Référence du document KMN 00002 – A

Référence client : AXMRSLU-UNIV2

CAHIER DE SPECIFICATIONS RESEAU

Résumé :

Ce cahier de spécification décrit l'ensemble du réseau à déployer chez notre client Aix Marseille université

Elaboration :

IND.	DATE	Rédacteur		Vérificateur		Approbateur	
		NOM	VISA	NOM	VISA	NOM	VISA
A	30/03/2018	P.CARLES		L .GRIMAUDO		P.MOYSE	

Historique :

IND.	DATE	REDACTEUR / MODIFICATIONS (ORIGINE, OBJET ...)
A1	30/03/18	Première diffusion

Contents

No table of contents entries found.

1. IDENTIFICATION DES BESOINS

Ce cahier de spécification ne prendra en compte uniquement l'aspect réseau.

Dans le cadre de ce projet, il nous a été donné le cahier des charges suivant :

1.1. CACHIER DES CHARGES

- L'architecture doit pouvoir supporter plus de 400 personnes en simultanée.
- La solution réseau doit comprendre une interconnexion avec trois sites distants.
- Cette solution doit avoir des politiques de sécurité personnalisées en fonction des besoins.
- L'architecture réseau est établie pour assurer :

    - Une conception hiérarchique : accès – distribution – coeur de réseau.
    - Un cloisonnement des services en différents vlans.
    - Du routage optimisé.
    - Support de VPN site-à-site.
    - Redondance de passerelle.
    - Routage externe.
    - Routage interne.
    - Architecture dual-stack.
    - Intégration de téléphonie IP.
    - Service d'alarme connectée.
    - Service de vidéosurveillance.
    - Implémentation de solution wireless.
    - Installation de baie de brassage – type DataCenter.
    - Supervision de réseau.

1.2. REFERENCES

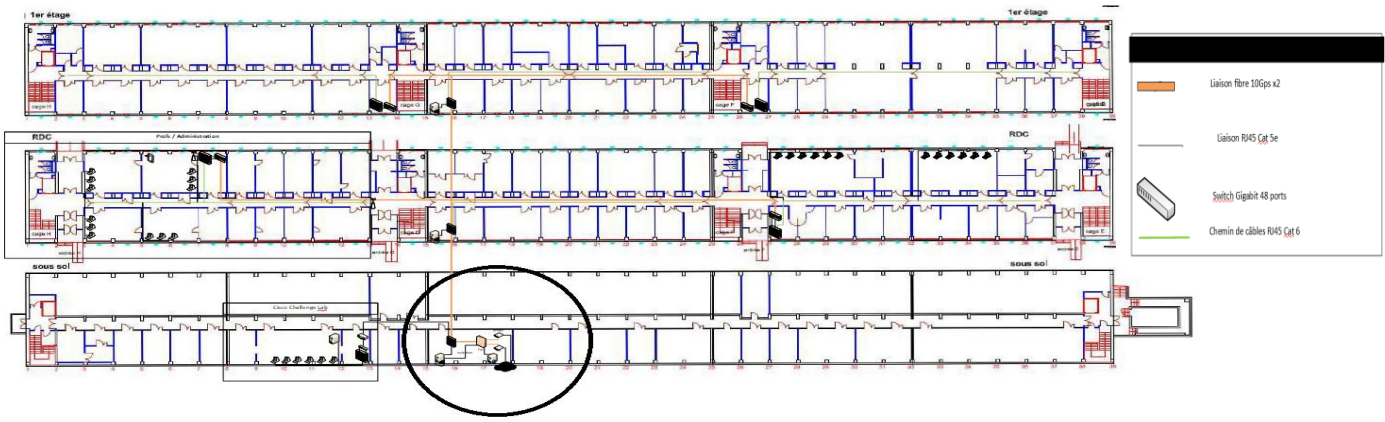
ID	Document	Référence	Indice
2	Cahier de spécification système	KMN 00002-SpecRes	B

2. SERVICES

2.1. Conception du Datacenter

Plusieurs points cruciaux sont à prendre en compte pour la mise en place de la salle qui accueillera le data-center.

Premièrement, elle doit être non-inondable, il est impensable que de l'eau puisse s'introduire dans une baie de brassage, d'autant plus qu'elle est placée au sous-sol comme le montre ce schéma :



Emplacement de la baie de brassage

Les équipements réseaux seront disposés dans une baie de brassage 19 pouces 26 U.

La salle se devra donc d'être totalement imperméable et l'accès y sera réglementé grâce à une solution de porte blindée de la compagnie Locken.

2.1.1. Portes blindées

Les solutions de contrôle d'accès smartphones & badges de LOCKEN s'utilisent de façon autonome ou en extension de solution de contrôle d'accès déjà existantes. Elles sont disponibles sous 3 formes : cylindres électronique boutons, plaques béquilles électroniques et lecteurs de badge. Chacune communique de façon chiffrée en RFID ou en Bluetooth. Elle est pilotée par le logiciel *Locken Smart Access*, sécurisé et ergonomique qui permet de configurer les accès sur mesure.

Vous trouverez toutes les informations nécessaires dans l'annexe dédiée à cette solution.

2.1.2. Alimentations électriques et risques

Premièrement nous avons tourné nos choix vers des équipements disposant d'alimentations électriques redondées afin de permettre une disponibilité décuplée.

L'électricité statique (dangereuse pour les équipements) sera gérée par le mise à la terre des masses.

Un groupe électrogène sera installé pour assurer la continuité de service si défaillance d'EDF et ainsi accentuer le côté disponible de l'infrastructure.

Par ailleurs, des parafoudres seront installés pour protéger l'installation électrique d'une surtension.

L'entièreté des équipements seront alimentés sur trois onduleurs Infosec.

Ils disposeront chacun d'une puissance de 2700watts , 30 minutes d'autonomie et seront bien sûr, rackables dans la baie de brassage.

2.1.3. Climatisation et refroidissement

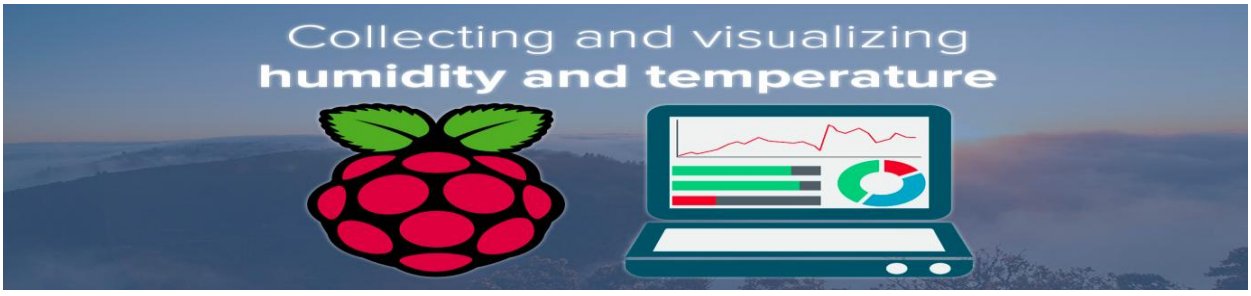
Les équipements produiront une chaleur importante et devront et la température de la salle devra être régulée pour ne pas laisser de périphérique surchauffer (18°C-20°C).

Une surchauffe pourrait causer des dégâts irréversibles sur l'appareil et même être l'origine d'un incendie.

L'air froid sera généré par deux climatiseurs Einhell MK 2600 E :

-Puissance de refroidissement de 2600W
-Classe d'efficacité énergétique : A
-65 dB sonore en marche (68 dB si les deux sont allumés en même temps).
-Capable de réguler la température ambiante à 18°C.
-Le deuxième climatiseur bien qu'optionnel, est vivement recommandé pour introduire de la redondance et réduire considérablement le risque de surchauffe.

Enfin, un raspberry sera installé dans la salle et disposera d'une sonde de température et d'hygrométrie. Il sera paramétré de sorte à indiquer par mail à l'administrateur réseau d'une éventuelle anomalie de montée de chaleur, d'une salle trop humide ou sèche par exemple.



Voici le lien vers le projet (en allemand) :
https://ikhaya.ubuntuusers.de/2015/02/12/projektvorstellung-raspi-sht21/

2.1.4. Gestion des incendies

Un incendie dans le bâtiment pourrait avoir des conséquences dramatiques sur l'installation réseau et électrique. Il est ceci dit, impensable de protéger le data center avec des extincteurs, qui pourraient causer des dommages importants sur l'électronique des machines.

Nous opterons plutôt pour une solution anti-incendie LES-Rack :

Un boîtier relié aux détecteurs de fumées capable d'inonder la salle de gaz d'Hexafluoropropane qui empêche la propagation de l'incendie en supprimant l'oxygène de la salle.

Ce dispositif respecte entièrement les règles & normes européennes de solution anti-incendie.

Il n'occupera que 3 unités de hauteur dans la baie de brassage et il dispose d'une batterie pour fonctionner même en cas de coupure d'électricité.

2.1.5. Vidéosurveillance et alarmes :

Afin de se protéger des intrusions dans la baie de brassage, il est indispensable d'instaurer un système de vidéoprotection qui sera non seulement capable de récolter des preuves d'infraction mais aussi de déclencher des alarmes pour dissuader les malfaiteurs.

Un vlan sera consacré à la vidéosurveillance et aux alarmes qui fonctionneront sur le réseau TCP/IP.

Pour simplifier le câblage, tous ces équipements seront alimentés en Power over Ethernet.

Les descriptifs détaillés des équipements sont disponibles dans les annexes dédiées.

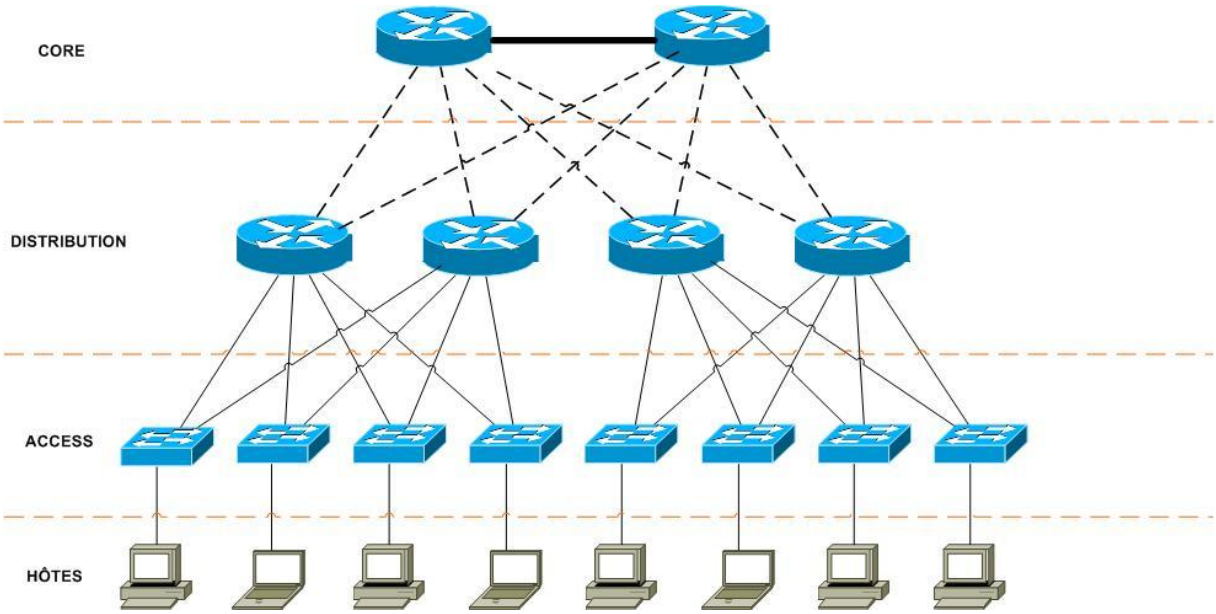
2.2. Conception hiérarchique et câblage

L'installation d'un réseau optimisé nécessite d'être construit sur un plan hiérarchique en 3 couches :

-La couche d'accès, permettant aux hôtes et terminaux de se connecter sur le réseau.

-La couche de distribution, permettant de joindre l'accès au coeur, de regrouper les domaines de diffusions et d'assurer une grande disponibilité grâce à la redondance.

-La couche cœur de réseau, permettant d'assurer la connexion haut débit du réseau fédérateur.



Pour la couche d'accès nous utiliserons les Cisco Catalyst 2960-X Series Switches :
Ce type de switch a été choisi pour les raisons suivantes :

-48 ports GigabitEthernet
-PoE supporté 740W (nécessaire pour l'alimentation des AP et caméras).
-Stackables.
-SPAN.
-Authentification 802.1x
-Power Supply redondé.
-QoS

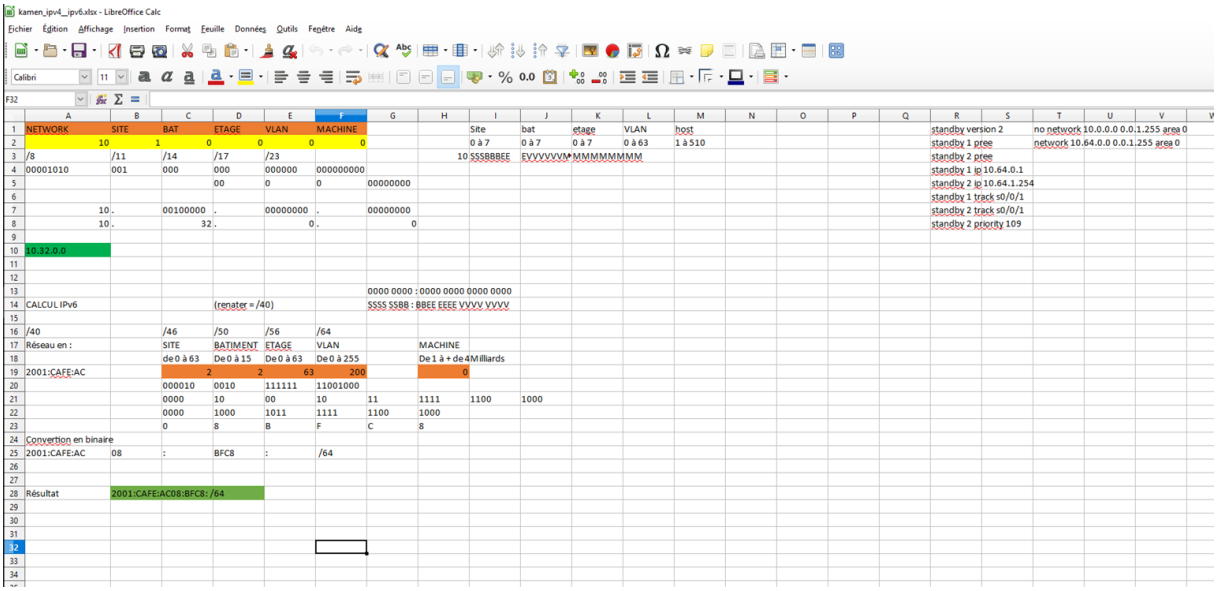
Pour les couches de distribution et de coeur nous utiliserons les Cisco Catalyst 3850-48U :

-Alimentation rendondée.
-QoS
-Stackable et Rackable.
-48 ports.
-Wireless controleur Intégré.
-40G de capacité wireless.
-Supporte 100 AP et 2000 clients wireless.

2.3. Plan d'adressage Dual-Stack

Le réseau supportera aussi bien IPv4 qu'IPv6.

Vous trouverez dans le dépôt de ressources, ce calculateur de sous-réseaux dont la capture d'écran ci-dessous est extraite pour déterminer n'importe quelle adresse IP de n'importe quel hôte dans n'importe quel sous-réseau en IPv4 et IPv6 !



	A	B	C	D	E	F	G	H	I	J	K	L	M	R	S	T	U	V
1	NETWORK	SITE	BAT	ETAGE	VLAN	MACHINE			Site	bat	etage	VLAN	host	standby version 2		no network 10.0.0.0 0.0.1.255 area 0		
2		10	1	0	0	0	0		0 à 7	0 à 7	0 à 7	0 à 63	1 à 510	standby 1 pree		network 10.64.0.0 0.0.1.255 area 0		
3	/8	/11	/14	/17	/23			10	SSSBBBEE	EVVVVVVV	MMMMMMMM			standby 2 pree				
4	00001010	001	000	000	000000	000000000								standby 1 ip 10.64.0.1				
5				00	0	0	00000000							standby 2 ip 10.64.1.254				
6														standby 1 track s0/0/1				
7		10.	00100000	.	00000000	.	00000000							standby 2 track s0/0/1				
8		10.	32.		0.		0							standby 2 priority 109				
9																		
10	10.32.0.0																	
11																		
12																		
13							0000 0000 : 0000 0000 0000 0000											
14	CALCUL IPv6			(renater = /40)			SSSS SSBB : BBEE EEEE VVVV VVVV											
15																		
16	/40		/46	/50	/56	/64												
17	Réseau en :		SITE	BATIMENT	ETAGE	VLAN		MACHINE										
18			de 0 à 63	De 0 à 15	De 0 à 63	De 0 à 255		De 1 à + de 4	Milliards									
19	2001:CAFE:AC		2	2	63	200		0										
20			000010	0010	111111	11001000												
21			0000	10	00	10	11	1111	1100	1000								
22			0000	1000	1011	1111	1100	1000										
23			0	8	B	F	C	8										
24	Convertion en binaire																	
25	2001:CAFE:AC	08	:	BFC8	:	/64												
26																		
27																		
28	Résultat	2001:CAFE:AC08:BFC8: /64																
29																		
30																		
31																		
32																		
33																		
34																		

2.4. Vlans

Le réseau sera cloisonné par un certain nombre de vlans :

1(shut)
5 etu
10 prof
15 admin
20 dsi
25 invite
30 wifietu
35 wifiprof
40 wifiadmin
42 native
45 wifiinvite
50 wifidsi
55 voip
60 ipcam
61 doorsecure
63 (défaut)poubelle

Ces vlans nous permettront dans un premier temps, de réduire les domaines de broadcast, si 400 utilisateurs doivent pouvoir être actifs en simultanée, il est nécessaire de limiter leur propagation sur l'ensemble du réseau.

2.5. Sécurité liaisons de données

Nous sommes conscients que cet établissement accueillera des étudiants en informatique, c'est pourquoi nous avons mis en place des mécanismes de protection de réseau.

Il sera plus compliqué pour d'éventuels utilisateurs mal-intentionnés de procéder à certaines attaques de couche 2, voici celles que nous sommes en mesure de parer grâce à nos configurations avancées des équipements réseaux :

Empoisonnement du cache ARP :

Falsifier les caches ARP des machines en envoyant des requêtes ARP non légitimes afin d'intercepter les paquets émis (Man-in-the-Middle) :

Nous utiliserons du Dynamic ARP Inspection (DAI) – ce protocole permet de supprimer les paquets ARP frauduleux, et de définir un seuil maximal de requêtes ARP sur un intervalle de temps donné. Si ce seuil est excédé le port sera éteint automatiquement.

Le fonctionnement du DAI est basé sur le DHCP snooping, et de la base de données qu'il crée des associations d'adresses IP / adresses MAC.
Nous définirons des ports « trusted » (typiquement les trunks, liaisons vers routeur etc) et « untrusted » (ports d'accès qui connecteront les utilisateurs).

Le protocole Dynamic Host Configuration Protocol :

Voici deux attaques sur le protocole DHCP connues et facilement exploitables que le réseau sera en mesure de parer :

- DHCP starvation (Épuisement du pool DHCP avec des requêtes non-légitimes).

- DHCP spoofing (Usurpation du serveur DHCP légitime, afin de compromettre la confidentialité/intégrité du trafic).

Nous utiliserons le dhcp snooping en réponse à cette attaque :

Seuls les ports connectés à des serveurs DHCP seront dans l'état « trusted ».
Tous les autres ports seront « untrusted ».
Le protocole dressera alors une base de données liant notamment ; l'adresse mac – l'adresse IP – le bail DHCP - numéro de vlan.

Les serveurs non-légitimes se trouveront sur des ports « untrusted » et ne pourrons donc pas répondre aux requêtes discover.

Inondation de la table Mac :

Pour se prévenir de se genre d'attaques , la méthode la plus pertinente est sans doute le port-security.

Un switch avec du port security n'apprendra que les adresses MAC spécifiées manuellement, ou dynamiquement mais avec une limite maximale à définir.

Quand un port reçoit une trame l'adresse MAC source est comparée à la base de données d'adresses MAC, et elle soit « forwardée » si elle correspond, elle est détruite si elle ne figure pas dans la base de données.

Attaques par Saut de Vlans :

Les sauts de vlans représentent une menace considérable dans un réseau cloisonné de la sorte. Cela consiste à voir le trafic des autres vlans sans l'aide de routeurs.

L'attaquant essaiera de faire passer sa liaison pour un lien trunk et pourra donc accéder aux autres vlans. Voici les mesures mises en place :

Les protocoles Cisco Discovery Protocol et Dynamic Ttrunking Protocol seront désactivés sur tous les équipements.

Le vlan natif ne sera pas laissé sur le vlan 1 , et il ne sera utilisé exclusivement par les trunks.

Les ports non-utilisés seront placés dans le vlan poubelle et seront éteints.

Usurpations d'adresses Mac & IP :

Si un attaquant connaît l'adresse MAC ou IP d'un autre hôte, il peut être tenté d'usurper son identité de couche 2 ou 3, et forcer les équipements à modifier leurs tables de routage et ainsi compromettre la sécurité du réseau.

L'IP Source Guard abrégé IPSG nous servira de solution pour valider la cohérence des 3 facteurs suivants : adresse IP – adresse Mac – Port . Il examine chaque paquet et se base sur les informations du dhcp snooping.

2.6. Téléphonie

Un besoin en téléphonie et vidéo sur IP a également été exprimé.

Pour satisfaire cette demande, nous désirons placer des téléphones IP Cisco 8845 :

Ce modèle de téléphone a en effet l'avantage d'être un visiophone avancé car il possède des fonctionnalités intéressantes à savoir :

- 5 lignes prises en charge.
- Commutateur intégré et donc possibilité de raccorder un ordinateur de bureautique.
- Messagerie vocale - ID d'appelant – Appel en instance – Renvoi automatique – Transferts Mise en attente.
- QoS.
- Compatbile Cisco Unified Communications Manager.
- Sécurité 802.1x
- Prise pour casque-micro

Ainsi, le personnel administratif et les professeurs pourront communiquer via téléphone et visioconférences d'une manière fiable et stable.

La Quality Of Service est configurée pour privilégier le trafic Voix et Vidéo en cas de congestion réseau et de saturation hardware.

L'opérateur téléphonique sera OVH, car leurs services sont d'une qualité pertinente pour un prix très compétitif.

Visiophone Cisco

2.7. Wireless

Le wi-fi est également important et nous vous proposons une solutions à base de bornes lourdes : Elles seront déployées et clientes d'un serveur RADIUS et de contrôleurs (qui seront pour le coup, les commutateurs de niveau 3 de distribution afin de réaliser des économies sur l'équipement).

Nous utiliserons une architecture centralisée Cisco Unified Wireless, un serveur WCS nous permettra de donner les configurations aux contrôleurs.

Une des bornes Cisco Meraki

2.8. Redondance et passerelle

Dans le but d'assurer une disponibilité maximale, il est crucial de redonder la passerelle par défaut et de disposer d'au moins deux accès internet.

Nous avons choisi d'utiliser le protocole Hot Standby Routing Protocol afin de créer un basculement potentiel entre les deux liaisons WAN : SFR et Renater.

2.9. Routage interne et externe

La liaison principale sera fournie par Renater.
La liaison de secours sera fournie par SFR.
Le protocole de routage interne sera OSPF, malgré que EIGRP soit compatible avec notre architecture, nous estimons qu'il est plus pertinent d'utiliser un protocole libre pour des raisons d'évolutivité.

Routeur Cisco 4413

Le protocole de routage externe sera BGP.
Une demande d'attribution d'autonomous system sera effectuée à l'IANA afin de créer les peerings chez Renater & SFR.

2.10. VPN

Le site de Luminy sera relié en VPN à Gap à l'autre agence.
La solution utilisée est du site à site GRE+IPsec.

Nous avons choisis de mettre en place du GRE+IPsec grâce à la souplesse d'un tunnel GRE : il permet d'envoyer n'importe quel trafic (multicast et broadcast particulièrement) contrairement à la grande majorité de protocoles de tunneling, cependant il n'est pas sécurisé car les informations qui y transitent sont en texte clair (non-chiffrées).

C'est pourquoi, en complément nous ajoutons une notion IPsec afin de :

-chiffrer les données en AES.
-échange de clefs par Diffie-Hellman.
-assurer l'intégrité des données par emprunte SHA2.

2.11. Firewall

Enfin, nous terminons par l'aspect « pare-feu » de l'architecture, maintenant que nous possédons une sécurité avancée dans le réseau local, nous devons également nous protéger de l'extérieur du réseau.

Nous utiliserons un Cisco ASA 5545-X Firewall Edition Il assurera les connexions VPNs aux sites distants, et il nous permettra de filtrer le contenu malveillant provenenant de l'extérieur du réseau.

Nous pourrons donc utiliser le protocole propriétaire GRE qui facilitera grandement le déploiement des VPN. Ce type de firewall fait partie du très haut de gamme, et il nous permettra d'améliorer drastiquement la sécurité de notre réseau.