Institut Universitaire de Technologie,
Aix-Marseille Université

Annexes

Mounir

BENLHAJ

Responsable entreprise : Didier Tonneau

Responsable académique : Roland DEPEYRE

2019

Table des matières

1 Proposition d’offre

Proposition D’Architecture Réseaux

Site de Saint-Jérome

Introduction

Le site universitaire de Saint Jérôme, souhaite lancer une formation incluant du smart grid, pour se faire il a besoin de deux nouvelles salles équipé de l’Iot.
Nous avons donc étés chargé de concevoir une nouvelle architecture réseaux pour les deux salles, et de faire une offre incluant le coût du matériel.
Dans cette proposition nous détaillerons, les choix que nous avons fait sur l’architecture réseaux, le choix des matériels et leurs positionnement.
Cette proposition n'incluant pas la main d’oeuvre.

SOMMAIRE

Devis et Conclusion……

Contexte

Aujourd'hui le site de Saint Jérôme, faisant partie de l'Université d'Aix-Marseille souhaite se préparer aux métiers de demain, et ainsi lancer une formation dans le smart grid(réseau électrique intelligent).

Figure 1 : Site de Saint-Jérôme

Le réseau électrique intelligent, est un réseau de distribution d'électricité qui favorise la circulation d'information entre les fournisseurs et les consommateurs, afin d'ajuster le flux d'électricité en temps réel et permettre une gestion plus efficace du réseau électrique, et ainsi réduire la production d'électricité. Tout cela à l'aide de différentes technologies reposant sur des capteurs, l'IOT (l'internet des objets) et des dispositifs de stockage.
Le smart grid sera donc un grand enjeux dans le domaine du développement durable. Ainsi les grands producteurs d'électricité comme EDF sont et seront à la recherche de personnes maîtrisant ses technologie, et leurs concepte.
Pour répondre à cette demande grandissante, le site de Saint-Jérôme a décidé d'ouvrir une formation spécialisé dans le smart grid.
Pour se faire elle compte ouvrir une section qui lui est dédiée, avec de l'IOT, ce qui inclut différents capteurs, des leds connectées, et des caméras ip.
Nous avons été sollicités pour proposer une architecture réseaux adapté aux salles.
Dans cette proposition, nous comparons différents modèles d'appareils que ce soient des capteurs ou des caméras, pour ensuite fournir une offre la plus complète, et la plus appropriée aux demandes exigées.

Architecture

Emplacement:

La section qui doit être aménagée, est celle du master génie électrique. Elle est constituée d'une grande salle de TP,d'un couloir principal reliant la salle de TP avec des salles annexes et des salles annexes de TP (figure 2) .

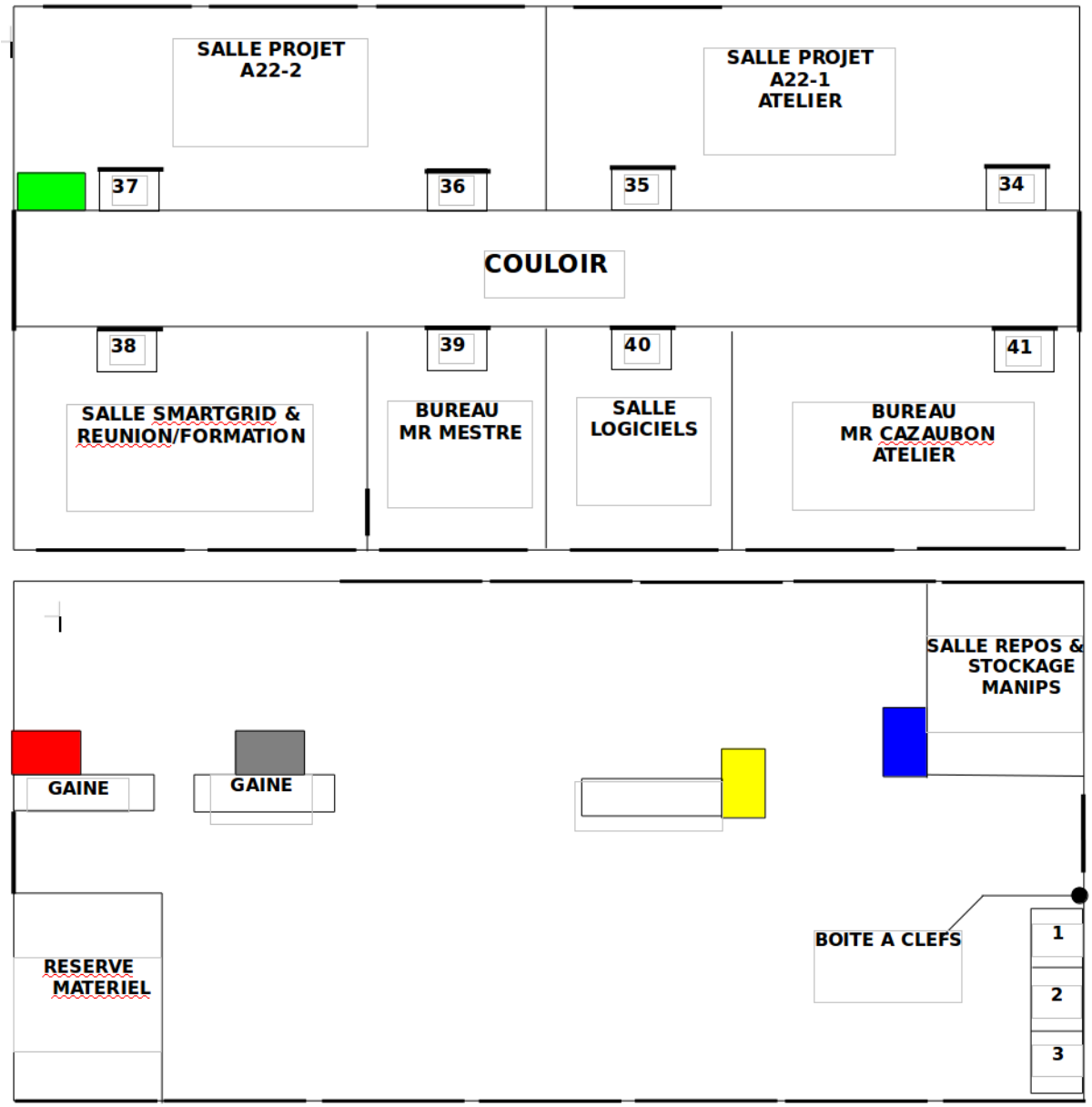
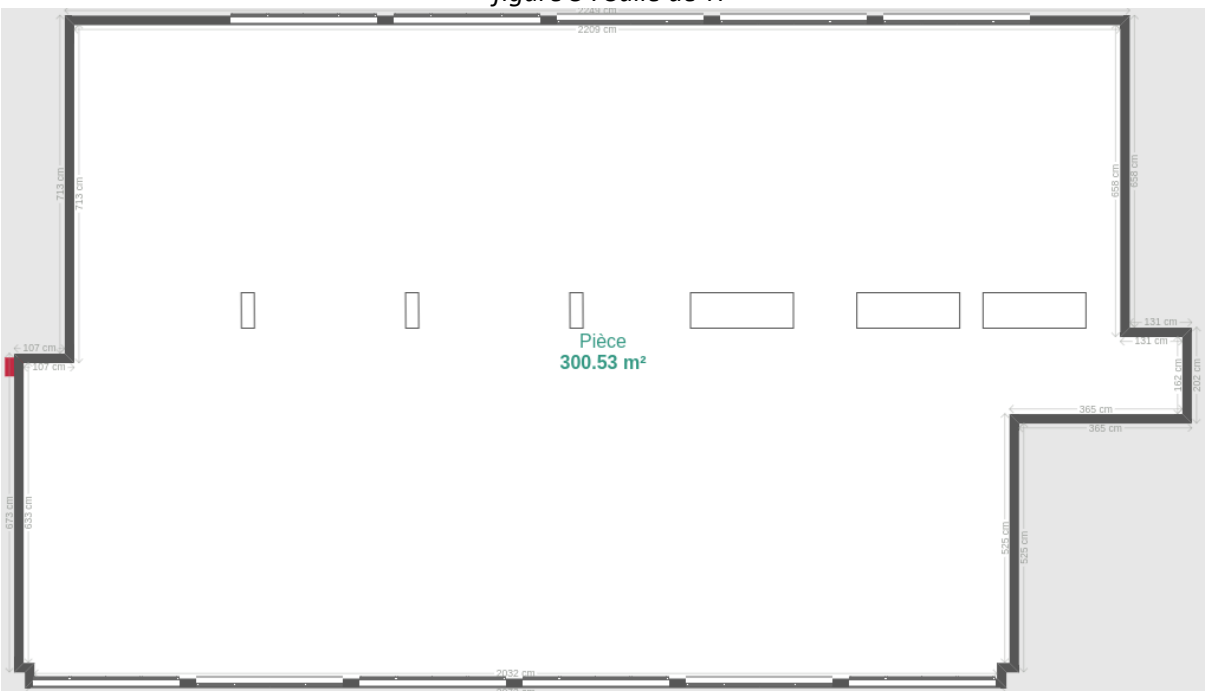


Figure 2 : Section du master génie electrique

La grande salle de TP mesure au total 343 m² (figure 3), comprenant une grande salle d'environ 300 m² et 2 salles de stockage d'environ 22 m² chacune.

La salle principale est traversé par plusieurs piliers au centre de la pièce, par lesquelles passe des gaines. De l'autre côté nous avons, 2 salles de projet de 63m² chacune, 2 bureau de 18m², un bureau de 36m² ainsi que la salle de Smart Grid qui fait également 36m².

figure 3 : Salle de TP



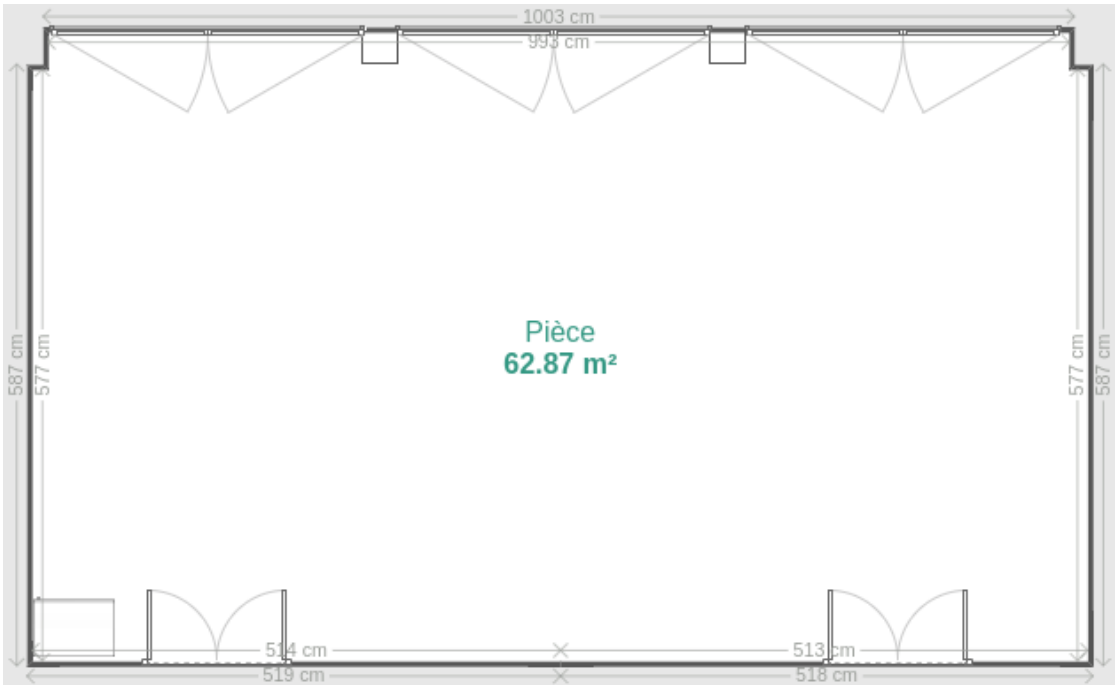


Figure 4 : Salle de projet

Figure 5 : Salle de Smart Grid

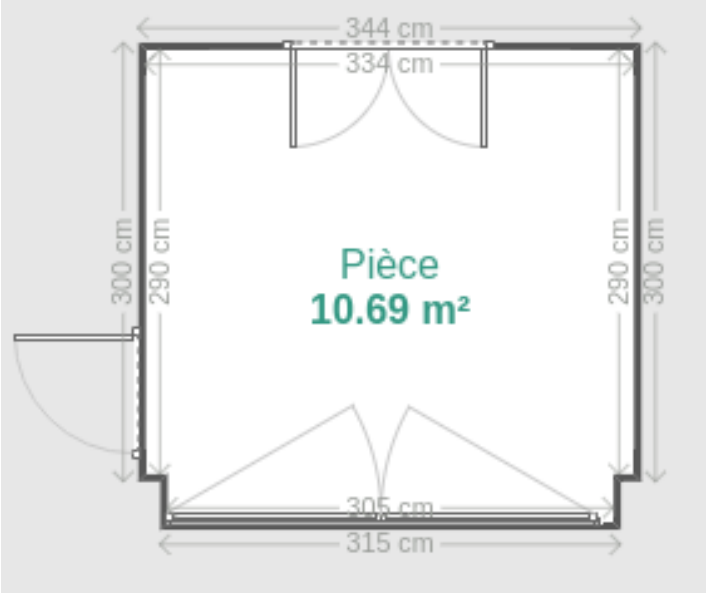


Figure 6 : Bureau

Comparatif de matériel

Câble

Le choix du type de câble est très important dans une architecture réseaux, ils doivent avoir une longue durée de vie car l'installation de câbles nécessite des travaux long et onéreux de ce faites le choix du câbles doit être pensé sur le long termes .
Ils existent 5 types de câbles, classés par ordre croissant en terme de qualité dans le tableau ci-dessous:

U/UTP	F/UTP	U/FTP	F/FTP	S/FTP
U	▪ **U** = Unfoiled (non blindé)			
TP	▪ **TP** = Twisted Pairs (blindage par paires torsadées)			
F	▪ **F** = Foiled (blindage par feuillard aluminium)			
S	▪ **S** = Shielded (blindage par tresse d'aluminium)			

U/UTP (Paire torsadée non blindée)

Les câbles les moins onéreux, et de moins bonnes qualités sont les U/UTP. U pour Unfoiled signifiant non blindé, le câble est donc sans protection par alluminium, et ne possède que des paires torsadées pour diminuer les bruits. Ce type de câble sont parfait pour un particulier qui souhaite relier ses appareils, sur de courte distance à son domicile.

F/UTP (Paire torsadée écrantée)

L'ensemble des paires torsadées a un blindage global assuré par une feuille d'aluminium. L'écran est disposé entre la gaine extérieure et les 4 paires torsadées. Les paires torsadées ne sont pas individuellement blindées, ce qui diminue les perturbations. Mais cette protection n'est pas suffisante si les câbles sont placé dans un lieu à forte perturbation.

U/FTP (Paire torsadée blindée)

Chaque paire torsadée blindée est entourée d'un feuillard en aluminium, de façon similaire à un câble coaxial.
Offre une protection supérieur contre les perturbations, comparé aux au F/UTP.

F/FTP (Paire torsadée doublement écrantée)

Chaque paire torsadée est entourée d'une feuille de blindage en aluminium, et l'ensemble des paires torsadées ont une feuille de blindage collectif en aluminium.
Protection contre les perturbations élevées, qui est suffisant dans des zones à fortes perturbations.

S/FTP (Paire torsadée super blindée)

Chacune des paires est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé. Protection optimale, pour les zones à très hautes perturbations.

Décision :

Pour le choix du type de câble il faut prendre en compte la disposition des câbles réseaux par rapport au câbles électrique.
La salle de TP de Saint-Jérôme nécessitera de tirer les cable reseaux avec les cable de courant fort.
Pour éviter les perturbations électromagnétique engendré par les câbles de courant fort
il sera impératif d'utiliser des câbles blindés avec une protection en aluminium.
Nous avons donc décidé d'utiliser des câbles S/Ftp de cat 6 pour assurer une bonne transmission des données qui ne risquera pas d'être atténuer par le bruit créer par les câbles électrique.

Equipement réseaux :

Switch :

Nous utiliserons 2 switchs Cisco modèle ws-c2960-48pst-l. Ils permettent l'utilisation du POE et possède 48 ports chacun, ce qui nous permettra d'utiliser 96 ports pour les capteurs.

Figure 7 : Switch Cisco ws-c2960-48pst-l

Pour ranger les switchs ainsi que les câbles nous aurons besoins d'une baie de brassage

Les Goulottes et port Rj 45 :

Pour les 2 salles, nous ferons passer le câbles par des goulottes prévues à cettes effet. Nous avons calculé que 40 mètres de goulottes, seraient suffisant.
Les goulottes seront de la marque Iboco, le modèle TA-C45 pour être précis.

Figure 8 : Goulotte

Ce modèle est clipsable, et compatible avec tous les appareillages du marché. Cela comprend aussi, le modèle de port Rj45 que nous avons sélectionné, le RJ45 C6 MOSAIC de LeGrand.

Figure 9 : Port RJ45

Le nombre estimé de port Rj45 est de 40.
En plus des goulottes, il faudra aussi commander différents angles pour goulottes intérieur, extérieur et plat.
Ils seront tous de la marque Iboco.

Figure 10 : Angle pour goulotte

Caméra :

Il a été demandé l'achat, et l'installation de caméra de surveillance, dans un but pédagogique. Les caméras devaient répondre à plusieurs critères:

- Elles devaient être IP
- Supporter la technologie PoE (Power over Ethernet) permettant de limiter le nombre de câbles.
- Avoir un prix raisonnable

En respectant ces conditions, nous avons sélectionné sur plusieurs centaines de modèles, 3 caméras qui avaient le meilleur rapport qualités prix.

	 D-Link Caméra IP DCS-4602EV	 TRENDnet TV-IP310PI	 Reolink Caméra IP RLC-410-5MP
Prix	**145,89 €**	**158 €**	**68.99 €**

Avantages	• Résistance • Détection de mouvement	• Détection de mouvement	• Détection de mouvement
Rotation	120/140°	70°	80°
Résolution	**1920x1080**	**1920x1080** **2048x1536**	**2560x1920**
Stockage	Pas de port SD	Pas de port SD	Carte SD 32Go
Mode Nuit	**OUI**	**OUI**	**OUI**
Poe	**OUI**	**OUI**	**OUI**
RoHs	**OUI**	**OUI**	**OUI**

Décision :

La caméra de Reolink est celle qui possède le meilleur rapport qualité prix sur les 3 caméras, elle semble toute désignée pour être sélectionnée. Mais son défaut est d'être très fragile contrairement à la D-LINK, et comme les caméras seront manipulées par des étudiants, et devront être fonctionnelle sur plusieurs années, nous avons finalement sélectionnés la Caméra IP de D-LINK.

Onduleur

La fonction première de tous les onduleurs est de protéger contre les coupures de courant. Certains d'entre eux permettent également de se prémunir contre 5 autres défaillances électriques existantes de la manière suivante :

Les Coupures : L'onduleur va maintenir la tension à 230 Volts grâce à ces batteries.
Les Chutes de tension : L'onduleur va faire remonter la tension à 230 Volts.
Les Surtensions : Les onduleurs vont faire baisser la tension à 230 Volts.
Les Pics : Les onduleurs lissent la courbe de tension de sortie en supprimant les pics de tension.
Les Bruits : L'onduleur vont permettre un filtrage des interférences électromagnétiques (EMI) et radio (RFI).
Les Distorsions : L'onduleur va réformer la courbe sinusoïdale de la tension en filtrant en permanence le courant produit.

Tous les onduleurs ne permettent pas de se protéger contre ces 5 défaillances, et sont donc répartie en 3 grands types : Onduleur off-line, Onduleur on-line, Onduleur in-line.
Chacun offrant un degré de protection plus ou moins élevé.

	Onduleur off-line	Onduleur in-line	Onduleur on-line
Coupure	X	X	X
Chute de tension		X	X
Surtension		X	X
Pic		X	X
Bruit		X	X
Distorsion			X

	 APC Back-UPS Pro 1500	 APC Smart-UPS 2200VA LCD 230V 2U Smart Connect	 APC SMART-UPS 2200VA LCD 230V SMART CONNECT	 APC Smart-UPS SRT 2200VA
prix	389€95	1499€95	883€	1 582€
Format de l'onduleur	TOUR	rack	TOUR	Rack/tour

Technologie de gestion de la batterie	Line-interactive (in-line)	Line-interactive (in-line)	Line-interactive (in-line)	ON-LINE
Puissance onduleur	1500VA	2200Va	2200Va	2200Va
Batterie	Batteries scellées plomb et acide sans entretien, avec électrolyte en suspension	Batteries scellées plomb et acide sans entretien, avec électrolyte en suspension	Batterie avec accumulateur au plomb sans entretien avec électrolyte suspendue, étanche	Batterie au plomb scellée sans entretien avec électrolyte suspendu, étanche
Autonomie	5.5 min pour 865 watts	16.1 minutes pour 990 watts	24 minutes pour 1000 watts	11 minutes pour 1000 watts
Nombre de prise	10	8	8	10
Evolutif	Non	Non	NON	OUI
Manageable	Oui	Oui	OUI	OUI
Type de serveur		Serveur intelligent	Serveur intelligent	Serveur intelligent

Décision :

Système d'éclairage

Ils nous à était demandé d'installer un système de gestion d'éclairage qui permettrait grâce à des capteurs de pouvoir contrôler et régler les luminaires, ce qui permettrait de faire des économies.

Il est apparu 3 solutions proposées par la société Philips Lighting :

La première serait de coupler des luminaires Led de la gamme des CoreLine avec l'OccuSwitch Dali, un système de gestion d'éclairage intelligent proposé par Philips.
La deuxième solution serait de prendre le service Interact Ready ….
La troisième solution proposé est une solution spéciale de philips utilisant des luminaires POE.

OccuSwitch Dali :

Fonction :
L'OccuSwitch DALI combine un détecteur de mouvement, une cellule photoélectrique et un récepteur Infrarouge. Ce dispositif contrôle l'allumage, l'extinction et la gradation des luminaires selon la détection de présence et des apports de lumière naturelle. Il est possible de le mettre en parallèle ou de le connecter à une GTB (Gestion Technique du Bâtiment) selon la version. Le capteur peut piloter jusqu'à 15 luminaires DALI. Facile à installer, il ne nécessite qu'une petite mise en service.

Avantage :
• Jusqu'à 55 % d'économies d'énergie et coût total de possession avantageux • Confort accru et contrôle local • Facilité d'utilisation (solution prête à l'emploi) et d'adaptation aux applications spécifiques ou souhaits de l'utilisateur

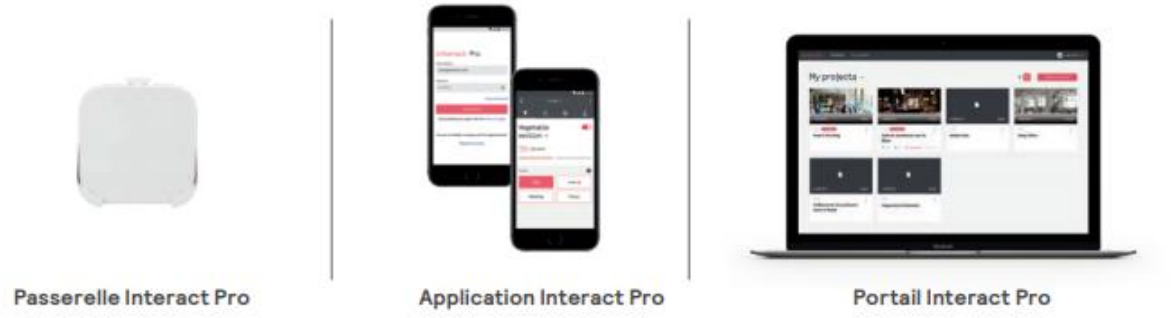
Il existe 3 versions de l'OccuSwitch Dali, Basic, Advanced et BMS. Nous avons choisis la BMS car elle offre une interaction avec la quasi-totalité des systèmes de gestion d'immeubles via l'interface DALI

Figure 11 : OccuSwitch Dali

Interact Ready

Fonctions :

Le système interact ready combine un large panel de capteur



Devis

Désignation	Quantité	Prix unitaire Euros HT	TOTAL Euros HT
D-LINK DCS-4602EV - CAMÉRA DÔME POE FULL HD	**14**		
Goulotte Iboco TA-C45 90/1X55 W0	**40**	**968.94/C**	
Port RJ45 LeGrand	**40**	**7.85**	**510.25**
Angle Intérieur Iboco	**20**	**906.78/C**	**181.36**
Angle Extérieur Iboco	**20**	**906.78/C**	**181.36**
Angle Plat Iboco	**20**	**1052.52/C**	**210.5**
Collier de Serrage	**100**	**7.55/C**	**7.55**
Bobine RJ45 Catégorie 6 SSTP	**200m**	**300**	**300**
Switch	**2**	**0**	**0**
	2	**0**	**0**

2 Synthèse du guide de l'ANSII

GUIDE DE DÉFINITION D'UNE ARCHITECTURE DE PASSERELLE D'INTERCONNEXION SÉCURISÉE

SYNTHÈSE

SOMMAIRE

Introduction

Cette synthèse présente, un résumé simplifié du guide de l'ANSSI sur une architecture de passerelle d'interconnexion sécurisée , qui est disponible grâce à ce lien: mil(https://www.ssi.gouv.fr/entreprise/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/).
Tout d'abord, nous allons définir qu'est ce qu'une passerelle d'interconnexion, et tout au long du rapport nous donnerons des conseils pour sécuriser la passerelle, en allant des plus simples et basiques jusqu'aux plus complexes mais plus sûr.

Une architecture passerelle d'interconnexions, permet d'interconnecter un réseau à un autre, dans notre cas entre un réseau privé (LAN) et un réseau externe (WAN) comme internet.

Analyse des menaces actuelles

Aujourd'hui quelque soit l'entreprise et son domaine d'activité, elle a ou aura besoin d'avoir un accès à internet, donc d'une passerelle d'interconnexion, mais une simple passerelle d'interconnexion ne permet pas de se protéger des différentes menaces et attaques provenant de l'extérieur. Or avec l'apparition et l'expansion d'internet, de nouvelles menaces ont vues le jour.

Les principales menaces qui pourraient impactées, une entreprise sont les suivantes:

- La fuite de données sensibles pour l'entreprise, sur internet;
- Les dénis de services, qui empêcheraient l'accès à internet depuis l'entreprise, et inversement;

- Modification du serveur web sans autorisation par l'entreprise. 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;

Pour lutter contre ces menaces, il faut mettre en place une passerelle d'interconnexion dites sécurisée.
Mais avant toute conception d'une architecture de passerelle sécurisée, il faut s'assurer que les postes provenant du LAN soient sécurisées, car une passerelle ne pourra jamais empêcher une attaque provenant de l'intérieur du réseau.

Voici les règles élémentaires et obligatoires pour sécuriser un poste utilisateur :

- Maintenir à jour l'intégralité des équipements du réseau;
- Ne jamais octroyer un accès de niveau administrateur sur aux utilisateurs, aux possibles seulement les privilèges et droits, qui leurs sont nécessaires;

- Désactiver les services inutiles;
- Mettre en place un pare-feu personnel, et soigneusement configuré, pour chaque machine;
- Superviser le réseau, journaliser et définir une organisation de gestion d'incidents ;
- Sensibiliser les utilisateurs aux menaces.
- Définir une politique de sécurité pour le réseau qui définisse notamment une politique en matière de gestion de supports amovibles ;

Principe généraux et démarches

Pour concevoir une passerelle d'interconnexion sécurisée, il est nécessaire de bien identifier, les fonctions de sécurité à mettre en oeuvre sur la passerelle, et leurs position dans l'architecture. Le choix des équipements de 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.

Apport pour la sécurité

L'apport pour la sécurité, correspond à la fonction principale de sécurité d'un produit, c'est à dire celle pour laquelle on met en œuvre le produit.
Prenons l'exemple d'un firewall(pare-feu), sa fonction principale est de bloquer les flux réseau non autorisés, les autres services comme la détection d'intrusion, le routage avancé ou la traduction d'adresses, sont des fonctions dites secondaires.

Robustesse

Désigne la robustesse ou la résistance d'un produit, contre les attaques. L'équipement ne doit pas affaiblir la sécurité de la passerelle d'interconnexion, à laquelle il appartient.
Par exemple certain équipement, possède des fonctions secondaires comme l'administration ou les mises à jour qui sont vulnérables et exploitables par d'éventuel attaquant.

Pour savoir si un produit est robuste, il faut se fier au CERT (Computer Response Team), plus particulièrement à la CERTA sur http://www.certa.ssi.gouv.fr . Il est très fortement recommandé, de prendre un équipement citer par la CERTA.

Maîtrise par les administrateurs et maintenabilité.

La maîtrise de la technologie de l'équipement par l'équipe d'administration, et la qualité de sa documentation son primordiale à la sécurité de la passerelle.
Un équipement à beau avoir une très haute qualité au niveau de la sécurité, si sa configuration est trop complexe pour l'équipe chargé de sa maintenance, cela pourrait provoquer de grosses failles de sécurités dans la passerelle.
Il vaut donc mieux prendre un équipement, que l'équipe chargé d'installer et maintenir maîtrise complètement, même si celui-ci est de qualité inférieur.

Il est aussi souvent recommandé,de prendre des équipements de marques différentes, pour éviter d'avoir une multiplication de la même failles sur des équipements du même constructeur. Mais cela est juste théorique, car il est impossible pour une petite, ou moyenne entreprise d'avoir les effectifs nécessaires pour leurs maintenance, cela serait beaucoup trop coûteux.
Donc, privilégié une seule marque qui est maîtrisé par vos équipe, et restera maintenable à long terme, si la solutions multimarques est impossible ou instable.

Différentes architectures

Démarche

La démarche retenue ici est de proposer différentes construction de 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 et plus coûteuse.
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.

Vocabulaire

LAN(Local Area Network**):** 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(Wide Area Network**):** 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.

FW(FireWall**):** 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 .
FW(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.

Architecture basique

Dans cette architecture, la passerelles d'interconnexions est composé d'un simple pare-feu situé entre le LAN et le WAN, et les serveurs comme les serveur web sont situé dans le LAN (figure 1).

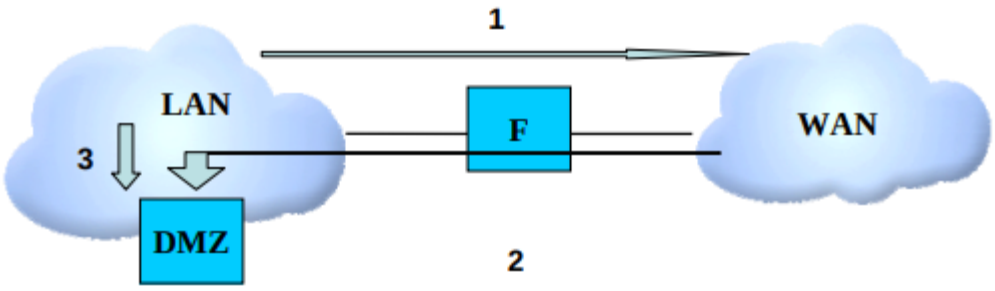


figure 1 : Architecture basique

Les flèches représentées correspondent aux flux qui traversent la passerelles, les échanges sont bidirectionnels.

C'est l'architecture la plus simple, les flux qui transitent entre le LAN et le WAN passent obligatoirement par le pare-feu, qui reconnaîtra les paquets provenant du WAN, qui n'ont pas été initié à la base par le LAN et les bloquera. C'est sa fonction principal, cela permet d'apporter une première sécurité. Mais un pare-feu peut aussi posséder plusieurs autres fonctions auxiliaire.
Cette architecture est simple et peu coûteuse, mais laisse 3 grosse failles :

- Le flux entre le WAN et le serveur WEB (la DMZ) passent par le LAN, donc un paquet à destination du serveur WEB depuis le WAN, pourraient être envoyé à une machine du LAN. Pour un attaquant il lui serait alors aisé, de lancer une attaque depuis un appareil du LAN et ainsi prendre rapidement le contrôle de la majeur partie des composants du réseau interne.

- Le pare-feu est la seul défense de la passerelle, si un attaquant arrive à le compromettre ou voir à prendre son contrôle, il pourra alors avoir accès à l'ensemble du LAN.
- Cette architecture ne propose, aucune mesure contre la défiguration du site web, les flux en provenance du WAN peuvent facilement atteindre le serveur WEB. Un attaquant peut exploiter une faille logiciel, et prendre le contrôle du serveur, et modifier le contenu du site.

Architecture << accès DMZ via le pare-feu >>

Le premier problème peut être facilement corrigé, en connectant la DMZ directement au firewall, ce qui sépare le LAN de la DMZ (figure 2).

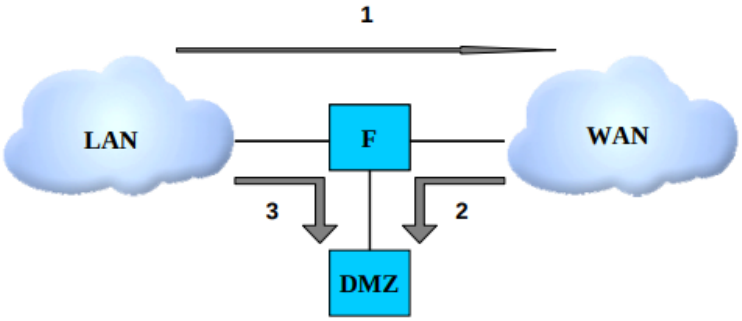


figure 2 : *Architecture « accès DMZ via le pare-feu »*

Il est important à noter que les serveurs qui seront placés dans la DMZ, sont des données accessibles par des utilisateurs du WAN, donc les données réservé uniquement aux utilisateurs du LAN, devront être stockées dans des serveurs dit interne présent dans le LAN.
Cette architecture corrige uniquement la première faille.

Architecture basée sur deux pare-feux

Pour résoudre le deuxième problème sur la compromission du pare-feu, il est possible de mettre en place une architecture multi firewall, ainsi si le premier firewall est compromis ou tombe, la passerelle pourra compter sur les autres firewall.
Nous allons ici partir sur une architecture basée sur deux pare-feux, un pare-feu intérieur entre la DMZ et le LAN, et un pare-feu extérieur entre le WAN et la DMZ (figure 3).

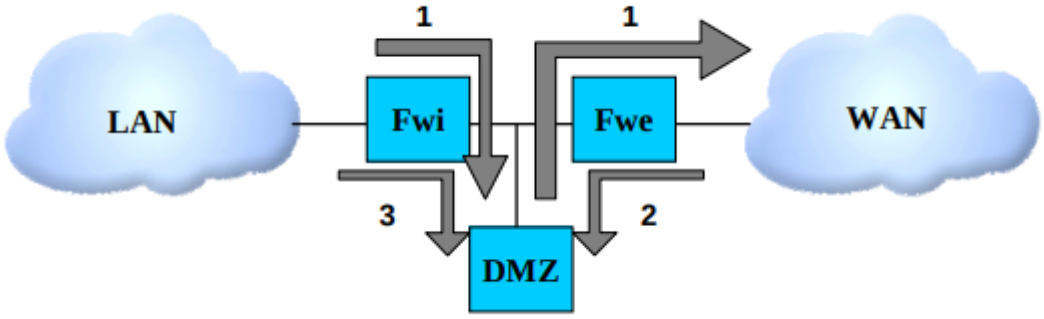


Figure 3 : Architecture basée sur deux pare-feux

Avec cette architecture, si le pare-feu externe viendrait à être compromis
le pare-feu interne continuerait à protéger le LAN, celui-ci étant plus compliqué à faire tomber.

Pour avoir une sécurité des plus efficace, il est conseillé que les pare-feux soient différents sur trois points:

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

Il est préférable que les pare-feux d'une même passerelle, soient de constructeurs différents, pour stopper ou du moins ralentir l'attaquant qui ne pourra exploiter les même failles sur les différents pare-feux. Ce choix est à utiliser si et seulement si la maintenance est possible, la mise en place de plusieurs pare-feux et de surcroît de marque différentes, exige un effectif dédié à l'administration de la passerelle conséquent, et que ce même effectif est la maîtrise des compétences nécessaires aux bon fonctionnement des pare-feux. Si la maintenance est impossible, il est préférable de choisir les même pare-feux.

Il est aussi préférable que la coupure entre les deux pare-feux ne soit pas uniquement logique mais aussi physique, cela permet d'assurer qu'aucun flux ne pourra passer entre les pare-feux, sans d'abord passer par la DMZ (figure 4)

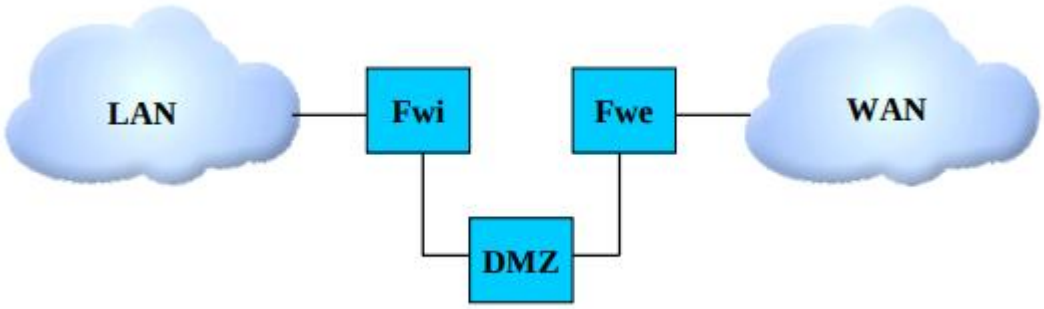


Figure 4 : Architecture basée sur deux pare-feux avec coupure physique.

Un serveur mandataire peut être installé dans la DMZ, pour appliquer un filtrage applicatif des échanges entre les machines du LAN, et les serveurs présent sur le WAN.

Architecture << en double DMZ>>

Dans cette architecture on cherche à pallier à notre dernier problème, qui est la défiguration du serveur WEB. Pour cela on ajoute une deuxième DMZ permettant de séparer les services fonctionnels,et les services de sécurités (figure 5).

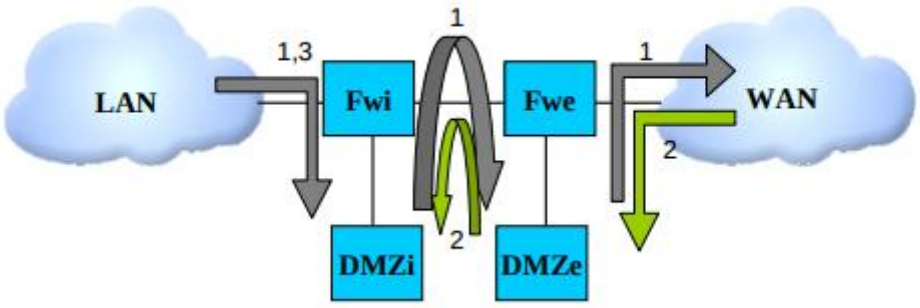


Figure 5 : Architecture « en double DMZ »

Sur la DMZe on place un reverse proxy dont le rôle sera d'assurer un filtrage des requêtes applicatives provenant de l'extérieur. La zone DMZi est la zone qui contient le vrai serveur WEB à proprement parler, avec un proxy cache qui stock temporairement les dernières pages ayant été consultées par les utilisateurs extérieur.

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.

Architecture avec 3 pare-feux

Dans l'architecture précédente les deux DMZ sont en coupure logique, il est donc sensé de les placer aussi en coupure physique. Si on effectue cette modification, il est nécessaire de mettre en place un troisième pare-feu entre les deux DMZ pour un cloisonnement physique, qu'on nommera FWm pour pare-feu médian (figure 6).

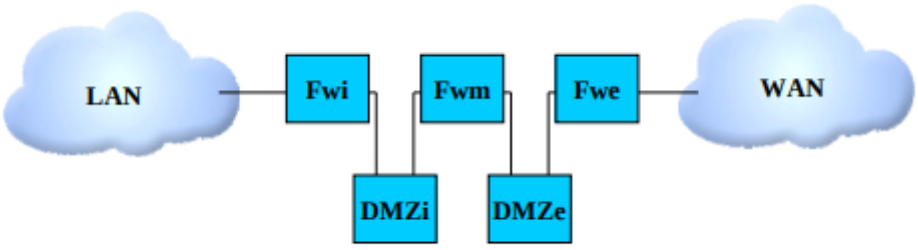


Figure 6 : Architecture avec 3 pare-feux et deux DMZ en coupure physique

Ce pare-feu médian est de permettre un cloisonnement physique entre les serveurs, en associant chaque serveur à une interface différentes du pare-feu. Cela évite de faire communiquer des services entre eux, par exemple si le reverse proxy du serveur dédié au courriel est faible au niveau de la sécurité et qu'il est compromis par un attaquant, celui-ci ne pourra pas tenter de rebondir sur ce proxy pour court-circuiter le proxy du serveur web, et ne pourra pas prendre le contrôle du serveur web.

Rappel: Cette architecture est à mettre en place, si et seulement si la maintenance est possible comme dit précédemment. Sinon il est préférable de choisir une architecture moins complexe.

Problèmes annexes

Problématique Ip:

Il est recommandé d'utiliser des adresses ip différentes, pour les flux entrant et sortant.
Une adresse fixe pour le flux entrant, et un adressage dynamique pour le flux sortant.
Cela permet d'éviter les risques en termes d'image, si un employé se rend sur un site non approprié, l'adresse ne correspondra pas à l'adresse des serveurs de l'entreprise.
Cela nécessite un opérateur principale, et un de secours, ce qui nécessitera plus de budget dédié aux réseaux.

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, regrouper plusieurs services sur une même machine physique peut être une solution en cas de manque de moyen. 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.
Il est recommandé d'utiliser cette option pour les cas suivants:

- 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 ;

Tout dépend aussi des moyens de l'entreprise, et le budget alloué pour ce domaine. Si l'entreprise ne peut se payer plusieurs services, elle devra mutualisé ses services, mais cela fragiliserait le serveur et pourrait augmenter les failles de sécuritées. Il est aussi conseillé d'avoir un serveur de secours qui prendrait le relais en cas de panne, le serveur de secours nécessitera un autre serveur physique.

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 ? Pour permettre cela, il est préférable voir obligatoire, que les postes nomades soient gérés comme les postes du LAN(pas de droit admin, etc..). De plus, il est nécessaires de rajouter des règles supplémentaires:

- Désactiver dans la mesure du possible les interfaces sans-fil, sources de nombreuses vulnérabilités ;
- Chiffrer le disque dur avec un moyen qualifié 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 faire passer les flux par une déviation, pour éviter de passer par les DMZ (figure 7).

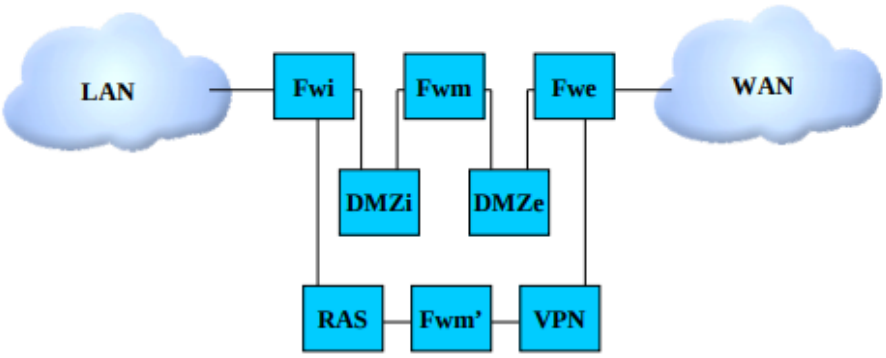


Figure 7 : Architecture avec accès pour les postes nomades

Pour sécuriser la connection il est recommandé d'utiliser un VPN pour chiffrer la connection , puis Firewall au milieu pour filtrer le flux, et un RAS (serveur d'accès distant) ftp ou http.
Idéalement, les flux internet des postes nomades passent systématiquement par la passerelle (VPN, FWm', FWi, DMZi, FWm, DMZe, FWe) pour sortir sur Internet.

Problématique de la supervision :

Chaque équipement de la passerelle doit avoir une interface dédiée à la supervision, aucun flux ne devra être routé sur ses interfaces. La machine en charge de la supervision sera, si possible protégée par un pare-feu pour limiter les risques de rebond entre les éléments de la passerelle.
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.

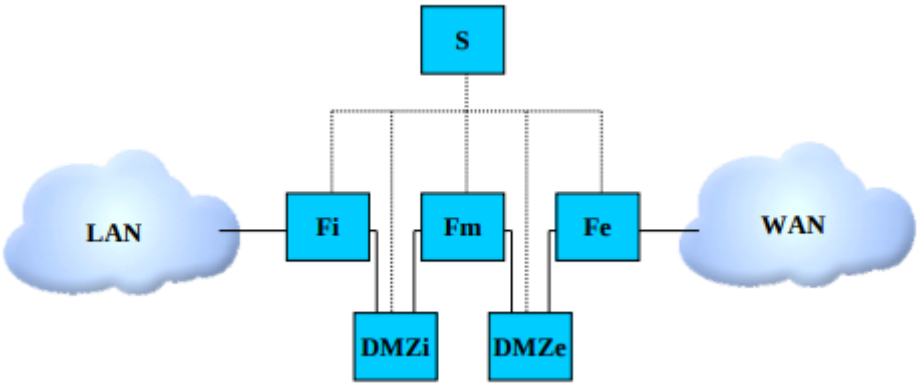


Figure 8 : Supervision de la passerelle d'interconnexion

Question des interfaces réseaux :

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.

Résumé et Conclusion

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.

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...).