DOSSIER D'ARCHITECTURE TECHNIQUE

Dossier d'Architecture Technique : « Architecture Microsoft Exchange Server 2013 Sécurisée »	**Référence** : DAT0120_Exchange **Nom du fichier** : DAT0120_Exchange.pdf **Date de création :** 10/01/2020 **Version :** Finale. **Dernière mise à jour :** 04/02/2020 **Statut :** Vérifié.
Objet : Dossier d'architecture technique de l'application **« Architecture Microsoft Exchange Server 2013 Sécurisée »**	

Synthèse / Mots clés : Architecture, Technique, Microsoft, Exchange, 2013, UTM9, PfSense, OWA, POP3S, SMTPS, ActiveSync, Outlook, AnyWhere, Gmail, Internet, Explorer, MBX, CAS, AD, HTTPS, HTTP, RPC.

Rédacteur(s)	Vérifié par	Approuvé par
+HADJ-ALI Nassim ; +CHEMLOUL Nassim.	+HARHIRA Hamed Bilel.	+M. ROZENBERG Marc Le : 07/02/2020.

Destinataires pour action	Destinataires pour information
+ Techniciens.	+ Direction.

Historique du document			
Date	**Version**	**Auteurs**	**Motifs**
31/01/2020	Brouillon	+ HADJ ALI Nassim ; + CHEMLOUL Nassim.	A soumettre pour vérification.
04/02/2020	Finale	+ HADJ ALI Nassim ; + CHEMLOUL Nassim.	Pour donner suite à la vérification.

Dossier d'Architecture Technique
« Architecture Microsoft Exchange Server 2013 Sécurisée »

Contact Maîtrise d'Ouvrage :

marc.rozenberg@univ-evry.fr

Contact Maîtrise d'Œuvre :

n.chemloul@outlook.fr
hadjali.nassim@gmail.com
bilelharhira@gmail.com

Architectes :

+ CHEMLOUL Nassim ;
+ HADJ-ALI Nassim ;
+ HARHIRA Hamed Bilel.

DOCUMENTS DE REFERENCE :

Référence	Date	Version	Description
DATTYPE	30/12 /2019	1.0	DAT Type fourni par M. ROZENBERG

Table des matières

Liste des Figures :

Liste des Tableaux :

1. Présentation Générale :

Ce document constitue le dossier d'architecture technique (DAT) de la mise en place d'une solution sécurisée de messagerie électronique fondée sur le serveur Exchange 2013 de Microsoft & son déploiement dans le cadre d'un projet académique.

Ce projet consiste à mettre en place une maquette constituée du firewall UTM9 de Sophos, d'un serveur Microsoft Exchange 2013 pour la messagerie électronique, d'un Active Directory (AD) posé sur un hôte Windows Serveur 2012 ainsi qu'un pare-feu PFSense pour le filtrage des requêtes provenant de clients externes.

1.1. Objet de l'Étude :

L'objectif principal de ce projet est de tester l'accès de manière sécurisée des différents clients de messagerie (OWA, POP3, Outlook AnyWhere, MS ActiveSync) hébergés intra-réseau (LAN) & extra-réseau (WAN), à un serveur MS Exchange 2013 sécurisé en profondeur par deux pare-feu, PFSense & UTM9, en l'occurrence.

1.2. Contexte du projet :

Le projet consistant en la mise en place de la maquette décrite plus haut, ainsi que l'ensemble des tests du bon fonctionnement des différents clients de messagerie, entre dans le cadre d'un projet pédagogique durant notre cursus en M2 ASR.

1.3. Présentation Fonctionnelle :

L'architecture fourni les besoins fonctionnels suivants :

- Un hôte interne[1] porte deux types de clients de messagerie, lesquels sont OWA & Outlook AnyWhere, pouvant se connecter au serveur Exchange 2013 à mettre en place ;
- Un hôte externe[2] porte deux types de clients de messagerie, lesquels sont OWA & POP3, pouvant se connecter au serveur Exchange 2013 ;
- Un smartphone externe[3] porte un type de client de messagerie, lequel est MS ActiveSync, pouvant se connecter au serveur Exchange 2013 ;
- Les requêtes des clients hébergées sur hôtes externes doivent être adressée à l'interface WAN du PFSense sur le port 4443 TCP, ce dernier est aussi responsable du filtrage des requêtes provenant des clients externes ;
- Un UTM9 de Sophos pour le cloisonnement des réseaux, ainsi que l'activation dessus d'un comportement Man In The Middle vis-à-vis des requêtes provenant des clients externes ;
- Un Active Directory sur lequel est activé les Rôles ADDS (Annuaire des utilisateurs & des machines du domaine local ainsi que Serveur DNS) & ADCS (Autorité de certification, dont la tâche est la signature des certificats serveurs) ;
- Les 2 rôles (CAS[4] & MBX[5]) du serveur MS Exchange 2013 sont répartis sur 2 hôtes distincts (➔ 2 VLAN Distincts).

[1] Machine connectée au réseau LAN.
[2] Machine connectée au réseau WAN.
[3] Smartphone connectée au réseau WAN.
[4] Client Access Server : le destinataire des requêtes des clients.
[5] Mail Box : Serveur des boites aux lettres.

2. Exigences :

L'architecture répond à différent exigences, nous citons ci-dessous les exigences fonctionnelles, de sécurité et de disponibilité.

2.1. Exigences d'Utilisation :

La description d'exigences d'utilisation des composants de notre architecture est montrée sur les 2 tableaux suivant, en commençant par les serveurs :

Serveurs :

Fonctionnalités des composants	Sync / Async	Description
MBX Exchange	Synchrone	+ Sauvegarde des boites aux lettres des utilisateurs.
CAS Exchange	Synchrone	+ Fait front aux requêtes des clients ; + Unique interlocuteur du MBX.
Active Directory	Synchrone	+ Contrôleur de domaine (dont authentifications des utilisateurs) ; + Serveur DNS ; + Autorité de certification de confiance des hôtes de l'infrastructure.
UTM9	Synchrone	+ Pare-feu pour le cloisonnement des réseaux (VLANs) ; + Sécurisation des sous réseaux du LAN ; + Reverse Proxy : Analyse anti-virus & malwares des requêtes adressées aux serveurs CAS & AD.
PFSense	Synchrone	+ Pare-feu pour le filtrage des requêtes externes ; + Redirection de ports (Port Forwarding) ; + NAT.

Tableau 1 : Description des exigences d'utilisation des serveurs de l'architecture.

Interfaces Clients :

Rôles utilisateurs (Ou applications clientes)	Description	Localisation/nombre
OWA (Navigateur web : Internet Explorer)	+ Connexion HTTPS (TCP 4443 WAN PFSense -> TCP 443 WAN UTM9) ; + Reverse Proxy UTM9 : connexion sur le port TCP 443 du serveur CAS.	Hôtes externes
POP3S (Outlook 2016)	+ Connexion Sécurisé sur le port TCP 995 du serveur CAS pour récupération des boites aux lettres ; + Connexion Sécurisé sur le port TCP 587 (SMTP Sécure, dit SUBMISSION) pour l'envoi des messages électroniques aux serveur CAS, qui les forwardent ensuite aux MBXs.	Hôtes externes
MS ActiveSync (Gmail)	+ ⇔ à OWA des Hôtes externes.	Smartphones externes
OWA (Navigateur web : Internet Explorer)	+ Connexion HTTPS sur le serveur CAS ; + Pas d'utilisation du reverse proxy de l'UTM9.	Hôtes internes
Outlook AnyWhere (Outlook 2016)	+ RPC over http.	Hôtes internes

Tableau 2 : Exigences interface client.

2.2. Exigences de fiabilité de service :

Les exigences de fiabilité de service de notre infrastructure sont présentées dans le tableau suivant :

Critères liés aux niveaux de service		
Ouverture de service		24H /24, 7J/7.
Taux de disponibilité global de l'application		95 % annuel, hors arrêt programmé.
Nombre d'arrêts de service tolérés		Fréquence des arrêts de services non planifiés : 2 fois /année Arrêts de service planifiés : 1fois /mois, pour mise à jour des patchs de sécurité.
Fenêtre d'exploitation demandée		Profil d'exploitation : quotidien.
Incident Mineur	**+RTO (Recovery Time Objective sur incident)**	+Durée d'interruption max. admissible : 15 minutes.
	+Type de bascule	+Type de bascule : Manuelle.
	+Ex: **Utilisateur n'ayant plus accès à sa boite aux lettres.**	+ Ex : 1) Réinstallation du client de messagerie sur l'hôte de l'utilisateur ; 2) Configuration du client de messagerie.
	+Fonctionnement en mode dégradé.	Fonctionnement en mode dégradé : Messagerie Sécurisé What's App.

	RPO (Recovery Point Objective)	Perte admissible : 15 mins de données.
Sinistre	**+RTO (Recovery Time Objective)**	+Durée d'interruption max admissible : 2H
	+Plan de reprise	+Plan de reprise : Référence du plan de reprise d'activité
	+ Fonctionnement en mode dégradé.	+Fonctionnement en mode dégradé : Messagerie Sécurisée What's App.
	RPO (Recovery Point Objective)	Perte admissible : 2H de données
Demandes exceptionnelles		Arrêts de la machine pour maintenance : 1fois/Trimestre.

Tableau 3 : Exigences de fiabilité.

2.3. Exigences de Conservation des Données :

Les données des utilisateurs (les informations relatives à leurs comptes dont celle à caractère personnel, leurs boites aux lettres) sont conservées pour une longue durée dans nos serveurs.

Toutes les données relatives aux information personnelles des utilisateurs sont enregistrées avec leur accord, en respectant la législation en vigueur depuis mai 2018 dans l'espace Shengen, la loi RGPD en l'occurrence. Les données sont supprimées une année après demande de clôture du compte par son propriétaire.

Ces données sont utilisées dans le cadre des besoins spécifiques de l'entreprise tels que les contrôle d'audit ou éventuellement dans le cadre d'une enquête judiciaire ordonnée par les autorités compétentes.

Les informations sur les comptes des utilisateurs sont sauvegardées dans l'Active Directory, tandis que leurs boites aux lettres le sont sur l'hôte du rôle MBX du serveur Exchange.

2.3.1. Plan de Restauration :

Notre infrastructure supporte 2 types de données critiques, dont la perte entrainerait un impact d'ordre vitale pour la survie de l'entreprise.

Ces 2 types de données sont :

1- Données relatives aux comptes des utilisateurs : Nous projetons une évolution de l'infrastructure afin de palier au scénario de pertes de ces données-ci, cette évolution consiste à répliquer les données de l'Active Directory « Principale » sur un second Active Directory, d'un site distant de préférence ;

2- Boites aux lettres des utilisateurs : Nous projetons une évolution de l'infrastructure afin de palier au scénario de pertes de ces dites boites aux lettres, en mettant en place un DAG MBX de type RAID 1 Mirroring, toujours dans un site distant de préférence.

3. Architecture technique :

3.1. Schéma d'architecture générale :

Le figure 1 montre l'architecture technique de l'infrastructure :

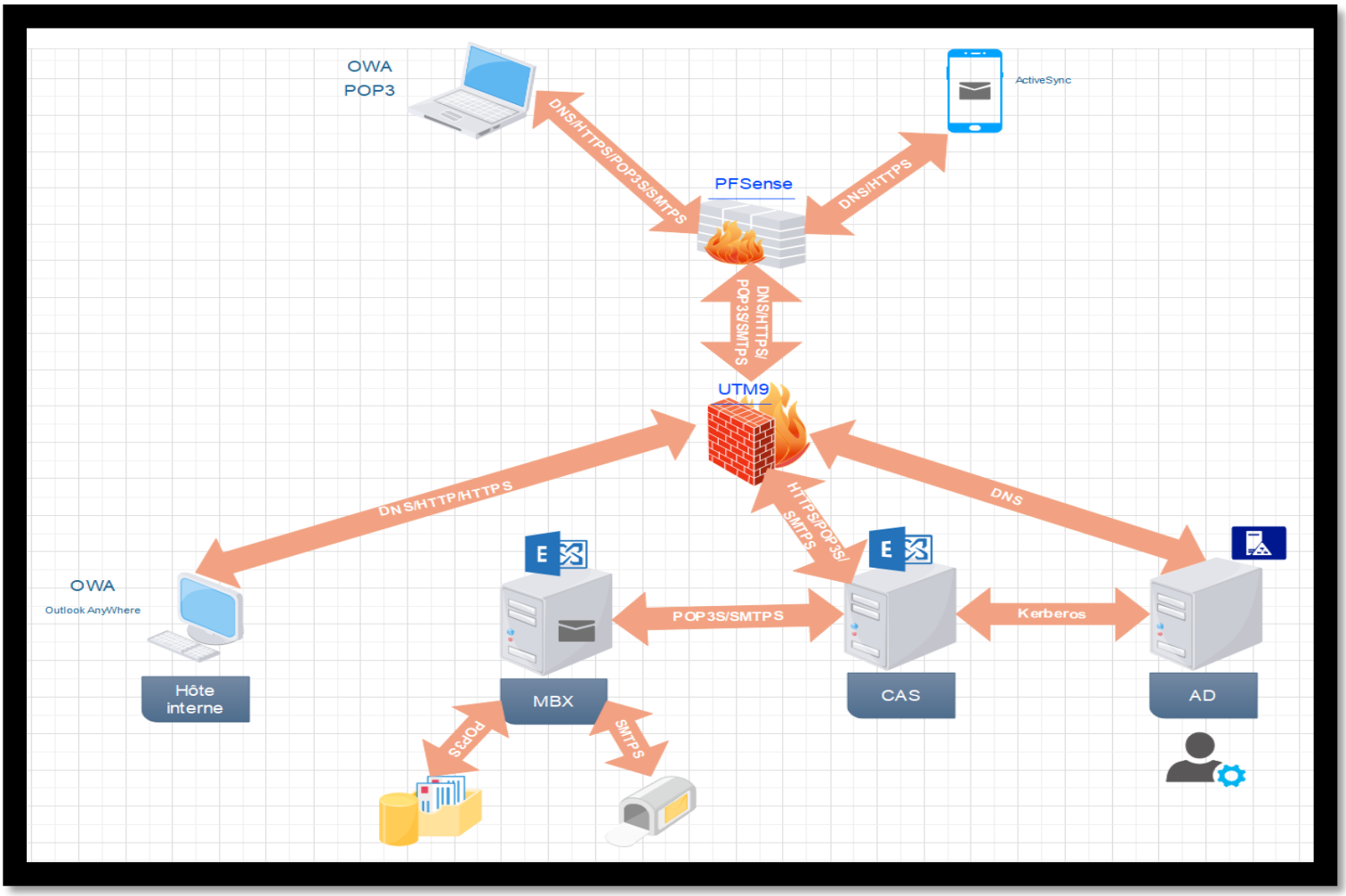

Figure 1 : Architecture Technique.

HardWare :

Notre maquette est composée de :

- Un hôte externe ;
- Un Smartphone externe ;
- Deux pares-feux :
  - PfSense : Pare-feu externe ;
  - UTM9 : Pare-feu interne ;
- Un Active Directory qui fait office d'annuaire, de serveur DNS & d'autorité de certification ;
- Un hôte qui porte le rôle CAS du serveur Exchange (faisant front aux requêtes des clients) ;
- Un hôte qui porte le rôle MBX du serveur Exchange (Contient les boites aux lettres des utilisateurs) ;
- Un hôte interne.

SoftWare Client :

L'utilisateur a la possibilité de consulter sa boîte email ou d'envoyer des emails en utilisant un des clients suivants :

- **OWA (Outlook Web App) :** (Client HTTPS) depuis les hôtes externes & internes, en utilisant un navigateur web tel que Internet Explorer ;
- **Outlook AnyWhere** : (Client http over RPC) depuis un hôte interne, en utilisant un client de messagerie, tel que Outlook 2016 ;
- **POP 3S** : (Client POP3S « Pour la récupération des boites emails depuis le serveur » & SMTPS « pour l'envoi des emails vers le serveur ») depuis un hôte externe, en utilisant un client de messagerie, tel que Outlook 2016 ;

- **ActiveSync** : (Client HTTPS) depuis un smartphone externe en utilisant un client de messagerie tel que Gmail (Application disponible sur tous les SmartPhones dont l'OS est Android).

SoftWare Pares-feux :

PfSense :

PfSense est un routeur/pare-feu open source basée sur le système d'exploitation FreeBSD. À l'origine, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs propriétaires. PfSense convient pour la sécurisation d'un réseau domestique ou de petite entreprise [1].

Dans notre infrastructure, les clients externes doivent d'abord passer par le pare-feu PfSense qui se charge du filtrage des requêtes provenant d'internet & fait également de la redirection de port vers les serveurs désignés par ces dites requêtes.

UTM9 :

C'est la première solution « **Unified Threat Management** » spécialement élaborée pour assurer une sécurité complète à partir d'un matériel ou d'un boîtier virtuel unique.

C'est un pare-feu réseau qui possède de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pares-feux traditionnels.

Parmi les fonctionnalités présentes dans l'UTM9, outre le pare-feu traditionnel, on cite généralement le filtrage anti-spam, un logiciel antivirus, un système de détection ou de prévention d'intrusion (IDS ou IPS), et un filtrage de contenu applicatif (filtrage URL) [2].

Dans notre infrastructure, ce pare-feu ne laisse passer que le trafic autorisé, agit comme un MIM[6] entre les clients externes & le serveur CAS, ce qui lui permet d'analyser le trafic pour s'assurer qu'il ne présente pas un risque pour l'intégrité du serveur.

SoftWare Serveur :

Afin que l'utilisateur puisse accéder à sa boite email, il connecte son client au serveur CAS, ce dernier contacte l'AD pour authentifier l'utilisateur. Une fois que le CAS ait authentifier l'utilisateur auprès de l'AD, il contacte le MBX pour récupérer la boite email de l'utilisateur, puis la transmet à son client.

Nous ajoutons à cela que l'hôte AD offre également un service de résolution de nom de domaine (contrôleur du domaine « ue19.lan ») ainsi que la signature des certificats du serveur CAS (celui hébergé sur l'hôte CAS & ceux présent sur l'UTM9[7]).

[6] Les clients externes se connectent d'abord au serveur web virtuelle abrité par l'UTM, puis ce dernier déchiffre leurs requêtes pour analyse (cela étant possible du fait que le chiffrement en amont des requêtes est réalisé avec la clé publique contenu dans le certificat que l'UTM présente, et dont il possède la clé privée). Si ces requêtes ne présentent pas de risque pour l'intégrité du serveur CAS, l'UTM génère de nouvelles requêtes à adresser au CAS.
[7] Un de nom « mail.ue19.lan » & un autre de nom « activesync.ue19.lan ».

3.2. Composants Matériels :

Le tableau 4 décrit les caractéristiques matérielles des hôtes de la maquette :

NOM de l'hôte	CPU	RAM	Espace Disque
Client Externe	2 Cœurs à 2.5 GHz	2 GO	40 GO
Smartphone Ext	2 Cœurs à 2.5 GHz	2 GO	20 GO
PfSense	2 Cœurs à 2.5 GHz	2 GO	20 GO
UTM9	2 Cœurs à 2.5 GHz	2 GO	40 GO
CAS	2 Cœurs à 2.5 GHz	2 GO	60 GO
AD & DNS	2 Cœurs à 2.5 GHz	2 GO	60 GO
MBX	2 Cœurs à 2.5 GHz	2 GO	60 GO
Client Interne	2 Cœurs à 2.5 GHz	2 GO	40 GO

Tableau 4 : Caractéristiques matériels des hôtes de la maquette.

3.3. Produits logiciels

Le tableau 5 décrit les caractéristiques logicielles des hôtes de la maquette :

Nom de l'hôte	Système d'exploitation	Logiciels
Client Externe	Windows 10 Pro	+ Outlook 2016 (accès POP3); + Internet Explorer (accès OWA).
Smartphone Ext	Android	Gmail (accès MS ActiveSync)
PFSense	FreeBSD	Dédié
UTM9	OS Sophos	Dédié
CAS	Windows Server 2012 R	Rôle CAS du Serveur Exchange 2013.
AD & DNS	Windows Server 2012 R	Rôle ADDS (Service d'annuaire & serveur DNS) ; Rôle ADCS (Autorité de certification).
MBX	Windows Server 2012 R	Rôle MBX du Serveur Exchange 2013.
Client Interne	Windows 10 Pro	+ Outlook 2016 (accès Outlook Anywhere); + Internet Explorer (accès OWA).

Tableau 5 : Caractéristiques logicielles des hôtes de la maquette.

3.4. Gestion des Changements :

Dans le cadre de notre projet, le passage à de nouvelles versions n'a pas été pris en compte. Pour d'éventuels changements dans le futur, il est nécessaire de mener une nouvelle étude et de voir ce que proposent les concepteurs des outils logiciels utilisés. Nous devons également tenir compte des risques d'un tel changement en termes de fonctionnement des services.

Pour cela il faut avoir un PCA et PRA pour garantir le SLA. Ci-dessous les deux cas de figure :

- **CAS 1 :** Passage à une nouvelle version matérielle et logicielles en même temps :
  - On garde l'ancienne infrastructure ;
  - Préparer des nouvelles machines et installer de nouvelle version dessus ;
  - Copier les données de l'ancienne infrastructure vers la nouvelle ;
  - Mettre en production la nouvelle infrastructure en parallèle avec l'ancienne ;
  - Faire une redirection DNS de l'URL de l'ancienne infrastructure vers la nouvelle,
  - Supprimer l'ancienne infrastructure et garder la nouvelle.
- **CAS 2 :** Mis à jour de l'infrastructure logicielle :
  - Installer la nouvelle version sur la préproduction ;
  - Vérifié son bon fonctionnement ;
  - Faire une redirection DNS de la production vers la préproduction ;
  - Installer la nouvelle version sur l'infrastructure de production ;
  - Supprimer la redirection DNS pour revenir sur la production.

4. Architecture réseau :

Le schéma suivant montre l'architecture réseau de notre infrastructure :

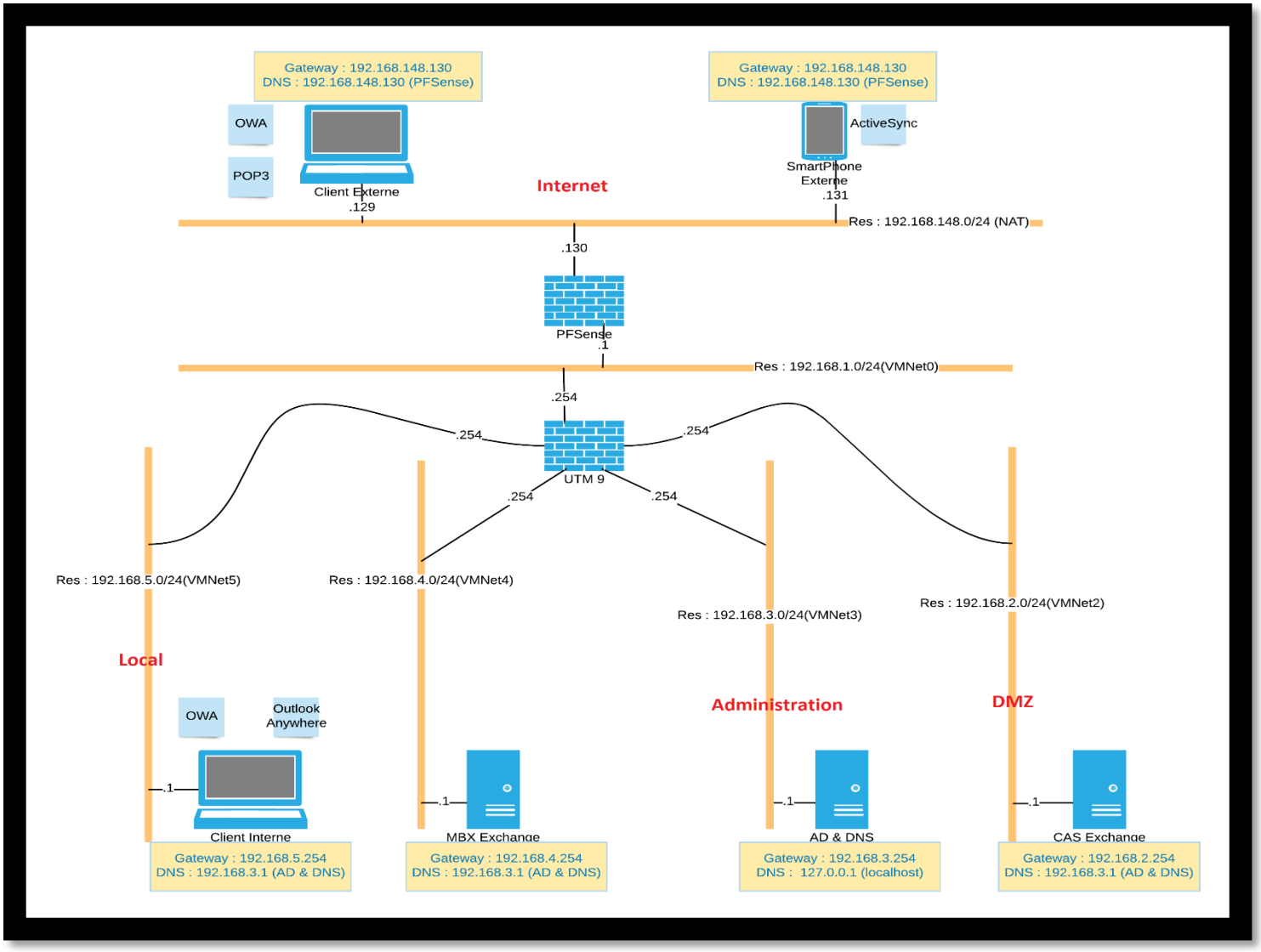

Figure 2 : Schéma d'architecture réseau de l'infrastructure.

4.1. Description :

Les hôtes externes (ClientExt & Smartphone) ont chacun une patte sur le VMNet NAT simulant un réseau internet.

Les deux pares-feux constituent le cœur de l'infrastructure. Ils protègent les quatre sous réseaux : DMZ, admin, S/Réseau du MBX & local.

Le premier pare-feu (PFSense) délimite le réseau de l'infrastructure du réseau extérieur (Considéré internet), il permet aussi de filtrer les requêtes des clients externes, en ne laissant le traverser que les requêtes DNS, HTTPS, POP3S & SMTPS. Nous ajoutons à ses fonctions celles du PAT (Port Forwarding) & du NAT (Network Address Translation).

Le second pare-feu (UTM9) assure le cloisonnement des différents VLANs de l'infrastructure, ainsi que le filtrage des flux inter VLANs échangés entre les hôtes internes[8]. Nous avons également enclenché sur cet UTM la fonction de reverse proxy, lui permettant d'agir comme un MIM entre les hôtes externes & le serveur CAS. L'objectif est que les requêtes des hôtes externes soient déchiffrées par l'UTM pour les analyser (analyse anti-virus) avant qu'elles n'atteignent le serveur CAS.

Nous avons quatre sous réseaux internes :

- DMZ ⇔ VMNet 2 ⇔ (192.168.2.0/24) : qui porte l'Hôte « CAS » ;
- Admin ⇔ VMNet 3 ⇔ (192.168.3.0/24) : qui porte l'Hôte « AD & DNS » ;
- VMNet 4 ⇔ (192.168.4.0/24) : qui porte l'Hôte « MBX » ;

[8] Le filtrage des échanges entres tous les hôtes internes (Clients & Serveurs) est la raison pour laquelle, nous avons positionné un hôte par VLAN.

- Local ⇔ VMNet 5 ⇔ (192.168.5.0/24) : qui porte les Hôtes « Client Interne », correspondant aux machines des utilisateurs.

Notre maquette illustrant l'infrastructure désiré a été réalisée sous VMware. Ainsi, le câblage & le Switching sont gérés par l'hyperviseur VMware Workstation.

4.2. Interfaces :

La figure 3 liste les différents flux échangés entres les machines de l'infrastructure & transitant par-delà via le pare-feu UTM9 :

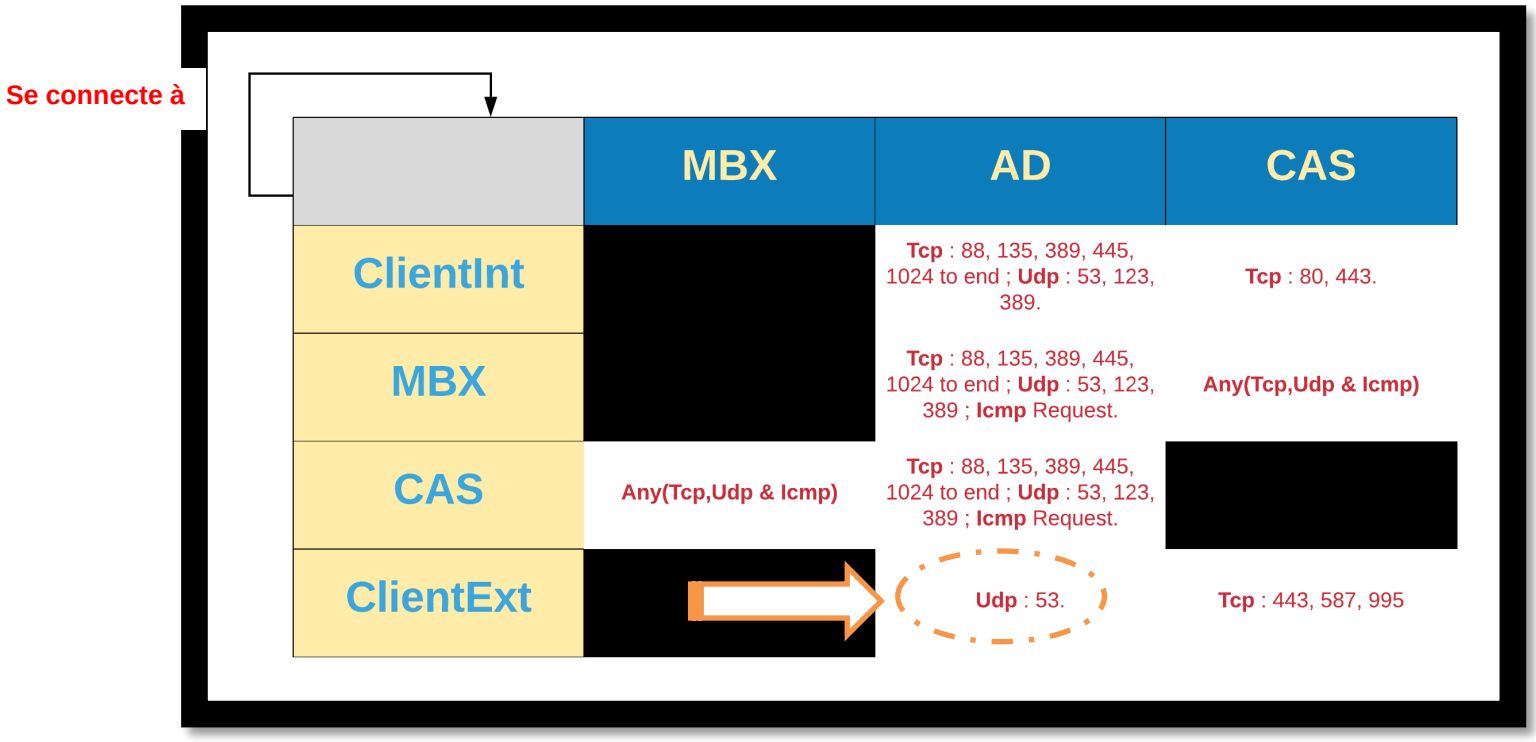

Figure 3 : Les flux échangés entre les machines de l'infrastructure.

On peut lire sur la figure 3, la case sélectionnée par une ellipse à contours discontinus de couleur orange, qu'un hôte externe a l'autorisation de se connecter sur le port UDP 53 (Protocole DNS) au serveur DNS à l'écoute sur l'hôte AD.

Pour ce faire, il a fallu insérer 2 règles firewall, une entrée de ports Forwarding ainsi qu'une entrée à la table de routage statique à PfSense lesquelles sont listées ci-dessous :

- Une règle firewall sur l'UTM9 :
  ***FROM** (any IPv4 @) & (any UDP Port) « Received On Wan if » **TO** (@AD) & (UDP Port 53) : PASS.*
- Une règle firewall sur PFSense :
  Similaire à la précédente.
- Une entrée de Port Forwarding sur PfSense :
  WAN UDP Port 53 → @AD UDP Port 53.
- Une entrée à la table de routage statique du firewall PfSense :
  (@S/Res AD) Via Gateway (if WAN UTM9).

La figure 4 liste l'ensemble des entrées de Port Forwarding mises en œuvre sur le pare-feu PFSense :

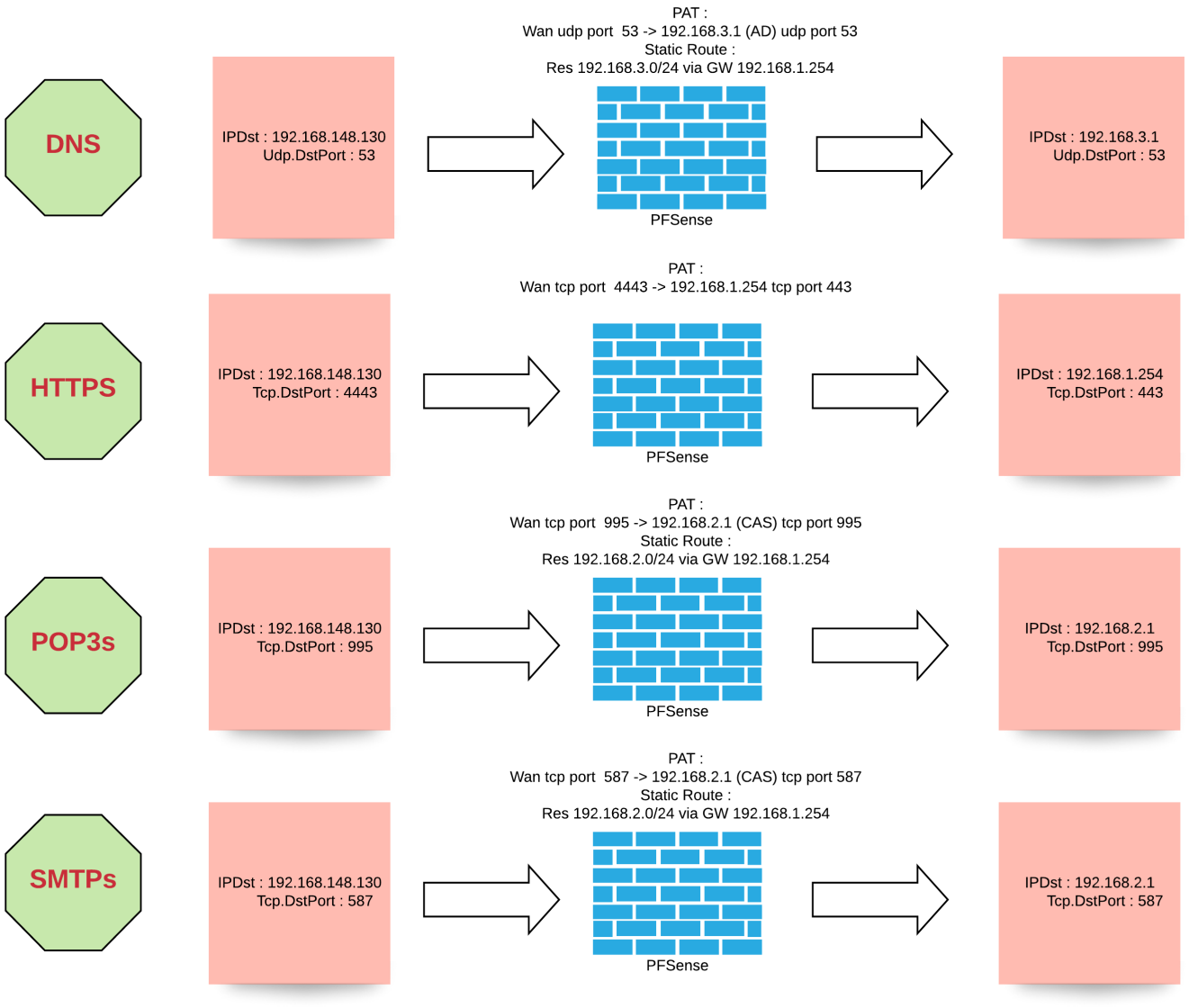

Figure 4 : Ensemble des entrées de Port Forwarding mises en œuvre sur le pare-feu PFSense.

5. Architecture fonctionnelle :

La figure 5 montre les échanges de paquets permettant au client de messagerie OWA (navigateur web comme Internet Explorer) de l'hôte externe de résoudre le nom de domaine « mail.ue19.lan » auprès du serveur DNS à l'écoute sur l'hôte AD :

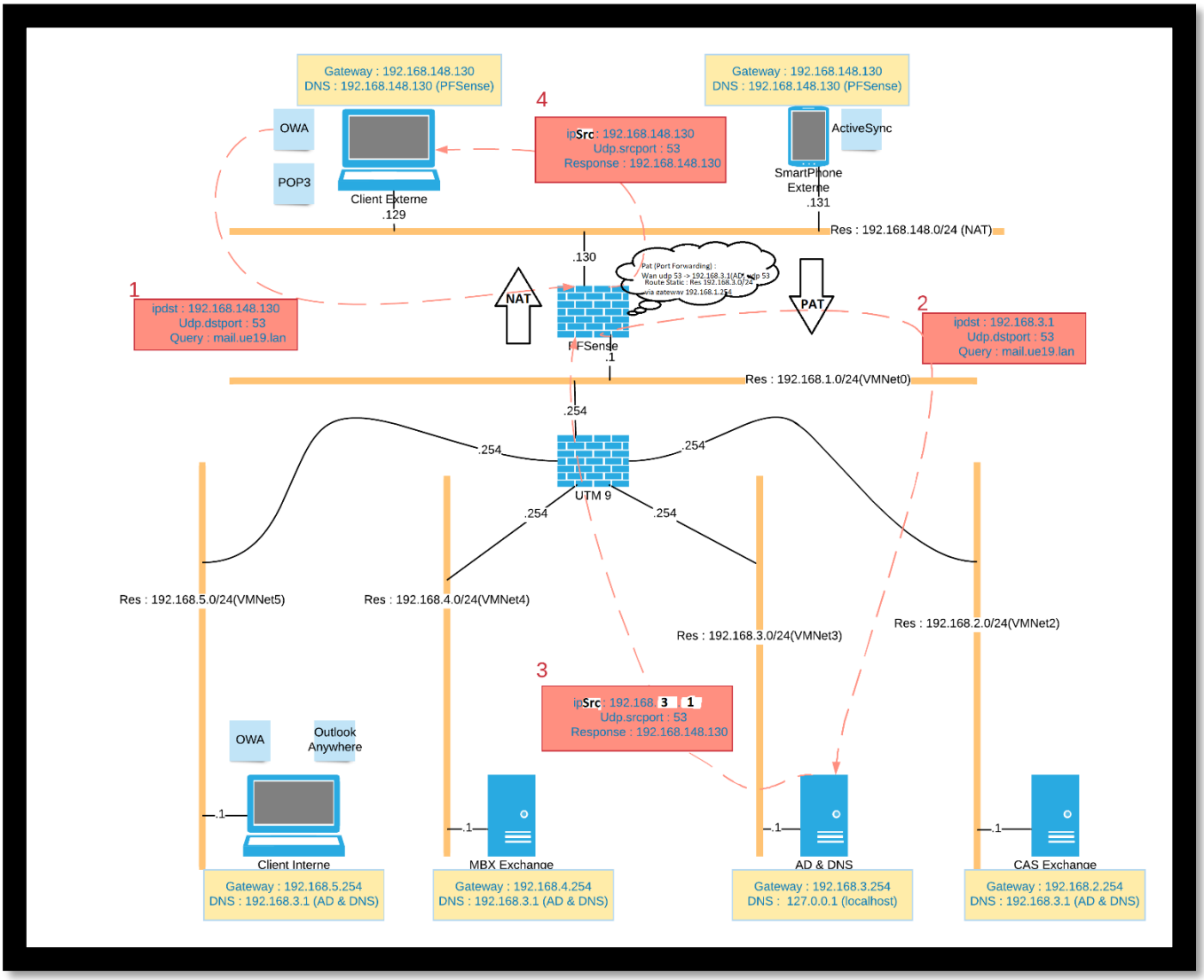

Figure 5 : Résolution de nom DNS

1- **Paquet 1 :** Le client émet une requête de résolution de nom adressé à l'interface WAN de PfSense ;
2- **Paquet 2** : PfSense modifie l'@IP de destination de la requête à celle de l'AD (grâce à l'entrée de Port Forwarding correspondant au protocole DNS), puis la redirige vers ce dernier (Il est nécessaire au firewall PfSense de connaitre le S/Res de l'AD grâce à une entrée dans sa table de routage statique) ;
3- **Paquet 3** : Le serveur DNS sur l'AD émet au client une réponse de résolution de nom (mail.ue19.lan ⇔ @WAN PfSense) ;
4- **Paquet 4** : PfSense capture la réponse de l'AD pour y modifier l'@ source de celle-ci en y incorporant la sienne coté WAN (grâce cette fois ci à la fonctionnalité NAT).

La figure 6 montre les échanges de paquets permettant au client de messagerie OWA (navigateur web Internet Explorer) présent sur l'hôte externe de se connecter au serveur Exchange :

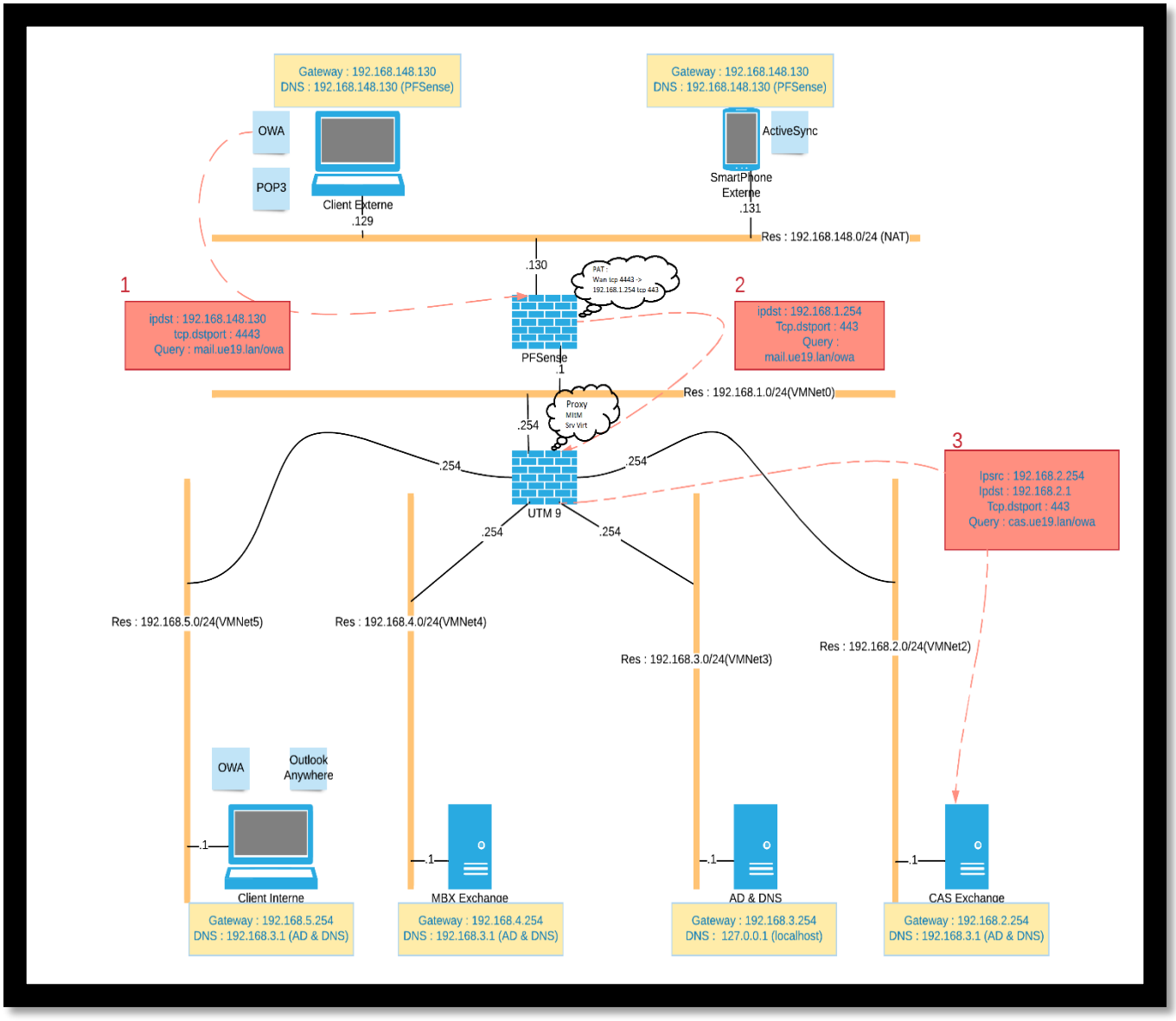

Figure 6 : Connexion OWA client externe.

1- **Paquet 1** : Le client émet une requête HTTPS adressé à l'interface WAN de PfSense sur le port TCP 4443 ;
2- **Paquet 2** : PfSense modifie l'@IP & N° de port de destination de la requête à l'@ IP Ext de l'UTM9 & TCP 443 (grâce à l'entrée de Port Forwarding « WAN TCP 4443 → @IPExt UTM9 TCP 443 »), puis la redirige vers ce dernier ;
3- **Paquet 3** : L'UTM9 agissant en reverse Proxy, déchiffre la requête HTTPS du client, car celle-ci a été chiffrée à l'aide de sa propre clé publique[9], analyse la requête pour s'assurer que celle-ci ne présente aucun risque pour le serveur Exchange & enfin forge sa propre requête HTTPS pour la transmettre au serveur Exchange ;

[9] Nous avons importé la clé privée du serveur CAS sur l'UTM9. Rappelons également que ces certificats sont signés par l'autorité de certification de l'AD, laquelle a été rajoutée comme autorité de confiance auprès de tous les hôtes de l'infrastructure.

La figure 7 montre les échanges de paquets permettant au client de messagerie POP3 (Outlook 2016) de l'hôte externe de se connecter au serveur Exchange :

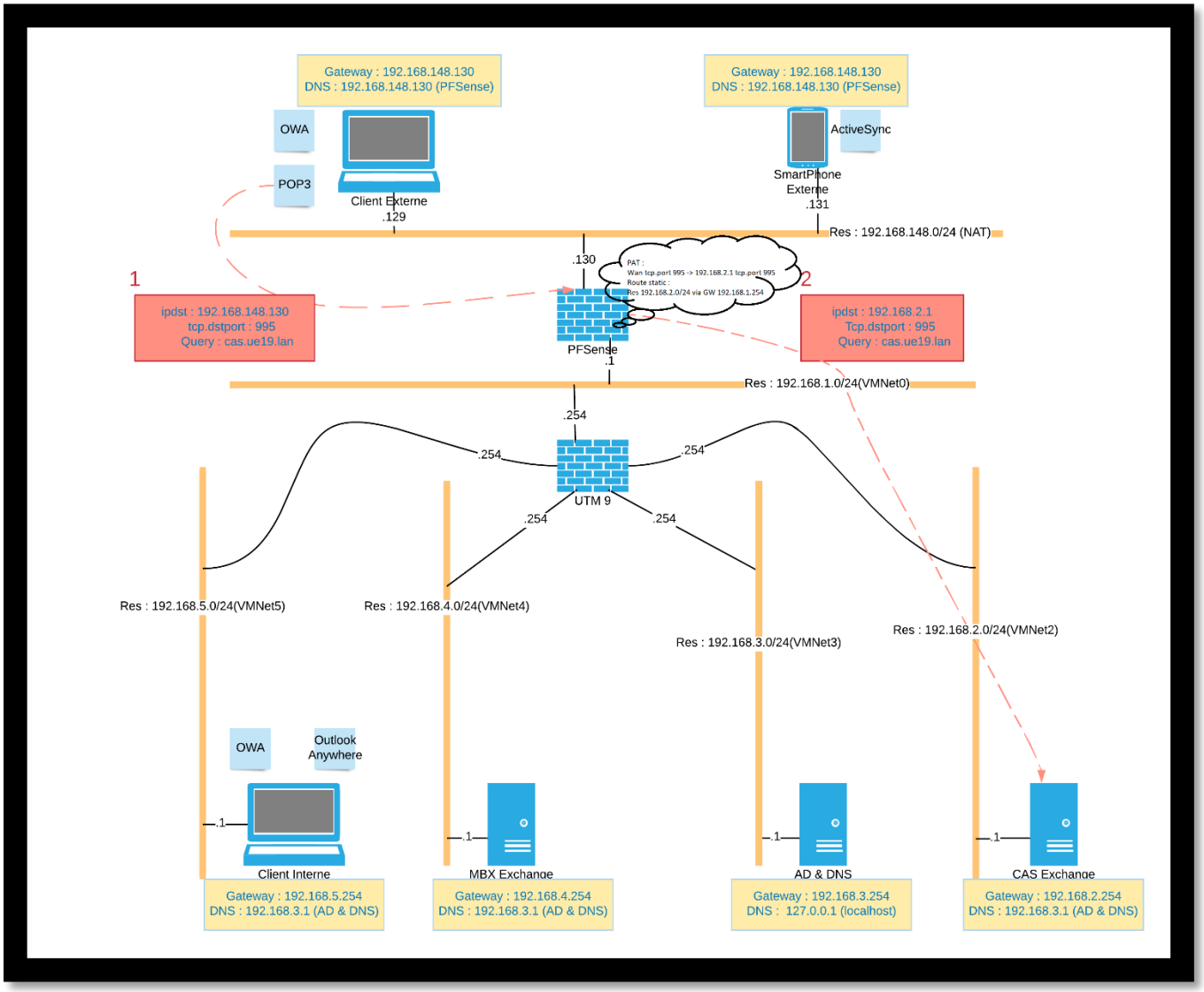

Figure 7 : Connexion pop3 client externe.

1- **Paquet 1** : Le client émet une requête POP3S adressé à l'interface WAN de PfSense sur le port TCP 995 ;
2- **Paquet 2** : PfSense modifie l'@IP de destination de la requête à celle du CAS (grâce à l'entrée de Port Forwarding « WAN TCP 995 → @IP_CAS TCP 995 »), puis la redirige vers ce dernier (A noter aussi que le firewall PfSense se doit de connaitre le S/Res du serveur CAS. Cela a été réalisé en ajoutant une entrée à sa table de routage statique).

6. Solutions et moyens de Sécurité (Accès et Fonctionnement) :

6.1. Fiabilité du service :

L'infrastructure mis en place doit assurer que le service de messagerie électronique soit fonctionnel 24H/24 & 7J/7. Pour ce faire, il faut mettre en place un plan de continuité d'activité ainsi qu'un plan de reprise d'activité.

La fiabilité de service est garantie par la redondance des données critiques (Informations relatives aux comptes des utilisateurs & leurs boites aux lettres) sur plusieurs sites (2 AD ainsi qu'un DAG MBX).

6.1.1. Disponibilité locale (incident mineur) :

Se référer à 2.2. Exigence de fiabilité de service.

6.1.2. Disponibilité sur sinistre :

Le sinistre majeur qui pourrait affecter notre infrastructure se décline soit par :

- La perte d'un serveur MBX ;
- Ou la perte d'un AD.

P.C.A.

Pour assurer la continuité des activités (échange de messages entre les utilisateurs inscrits au domaine « UE19.lan. ») en cas de sinistre, nous proposons l'utilisation d'un service de messagerie sécurisé, What's App en l'occurrence, le temps de remettre en route le système opérant chargé de la messagerie.

P.R.A

Dans le cas d'un sinistre correspondant à la perte d'un serveur MBX, la procédure à suivre pour remettre en route l'ensemble de l'infrastructure est la suivante :

1- Redirection des requêtes du CAS vers le MBX secondaire ;
2- Préparer une nouvelle machine et y installer le rôle MBX du serveur Exchange ;
3- Copier les boites aux lettres du MBX secondaire vers la nouvelle machine ;
4- Intégrer la nouvelle machine dans le DAG ;
5- Rediriger des requêtes du CAS vers la nouvelle machine MBX.

6.1.3. Scalabilité :

La scalabilité verticale est garantie en augmentant les métriques de performance des machine virtuelles sous VMWare (Processeur, RAM, Stockage).

Ex : sur un serveur 16 cœur, VMware permet de doubler le débit maximal atteint avec un exchange 2013 pour passer de 8000 à 16000 boites aux lettres [3].

6.2. Identification/authentification et contrôle d'accès :

Les comptes AD se trouvent sur une machine dans le réseau administrateur. Chaque boîte aux lettres créée sur exchange est associée à un compte sur l'AD. Ces comptes sont protégés par des mots de passe de plus de quinze caractères à changer régulièrement (1fois/trimestre).

Nous avons créé un compte administrateur ainsi que d'autres comptes d'utilisateur, nous permettant d'effectuer des tests.

6.3. Sécurité (confidentialité et intégrité) :

La confidentialité des échanges entre clients & serveurs est assurée par l'usage de protocoles sécurisés via TLS (Certificats de clé publique & privée).

Les certificats exposés par les serveurs sont signés par l'autorité de certification de confiance mise en œuvre sur l'Active Directory.

Les clients ont ainsi l'obligation d'importer le certificat de l'autorité citée.

Les utilisateurs sont informés de la nécessité de vérifier la correspondance du certificat exposé par le serveur auquel ils se connectent. Cette vigilance leurs assure qu'ils s'adressent au bon serveur, ainsi des attaques MIM ne porteraient pas atteinte à l'intégrité des échanges.

6.4. Traçabilité :

La traçabilité est garantie par les logs.

7. Pré requis du poste client :

Pour les prérequis du poste client Externe, il faut installer soit :

- Un client léger (navigateur web, tel que Internet Explorer) : sur lequel, on importe le certificat de l'autorité Active Directory.
- Ou un client lourd (tel Outlook 2016), puis le configurer de tel sorte à utiliser le protocole POP3Sec pour récupérer les emails auprès du serveur « cas.ue19.lan », ainsi que SMTPSec (Port TCP 587) pour envoyer les emails au serveur.

Pour les prérequis du poste client Interne, il faut :

- Inscrire l'hôte auprès de l'Active Directory sur le domaine « ue19.lan » & ;
- Installer un client léger (navigateur web, tel que Internet Explorer) : sur lequel, on importe le certificat de l'autorité Active Directory.
- Ou Installer un client lourd (tel Outlook 2016), puis il suffit à l'utilisateur d'entrer son login portant la notion du domaine ue19.lan ainsi que son mot de passe afin que son client de messagerie utilise Outlook AnyWhere.

Pour les prérequis du Smartphone Externe, il faut installer :

- Un client lourd (tel Gmail), puis lui spécifier les informations sur le compte utilisateur ainsi que le nom du serveur « activesync.ue19.lan ».

8. Bibliographie :

Référentiel réparti	Site	Description
[1]	https://fr.wikipedia.org/	Wikipédia
[2]	https://www.sophos.com/fr-fr/press-office/press-releases/2012/07/utm-9-release.aspx	Site officiel de Sophos
[3]	https://www.vmware.com/fr.html	Site officiel de VMWare

9. Glossaire des technologies utilisées :

Sigle & acronyme	Signification
DAT	Dossier d'Architecture Technique
Synchrone	Une invocation est dite synchrone si, après la requête, le client bloque son exécution en attendant la réponse du serveur.
Asynchrone	Une invocation est dite asynchrone si, après la requête, le client peut continuer son exécution. La réponse à la requête peut être obtenue plus tard.
DMZ	est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu.
HTTP/HTTPS	**HyperText Transport Protocol (Secured)** : protocole de transfert normalisé, utilisé par les navigateurs pour dialoguer avec un serveur Web.
IP	Internet Protocol : le type de réseau utilisé pour les réseaux locaux d'entreprise, pour Internet et pour l'Intranet.
Scalabilité	Caractéristique permettant l'agrandissement physique sans contrainte architecturale.
URL	**Uniform Resource Locator** : le chemin complet d'un document sur Internet.
AD	Active Directory.
OWA	Outlook Web App est un logiciel de messagerie web créé par Microsoft. Il permet aux usagers d'accéder à leur courrier électronique à l'aide d'un navigateur web.

POP3	est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.
DAG	Un groupe de Serveur MBX, assure ainsi la résilience des boites aux lettres