs, on veillera à bien assurer un partitionnement physique clair des différentes zones réseau : les architectures présentées ci-dessous ne sont valides qu'en l'absence d'interconnexions supplémentaires. On prendra en particulier garde à l'absence de tout type d'accès réseau complémentaire qui permettrait de relier le LAN au WAN sans passer par la passerelle (notamment par des communications sans fil : wifi, 3G, etc.).

2 Études d'architecture

2.1 Architecture basique

L'architecture la plus simple que l'on puisse proposer est présentée sur la Figure 1. L'interconnexion se résume ici à un simple pare-feu. Les serveurs applicatifs (y compris les serveurs web accessibles depuis internet) sont directement connectés au LAN. Les flux applicatifs considérés ici sont représentés par les schémas. Il s'agit ici:

1. des flux de consultation internet depuis le LAN ;
2. des flux de consultation du serveur Web par les internautes depuis internet ;
3. des flux de mise à disposition de contenu sur le serveur Web depuis le LAN.

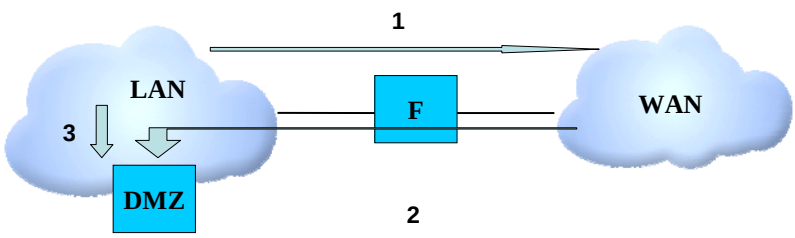

Figure 1: architecture basique et identification des flux

Les flèches représentées correspondent aux flux logiques. Il est évident que les échanges réels sont bidirectionnels. Toutefois la flèche indique quelle est l'entité à l'origine de la création du flux (point de départ de la flèche) et celle qui n'est pas à l'initiative du flux mais qui en est destinataire (pointée par la flèche). **Identifier les flux et leur sens est primordial**. La plupart des pare-feux modernes sont aujourd'hui contextuels (*stateful*). Ils sauront donc identifier les paquets provenant du WAN dont l'émission n'a pas été sollicitée par une machine du LAN et les filtrer en conséquence.

Cette architecture souffre de plusieurs problèmes de conception :

- Problème 1: les flux depuis Internet vers le serveur web traversent systématiquement le LAN. Ce point est extrêmement problématique. La moindre erreur risque donc de permettre à un internaute quelconque d'adresser un paquet initialement destiné au serveur vers n'importe quelle machine du LAN. Un attaquant pourrait tirer parti d'une telle erreur pour adresser un paquet d'attaque à l'une des machines du LAN. A partir de l'une des machines du LAN, il est généralement relativement aisé de prendre contrôle de la majeure partie des composants du réseau interne. Mais surtout, en cas de compromission du serveur, le rebond vers les machines du LAN est quasi-trivial ;
- Problème 2: le pare-feu est un point névralgique de l'architecture. Si l'attaquant parvient à le compromettre où à le rendre complètement traversant (il ne fait alors que router des paquets entre ses interfaces), il peut alors accéder à l'ensemble du réseau cible. Ici encore, la compromission multiple de machines s'avère relativement aisée ;
- Problème 3: l'architecture ne propose aucune mesure de protection contre la défiguration du site web. En effet, les flux en provenance d'Internet peuvent légitimement atteindre le serveur web de l'entreprise. Si l'on suppose que l'attaquant connaît une attaque non publique sur l'un des logiciels mis en œuvre par le serveur web et accessible par internet, il peut alors prendre le contrôle du serveur et en modifier le contenu.

2.2 Architecture « accès DMZ via le pare-feu »

Le premier problème peut être aisément corrigé en connectant directement le serveur web de l'entreprise sur une des interfaces réseau du pare-feu. L'architecture obtenue est représentée sur la Figure 2.

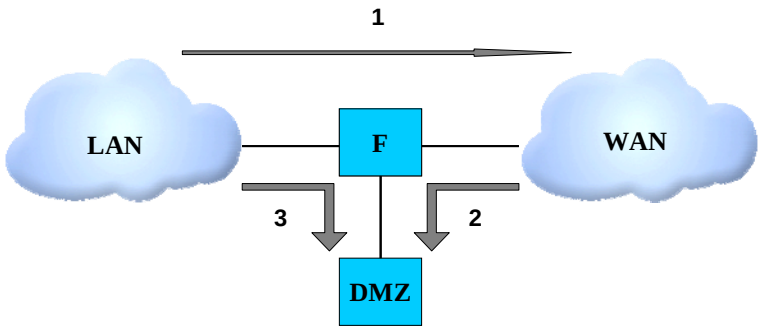

Figure 2: architecture « accès DMZ via le pare-feu »

Note importante : dans ce cas, seuls sont déplacés les serveurs devant être accessibles de l'extérieur. Les serveurs à usage interne (serveurs de fichier, base de données par exemple) doivent rester quant à eux connectés directement au LAN et accessibles uniquement depuis ce dernier. Cela nécessite pour l'entreprise d'identifier clairement les données qui peuvent être mises à disposition du grand public sur le serveur web et celles qui ne doivent pas l'être.

Cette architecture corrige correctement le premier problème (les flux à destination des serveurs Web ne circulent plus au travers du LAN) mais pas les deux autres dans la mesure où le pare-feu constitue toujours un point critique de l'architecture et où aucune protection spécifique n'est mise en place pour prendre en compte le risque de défiguration du site web.

2.3 Architecture basée sur deux pare-feux

Afin de prendre en compte le second problème, il convient de mettre en place deux pare-feux comme indiqué sur la Figure 3. L'un est placé en entrée de LAN (pare-feu interne, FWi) et l'autre à la frontière du WAN (pare-feu externe, FWe). Le nœud entre DMZ, FWi et FWe est par exemple assuré par un commutateur réseau.

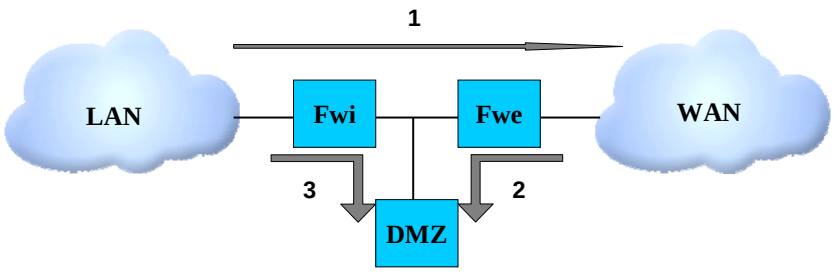

Figure 3: architecture basée sur deux pare-feux

La mise en place de ces deux pare-feux rend chacun de ces équipements non critiques. La compromission de FWe ne permet pas à un attaquant d'attaquer directement le LAN (FWi est toujours en coupure), et la compromission de FWi n'est pas aisée car, sauf en cas de compromission de FWe, aucun paquet de l'attaquant n'est routé vers FWi.

De plus, la configuration par un administrateur de FWi est relativement simple puisque ce dernier ne voit que des flux logiques sortants. Une erreur de configuration se remarque donc aisément.

Toutefois, la mesure n'est réellement efficace que lorsque les pare-feux sont réellement différents. Si les deux pare-feux sont identiques, un attaquant ayant connaissance d'une vulnérabilité pourrait prendre le contrôle successif de ces deux pare-feux sans réel problème. Il est donc important de mettre en place une diversification à tous les niveaux:

- au niveau du système d'exploitation (JunOS, IOS, OpenBSD, Linux, etc.);
- au niveau du moteur de filtrage (Packet Filter (PF), Netfilter);
- au niveau (si possible) du matériel.

Plus les équipements seront différents, plus le risque qu'un attaquant ait connaissance d'une vulnérabilité exploitable sur les deux pare-feux sera faible. Bien entendu, cette diversification technologique ne doit se faire que dans les limites de la maintenabilité du parc. Si la conséquence d'une telle diversification technologique est que le parc n'est plus maintenable (par manque de moyens et de compétences), il est certainement préférable de ne pas la mettre en œuvre.

Par ailleurs, il est fortement recommandé d'ajouter sur la DMZ un serveur mandataire (*proxy)* en charge d'effectuer un filtrage applicatif des échanges (dépollution, filtrage des contenus dangereux, maintien d'une liste blanche des sites accessibles et/ou d'une liste noire des sites interdits) entre les machines du LAN et les serveurs auxquels elles accèdent sur Internet. Les flux deviennent alors tels que présentés sur la Figure 4.

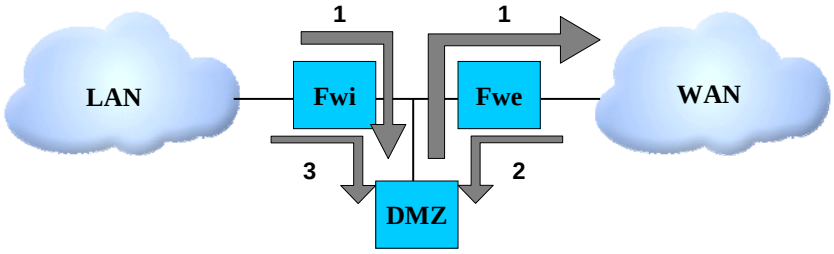

Figure 4: Flux lors de l'utilisation d'un serveur mandataire

Il est important de noter que, sur cette nouvelle architecture, la DMZ est en coupure sur l'ensemble des flux. Il est donc préférable de la placer en coupure physique sur les flux selon le principe présenté sur la Figure 5. L'utilisation d'une coupure physique en lieu et place d'une coupure logique permet physiquement de garantir qu'aucune communication n'est possible entre les deux pare-feux sans passer par la DMZ. Sans cette coupure, il existe un risque qu'un flux sortant soit adressé au WAN directement sans qu'il ne soit filtré au niveau applicatif.

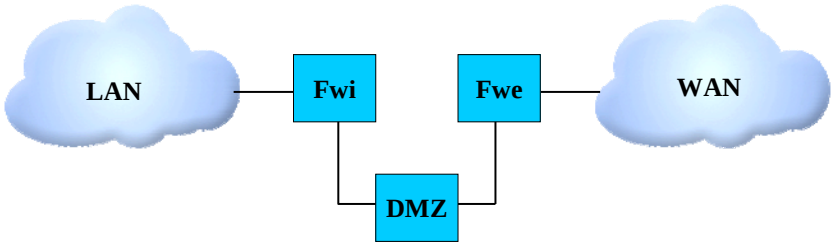

Figure 5: architecture DMZ en coupure physique

L'architecture obtenue est malheureusement encore imparfaite car elle ne fournit toujours aucun mécanisme permettant de protéger le serveur web contre une éventuelle défiguration.

2.4 Architecture « en double DMZ »

La prise en compte de cette dernière menace nécessite de mettre en place deux DMZ:

- une zone de service dite interne DMZi connectée directement à FWi et destinée à recevoir un ensemble de services fonctionnels ;
- une zone de service dite externe DMZe connectée directement à FWe et destinée à recevoir des services de sécurité.

Les différents flux sont représentés pour cette nouvelle architecture sur la Figure 6.

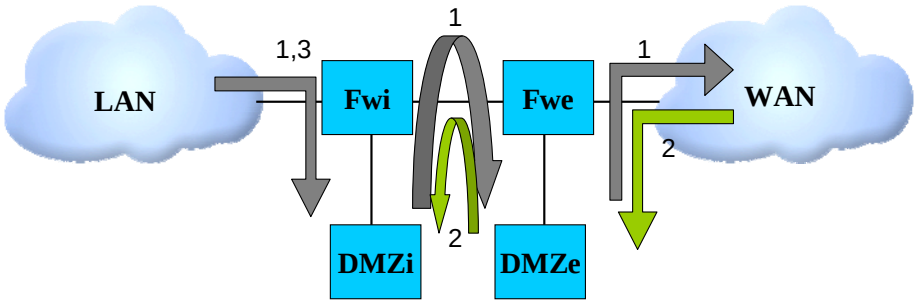

Figure 6: architecture avec deux DMZ

Ainsi, pour les flux entrants :

- la zone de service DMZi contient le serveur web proprement dit ;
- tandis que la zone DMZe contient un *reverse proxy* dont le rôle est d'assurer un filtrage des requêtes applicatives des internautes. Différents types de filtrage peuvent ainsi être effectués (analyse de requêtes suspectes avec des tailles d'URL trop grandes, contenant des mots clefs associés à des bases de données, etc.). Contrairement au *proxy* qui analyse prioritairement les réponses des serveurs externes aux requêtes, le *reverse proxy* analyse prioritairement les requêtes émanant de l'extérieur.

Pour les flux sortants:

- la zone DMZi fournit un *proxy cache* destiné à stocker temporairement les dernières pages ayant été consultées sur Internet. Ce service permet une accélération substantielle des requêtes ultérieures vers cette même page ;
- la zone DMZe fournit un *proxy* tel que celui décrit dans les précédentes architectures.

La protection du serveur web contre la défiguration s'effectue essentiellement grâce au *reverse proxy* de la DMZe. Cependant, il est important de comprendre que cette mesure seule ne permet pas de garantir la sécurité du serveur web. En effet, il existe de nombreuses façons de défigurer une page web :

- en compromettant le serveur web lui-même par modification du contenu des supports de stockage de masse - disques durs - ou de la mémoire du serveur uniquement. Dans ce second cas, la modification ne subsiste pas après un redémarrage de la machine ;
- en compromettant l'un des équipements réseau de la passerelle qui se trouve sur le chemin logique des paquets (pare-feu externe, reverse-proxy). L'attaquant peut en effet simuler un serveur web sur ces équipements qui se substituera au serveur web légitime ;
- en compromettant l'un des serveurs DNS utilisés successivement pour associer l'adresse IP du serveur web à son nom de domaine. Dans ce cas, l'attaquant peut rediriger tout le trafic destiné au serveur web vers la machine de son choix. Il est à noter qu'un certain nombre de ces serveurs étant obligatoirement hors du champ de responsabilité de l'entreprise, il n'existe en réalité pas de moyen simple d'obtenir une confiance absolue dans leur fonctionnement.

L'utilisation d'un site HTTPS (plutôt qu'un site HTTP) permet de réduire l'impact d'un dysfonctionnement des DNS externes ou d'une attaque sur ces dernières, en associant au serveur web une identité numérique rattachée à une racine dite « de confiance ». Cependant, les flux web sont alors encapsulés dans une session SSL/TLS chiffrée sur laquelle il n'est plus possible d'effectuer de filtrage. Dans ce cas, l'utilisation d'accélérateurs SSL avant le reverse proxy peut constituer une solution satisfaisante.

2.5 Architecture avec 3 pare-feux

Les deux DMZ de la figure précédente étant en coupure logique, il apparaît à nouveau sensé de les placer en coupure physique. Si l'on effectue une telle modification, il est nécessaire de faire apparaître un troisième pare-feu entre ces deux DMZ (FWm pour « filtre médian »). Le rôle de ce pare-feu est de permettre un cloisonnement physique entre les serveurs eux-mêmes. En effet, par souci de simplification, nous avons considéré jusqu'ici qu'il n'y avait qu'un seul et unique serveur accessible de l'extérieur. En réalité, il devra probablement exister plusieurs serveurs (courriel, web, DNS) accessibles depuis l'extérieur de l'entreprise et donc autant de *reverse proxies*. Le cloisonnement physique est réalisé en associant chaque serveur à une interface différente du pare-feu. Cette architecture permet de plus de limiter le risque de compromission de la passerelle en n'autorisant explicitement au niveau du filtre médian que les flux autorisés entre serveurs et *reverse proxy* ayant besoin de communiquer. Si l'on suppose que par exemple, le *reverse proxy* de courriel utilisé est faible sur le plan de la sécurité et peut être compromis par un attaquant, ce dernier peut tenter de rebondir sur ce *reverse proxy* pour court-circuiter le *reverse proxy web* et attaquer le serveur web. Ce flux n'étant pas prévu par la politique de sécurité du filtre médian, ce dernier pourra bloquer les flux d'attaque et lever une alerte. En d'autres termes, le cloisonnement effectué permet de réduire le risque d'exploitation successive de vulnérabilités dans des composants faibles qui n'ont pas impérativement besoin de communiquer.

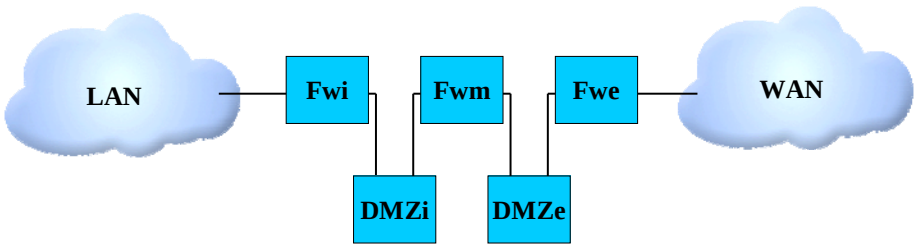

Figure 7: architecture avec deux DMZ en coupure physique

3 Problèmes annexes

3.1 Problématique de l'adressage IP

Il est bien entendu possible d'utiliser le même accès internet pour la gestion des flux entrants à destination de la DMZ et des flux sortants. Cependant, il est préférable dans la mesure du possible d'utiliser au minimum des adresses IP distinctes pour ces deux types d'accès. Idéalement, l'adresse IP associée aux flux sortants est dynamique et moins visiblement reliée à l'entité concernée, ce qui permettra de limiter le risque en termes d'image (voire de service) dans le cas où un employé peu scrupuleux se livrerait à des activités douteuses (consultation de sites pornographiques par exemple) depuis l'accès internet professionnel. L'adresse IP utilisée pour les flux entrants peut bien évidemment être fixe.

Dupliquer les moyens d'accès internet (accès nominal par le réseau d'un opérateur, accès de secours par le réseau d'un second opérateur) permet par ailleurs de garantir une meilleure disponibilité de l'accès. L'intégration d'une telle redondance sur les flux entrants nécessite toutefois un peu de travail car il est nécessaire de gérer un routage dynamique (une AS[5]) 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. Gérer une redondance uniquement pour le trafic sortant est plus aisé.

[5] Autonomous System.

3.2 Problématique de la mutualisation des ressources

En fonction de l'architecture qui sera retenue, le nombre de machines logiques constitutives de l'interconnexion peut être potentiellement élevé. Aussi peut-il paraître intéressant de regrouper les différents services sur une même machine physique. Ce regroupement peut simplement se faire en faisant tourner différentes applications sur le même système d'exploitation ou en mettant en œuvre des techniques de virtualisation plus ou moins lourdes.

Les risques liés à la mutualisation des ressources sont les suivantes :

- déni de service. Le dysfonctionnement d'une des applications installées sur une machine physique peut entraîner une panne de la machine et donc 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),

En conclusion, l'opportunité de faire s'exécuter sur une même machine plusieurs services devra être évaluée en prenant en compte les recommandations suivantes :

- il est recommandé de ne faire fonctionner sur une même machine que des services de même nature. Par exemple, il est risqué de faire tourner 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 ;
- bien entendu, il n'est pas souhaitable de faire tourner sur une même machine physique un serveur nominal et son éventuel serveur de secours.

Certaines limitations opérationnelles liées aux éventuelles adhérences des services à un système d'exploitation ou à une architecture matérielle particulière viennent par ailleurs limiter les capacités en matière de mutualisation de services. Enfin, il est important de noter que certains serveurs sont interdépendants. Typiquement, si le serveur DNS de l'entreprise tombe, son serveur web ne sera plus accessible. Réciproquement, si le serveur web tombe, les clients n'auront peut-être plus de raisons de faire des requêtes au serveur DNS. Il est donc envisageable de regrouper ces deux services sur une même machine, dans la mesure où leurs besoins en matière de disponibilité sont similaires.

3.3 Problématique des postes nomades

Une question qui se pose à ce stade est celle des utilisateurs nomades du système d'information. Est-il possible d'autoriser des utilisateurs à accéder à distance à tout ou partie des informations disponibles sur le LAN ? Il s’agira ici de faire un arbitrage entre le niveau de durcissement du poste nomade des opérateurs (et les contraintes éventuelles d’utilisation qui en découlent) et les fonctions offertes via le terminal nomade. La règle générale est que plus le terminal sera sécurisé, plus les fonctions offertes pourront être nombreuses.

En particulier, un facteur favorable est que les postes nomades soient gérés comme les postes d'infrastructure du LAN :

- les utilisateurs ne doivent pas être administrateurs de leur machine ;
- la politique de mise à jour doit être strictement identique à celle des postes fixes, de même que la politique d'authentification, qui peut même être renforcée en raison du caractère nomade des postes ;

- les flux web doivent être véhiculés par la passerelle d'interconnexion (voir ci-dessous).

De plus, il est nécessaire de prendre en compte les usages spécifiques aux postes nomades, notamment :

- désactiver dans la mesure du possible les interfaces sans-fil, sources de nombreuses vulnérabilités ;
- chiffrer le disque dur avec un moyen qualifié[6] par l'ANSSI pour réduire l'impact de la perte ou du vol d'un poste nomade ;
- sensibiliser les utilisateurs à la politique de sécurité. En particulier, il doit être explicitement interdit d'accéder à des informations sensibles dans des endroits publics (trains, métro, parcs, cafés, etc.).

Au niveau de l'architecture de la passerelle, il est conseillé de retenir une architecture telle que celle qui est décrite ci-dessous.

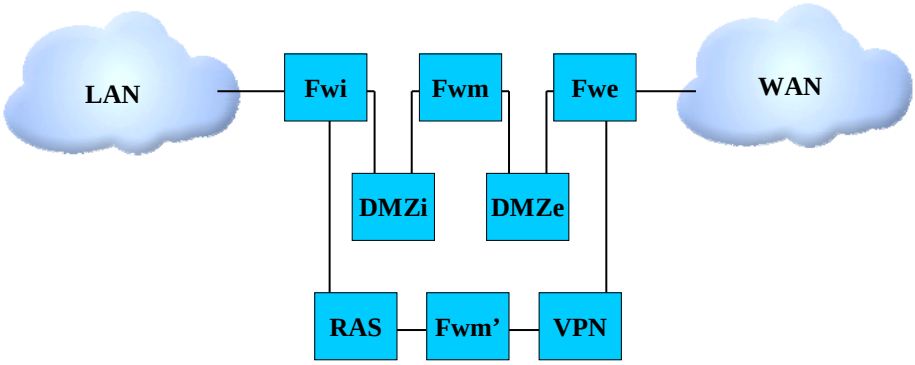

Figure 8: accès nomade

L'architecture proposée met en œuvre une machine effectuant une authentification des postes distants et un déchiffrement des flux au niveau IP (protection de type IPsec) depuis et à destination de ces postes (VPN). Le lien entre authentification et chiffrement doit être fort pour garantir que seuls les postes réellement authentifiés pourront adresser des paquets à la passerelle[7]. Il est fortement conseillé que la machine VPN soit située sur une interface spécifique du pare-feu FWe. En effet, les flux chiffrés par IPsec sont difficilement filtrables par les pare-feux car leur contenu ne peut être inspecté et le protocole est « sans état » (pas de filtrage contextuel possible). Les faire transiter via la passerelle principale annule donc tous les efforts faits pour maîtriser les différents échanges au sein de la passerelle.

Les flux déchiffrés par la machine VPN sont ensuite traités par un filtre médian (FWm) chargé d'effectuer un filtrage au niveau des couches réseau et éventuellement au niveau des couches applicatives. En effet, le fait qu'une machine soit authentifiée ne garantit pas que les flux qu'elle émet ne puissent pas être vecteurs d'attaques. En d'autres termes, le fait que les flux soient authentifiés ne garantit pas leur innocuité. Ensuite, les flux peuvent être adressés à un serveur d'accès distant (RAS). Ce serveur peut être un simple serveur http, ou ftp. Il est possible de se passer de ce serveur et de connecter directement le filtre FWm' à FWi pour permettre un accès distant au LAN. La décision de se passer ou non de ce serveur dépend du niveau de confiance que l'on peut avoir dans les postes clients. Idéalement, les flux internet des postes nomades passent systématiquement par la passerelle (VPN, FWm', FWi, DMZi, FWm, DMZe, FWe) pour sortir sur Internet.

---

[6] http://www.ssi.gouv.fr/fr/qualification.

[7] Il est fondamental que l'authentification permettant d'ouvrir le tunnel soit reliée au protocole utilisé pour protéger la confidentialité et l'intégrité de la communication.

3.4 Problématique de la supervision

La supervision, la mise à jour et l'administration à distance des équipements de la passerelle doivent être effectuées par un ensemble de stations dédiées, connectées à une interface dédiée de chacune des machines de la passerelle. Les équipements ne routent aucun flux vers cette interface. La machine en charge de la supervision doit elle-même être protégée par un pare-feu pour limiter le risque de rebond entre deux éléments de la passerelle au travers de la machine de supervision.

Il est à noter que les flux d'administration ou de mise à jour sont bien souvent chiffrés ce qui complique les capacités de filtrage sur ces flux. Il faut donc en principe éviter de les faire transiter par les pare-feu de la passerelle.

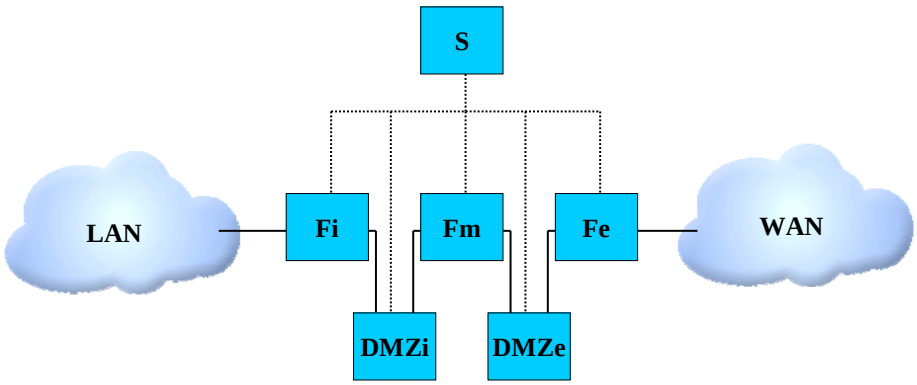

Figure 9: supervision de la passerelle d'interconnexion

3.5 Question des interfaces réseau

Chacune des machines de la passerelle doit piloter un nombre potentiellement important d'interfaces réseau. Un certain nombre de cartes réseau sont commercialisées avec plusieurs interfaces (par exemple 4 interfaces Ethernet sur la même carte). Il est conseillé d'avoir recours sur les pare-feux à des cartes différentes (et non seulement des interfaces) pour les flux entrants, sortants et les flux d'administration. En effet, les cartes disposant d'interface multiples ne comprennent bien souvent qu'un unique composant réseau connecté à toutes les interfaces. Le cloisonnement physique n'est donc pas réellement assuré en cas d'utilisation de telles technologies car tous les flux sont mélangés au sein d'un même composant.

4 Résumé et conclusions

4.1 Points importants à retenir

Les points suivants sont particulièrement critiques en matière de conception de passerelle d'interconnexion :

- disposer d'une politique de mise à jour la plus efficace et rapide possible pour l'ensemble des composants de la passerelle ;
- superviser en temps réel la passerelle et analyser les alertes. Toute connexion non prévue entre deux équipements doit être considérée comme une possible tentative d'attaque ;
- l'utilisation du protocole *DNS* pour résoudre les noms de machine au sein de la passerelle est à proscrire. Les machines doivent communiquer au niveau IP par la seule connaissance de leurs adresses respectives. De même il est possible de proscrire l'utilisation du protocole *ARP* dans la passerelle et de configurer les associations adresses Ethernet et adresses IP en dur.

Cette configuration vise à limiter les risques d'usurpation d'identité depuis l'un ou l'autre des composants du réseau ;

- utiliser un principe de diversification technologique dans la limite de la maintenabilité du parc.

4.2 Conclusion

Les principes exposés ici visent à décrire les fonctions de sécurité à mettre en œuvre dans une passerelle d'interconnexion face aux différentes menaces à prendre en compte. Le choix de l'architecture retenue doit être fait au cas par cas en fonction du niveau de sécurité attendu et des contraintes opérationnelles (financières, gestion du parc, maintenabilité, etc.).

5 Pour en savoir plus

Le Centre de formation en sécurité des systèmes d'information de l'ANSSI propose des formations destinées aux membres de l'administration. Notamment le stage 7b, organisé plusieurs fois par an, permet de mettre en pratique ces concepts en installant et configurant une passerelle d'interconnexion telle que décrite au point 2.3.

Diffusion

Diffusion publique sur www.ssi.gouv.fr.