Atelier Pro

Mise en place VOIP

RASCLE Rémi

Sommaire

Description du laboratoire GSB

Le secteur d'activité :

L’industrie pharmaceutique est un secteur très lucratif dans lequel le mouvement de fusion acquisition est très fort. Les regroupements de laboratoires ces dernières années ont donné naissance à des entités gigantesques au sein desquelles le travail est longtemps resté organisé selon les anciennes structures. Des déboires divers récents autour de médicaments ou molécules ayant entraîné des complications médicales ont fait s'élever des voix contre une partie de l'activité des laboratoires : la visite médicale, réputée être le lieu d' arrangements entre l'industrie et les praticiens, et tout du moins un terrain d'influence opaque.

L'entreprise :

Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui-même déjà union de trois petits laboratoires . En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris. Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis. La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

Description du laboratoire GSB

Le système informatique :

Sur le site parisien, toutes les fonctions administratives (gestion des ressources humaines, comptabilité, direction, commerciale, etc.) sont présentes. On trouve en outre un service labo-recherche, le service juridique et le service communication.

La salle serveur occupe le 6ème étage du bâtiment et les accès y sont restreints (étage accessible par ascenseur à l'aide d'une clé sécurisée, portes d'accès par escalier munies d'un lecteur de badge, sas d'entrée avec gardien présent 24h/24).

Les serveurs assurent les fonctions de base du réseau (DHCP, DNS, Annuaire et gestion centralisée des environnements) et les fonctions de communication (Intranet, Messagerie, Agenda partagé, etc.).

On trouve aussi de nombreuses applications métier (base d'information pharmaceutique, serveurs dédiés à la recherche, base de données des produits du laboratoire, base de données des licences d'exploitation pharmaceutique, etc.) et les fonctions plus génériques de toute entreprise (Progiciel de Gestion Intégré avec ses modules RH, GRC, etc.).

Un nombre croissant de serveurs est virtualisé.

Constitué autour de VLAN, le réseau segmente les services de manière à fluidifier le trafic.

Les données de l'entreprises sont considérées comme stratégiques et ne peuvent tolérer ni fuite, ni destruction. L'ensemble des informations est répliqué quotidiennement aux Etats-Unis par un lien dédié. Toutes les fonctions de redondances (RAID, alimentation, lien réseau redondant, Spanning-tree, clustering, etc.) sont mises en œuvre pour assurer une tolérance aux pannes maximale.

L'équipement :

L'informatique est fortement répandue sur le site. Chaque employé est équipé d'un poste fixe relié au système central. On dénombre ainsi plus de 350 équipements terminaux et un nombre de serveurs physiques conséquent (45 en 2012) sur lesquels tournent plus de 100 serveurs virtuels.

On trouve aussi des stations de travail plus puissantes dans la partie labo-recherche, et une multitude d'ordinateurs portables (personnels de direction, service informatique, services commerciaux, etc).

Les visiteurs médicaux reçoivent une indemnité bisannuelle pour s'équiper en informatique (politique Swiss-Bourdin) ou une dotation en équipement (politique Galaxy). Il n'y a pas à l'heure actuelle d'uniformisation des machines ni du mode de fonctionnement.

Segmentation du réseau :

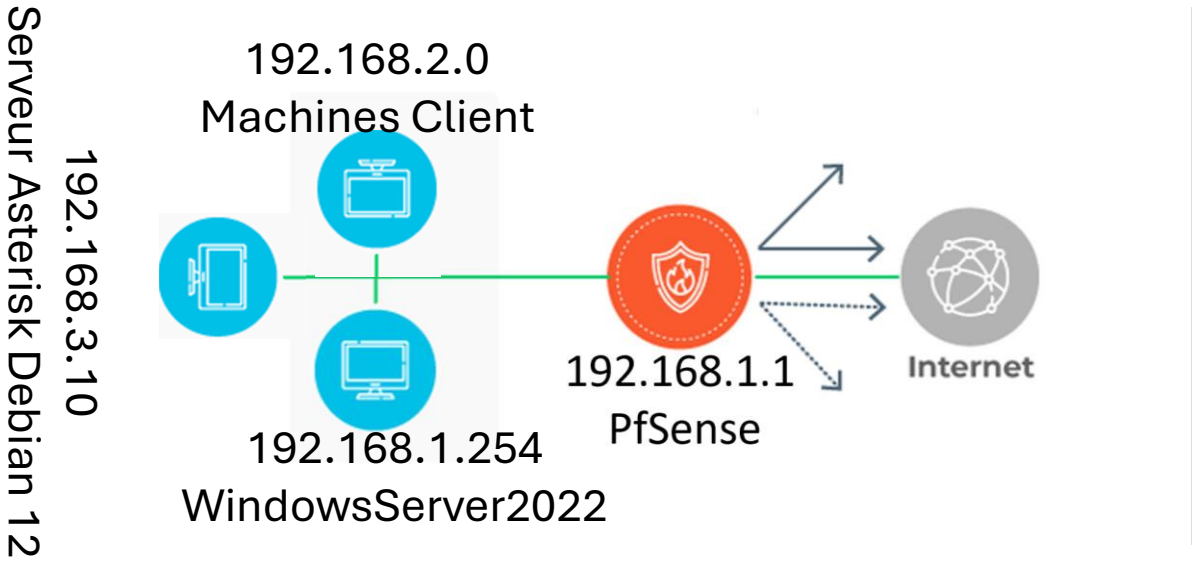
L'organisation des VLAN et de l'adressage IP est la suivante :

N° VLAN	Service(s)	Adressage IP
210	Serveur	192.168.1.0
211	Clients	192.168.2.0
212	Asterisk	192.168.3.0

Salle serveur et connexion internet :

L'organisation des serveurs et des équipements réseaux est la suivante :

- Le serveur principal est virtualisé sous le système Vmware Vcenter 7.0
- Un Commutateur Multicouche Cisco permet l'interconnection du serveur principal et la liaison vers le firewall de proximité (Internet).
- L'environnement Virtuel et réseau des Projets d'Atelier de Professionnalisation sont référencées ci-dessous :



Cahier des Charges

Déployer une solution VoIP interne basée sur Asterisk :

- Chaque utilisateur doit avoir un compte SIP
- Appels poste à poste possible
- Messagerie vocale
- Chiffrement
- Filtrage PfSense

- Mise en place d’un serveur Ubuntu
- Installation de softphones sur les machines clients

Solution et mise en place

Installation et préparation du serveur Asterisk

Le serveur Asterisk a été installé sur Ubuntu Server. Après mise à jour du système, les paquets suivants ont été installés :

sudo apt update && sudo apt upgrade -y
sudo apt install asterisk asterisk-mp3 asterisk-modules –y

Après installation, le service Asterisk a été activé et testé via :
sudo systemctl enable asterisk
sudo systemctl start asterisk
sudo asterisk -rvvv
L'invite *CLI> confirme le bon fonctionnement du service.

```
AsteriskRemi*CLI>
```

Mise en place du chiffrement TLS et SRTP

Pour sécuriser les communications SIP, un certificat auto-signé a été créé manuellement avec OpenSSL.
La commande correcte a été :
sudo mkdir -p /etc/asterisk/keys
cd /etc/asterisk/keys
sudo openssl genrsa -out asterisk.key 2048
sudo openssl req -new -x509 -key asterisk.key -out asterisk.pem -days 3650 -subj "/CN=pbx.rascle.local/O=Rascle/C=FR«

Les permissions du répertoire /etc/asterisk/keys ont ensuite été ajustées pour être accessibles par l'utilisateur asterisk (propriétaire : asterisk, droits : 600).

```
[transport-tls]
type=transport
protocol=tls
bind=0.0.0.0:5061
method=tlsv1_2
cert_file=/etc/asterisk/keys/asterisk.pem
priv_key_file=/etc/asterisk/keys/asterisk.key
verify_client=no
verify_server=no
allow_reload=yes
cipher=TLS_AES_256_GCM_SHA384
external_signaling_port=5061
external_media_address=192.168.3.10
```

Configuration des comptes SIP

Deux utilisateurs SIP ont été créés dans le fichier /etc/asterisk/pjsip.conf :

nano /etc/asterisk/pjsip.conf

```
; Utilisateur Edith Piaf ======; Utilisateur Joe Dassin ======

[1001]                          [1002]

type=endpoint                   type=endpoint
context=interne                 context=interne
disallow=ulaw,alaw,gsm          disallow=ulaw,alaw,gsm
auth=auth1001                   auth=auth1002
aors=1001                       aors=1002
callerid=Edith Piaf <1001>      callerid=Joe Dassin <1002>
media_encryption=sdes           media_encryption=sdes
transport=transport-tls         transport=transport-tls
force_rport=yes                 force_rport=yes
rewrite_contact=yes             rewrite_contact=yes
rtp_symetric=yes                rtp_symetric=yes
force_rport=yes                 force_rport=yes

[auth1001]                      [auth1002]
type=auth                       type=auth
auth_type=userpass              auth_type=userpass
username=1001                   username=1002
password=Azerty123+             password=Azerty123+

[1001]                          [1002]
type=aor                        type=aor
max_contacts=1                  max_contacts=1
```

Vérification et diagnostic du fonctionnement

Depuis la console Asterisk :

```
AsteriskRemi*CLI> pjsip show transports

Transport:  <TransportId........>  <Type>  <cos>  <tos>  <BindAddress.....................>
==============================================================================================

Transport:  transport-tls             tls      0      0  0.0.0.0:5061
Transport:  trasnport-udp             udp      0      0  0.0.0.0:5060

Objects found: 2
AsteriskRemi*CLI> pjsip show endpoints

 Endpoint:  1001/1001                                          Unavailable   0 of inf
    InAuth:  auth1001/1001
        Aor:  1001                                           1
  Transport:  transport-tls             tls      0      0  0.0.0.0:5061

 Endpoint:  1002/1002                                          Unavailable   0 of inf
    InAuth:  auth1002/1002
        Aor:  1002                                           1
  Transport:  transport-tls             tls      0      0  0.0.0.0:5061


Objects found: 2
```

Les deux utilisateurs apparaissent bien mais initialement en statut “Unavailable”.
Une erreur SSL « no start line » a révélé une mauvaise lecture du certificat TLS.

Intégration avec Active Directory

Le serveur Asterisk (192.168.3.10) a été intégré dans le réseau de l'entreprise et communique avec le contrôleur de domaine Active Directory. Le fichier /etc/resolv.conf a été ajusté :
nameserver 192.168.1.254
domain rascle.local

(serverad.rascle.local – 192.168.1.254). La résolution DNS du domaine rascle.local a été vérifiée :
nslookup rascle.local
nslookup serverad.rascle.local

L'objectif à terme est de synchroniser les comptes SIP avec les utilisateurs du domaine AD, afin que chaque utilisateur connecté à une session Windows dispose automatiquement de son softphone Linphone configuré avec son extension correspondante.

Installation et configuration des softphones Linphone

Les softphones Linphone version 5.3.1 ont été installés sur les postes clients Windows 10.
À la première ouverture, l'utilisateur a choisi :
→ Utiliser un compte SIP

Les paramètres suivants ont été rentré :

Nom d'utilisateur : 1001
Mot de passe : Azerty123+
Domaine / Serveur SIP : 192.168.3.10
Port : 5061
Transport : TLS

Dans les préférences du compte, la vérification du certificat serveur a été désactivée
(pour permettre l'utilisation du certificat auto-signé d'Asterisk).

Après enregistrement l'utilisateur apparait comme connecter et peux passer des appels aux autres utilisateurs connectés.