Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Infrastructures Réseaux et Serveurs

Arno COURTINAT

Préfecture des Bouches-du-Rhône,
Service de l'Innovation Numérique et des Systèmes d'Information et de Communication

Responsable entreprise : Lionel MOURRE

Responsable académique : Éric SOCCORSI

2024

Table des matières

1 Introduction

J’ai effectué mon stage de fin de deuxième année de Bachelor Universitaire de Technologie (BUT) au sein de la Préfecture des Bouches-du-Rhône, dans le Service de l’Innovation Numérique et des Systèmes d’Information et de Communication (SINSIC). Réalisé plus précisément au sein du Bureau des Infrastructures (BI) du SINSIC, ce stage a porté sur l’administration, l’installation, le dimensionnement et la sécurisation des infrastructures réseaux et serveurs.

Ce stage s’est articulé en diverses missions menées en parallèle (plusieurs projets secondaires venant, pour la majorité, alimenter un projet principal). L’objectif devant être mené à bien par ces missions était d’appliquer les concepts théoriques appris au cours de mes deux premières années de BUT et d’acquérir une expérience professionnelle concrète, tout en remplissant efficacement les tâches confiées au BI et en offrant mon soutien aux membres de l’équipe.

Afin d’étudier de façon exhaustive le contexte et les enjeux de ce stage, nous nous intéresserons dans un premier temps à la présentation détaillée de l’institution et de l’articulation de ses différents services, en plus de l’organisation interne et des missions du SINSIC. Nous présenterons dans un second temps le cadre théorique et technique général (c’est-à-dire les objectifs de ce stage posés en amont par-rapport à leur réalisation effective, le contexte théorique des savoirs accumulés avant le stage par-rapport à l’ensemble des savoirs théoriques accumulés après celui-ci, et les compétences techniques requises avant le stage ainsi que leur renforcement pendant celui-ci ; en somme, l’ensemble des savoirs, savoirs-faire et savoirs-être acquis avant le stage ainsi que leur évolution après celui-ci). Nous analyserons dans un troisième temps le travail réalisé dans les différents projets, son évolution par rapport aux cahiers des charges initiaux, ainsi que les difficultés rencontrées et les solutions apportées. Enfin, nous conclurons en mettant en lumière les résultats obtenus ainsi que les innombrables enseignements tirés de cette expérience enrichissante.

2 Présentation de l'Institution, de ses Services et du SINSIC

2.1 Organigramme et Articulation des Services

L'organigramme détaillé de la Préfecture des Bouches-du-Rhône peut être trouvé en Annexes (Fig. 1), en plus d'un zoom sur le Secrétariat Général Commun (SGC) dont fait partie le SINSIC (Fig. 2).

Sous l'autorité directe du Ministère de l'Intérieur ainsi que du Premier Ministre et représentant localement l'entièreté du Gouvernement, la Préfecture des Bouches-du-Rhône est le véritable centre opérationnel et décisionnel dont dépend l'administration publique jusqu'à l'échelle de la zone de Défense et de Sécurité Sud : celle-ci fait à la fois office de Préfecture de Zone («échelon administratif [sous l'autorité du préfet de zone] spécialisé dans l'organisation de la sécurité nationale et de la défense civile et économique […] [assurant] la mise en cohérence et la coordination des politiques de sécurité et de défense de l'État»), Préfecture de Région («garant de la cohérence de l'action de l'État dans la région [régissant les Préfectures de Département et de Police administrative et de contrôle de légalité, et dirigeant les services déconcentrés régionaux de l'État]»), Préfecture de Département («[direction des] services déconcentrés des administrations civiles de l'État [chargée de] l'ordre public, de la sécurité et de la protection des populations»), et Sous-Préfecture d'Arrondissement (aux côtés des Sous-Préfectures d'Aix, Istres et Arles ; «[sièges] de l'administration de l'État au niveau infra-départemental [veillant] au respect des lois et règlements, au maintien de l'ordre public et à la sécurité des populations [tout en animant] les services de l'État dans la mise en œuvre des politiques interministérielles infra-départementales»). La majorité des services sous tutelle de la Préfecture des Bouches-du-Rhône, qu'ils soient locaux au bâtiment (par exemple le Cabinet du Préfet, le Secrétariat Général pour les Affaires Régionales (SGAR), la Direction de la Citoyenneté, de la Légalité et de l'Environnement (DCLE), etc.) ou appartenant à l'un des nombreux sites distants (par exemple la Direction Départementale de la Protection des Populations (DDPP) à Marseille Rue Borde ou bien Vitrolles, la Direction Départementale de l'Emploi, du Travail et des Solidarités (DDETS) à Marseille Boulevard Périer ou bien Aix, etc.) obéissent à des fonctions et domaines d'intervention spécifiques, sous l'autorité du Cabinet du Préfet, ou bien du Secrétaire Général (SG). Toutefois, le SGC est un ensemble de services «supports», c'est-à-dire que celui-ci ne possède pas de mission politique spécifique si ce n'est la gestion et l'assistance aux autres branches précédemment citées : en-dehors du SINSIC, le SGC est également composé du Service des Ressources Humaines (SRH), du Service du Budget et des Achats (SBA), ou encore du Service du Patrimoine Immobilier et de la Logistique (SPIL). Cet ensemble de services «supports» est quant à lui sous l'autorité unique du Préfêt.

Maintenant que nous avons étudié les différents services au sein de la Préfecture ainsi que les interactions qui les articulent, nous devons aborder plus en détail le SINSIC (c'est-à-dire les activités, fonctions et missions auxquelles il obéit), tout en étudiant les différents Bureaux au sein du SINSIC ainsi que leurs interactions et les missions qui les régissent.

2.2 Activités, Missions, Organisation et Culture d'Entreprise du SINSIC

Le SINSIC est lui-même composé de différents Bureaux (le Bureau des Infrastructures (BI) duquel j'ai fait partie, le Bureau de l'Environnement Numérique et de Travail (BENT), le Bureau de l'Innovation Numérique (BIN) et le Bureau de la Sécurité et de la Relation aux Usagers (BSRU)) possédant eux-mêmes leurs propres missions, outils de travail dédiés et activités spécifiques. Tandis que le BI sera chargé du bon fonctionnement de l'infrastructure réseau en place ainsi que de son évolution (gestion de l'Active Directory (AD) avec bon placement des machines et des personnels dans les bonnes Unités d'Organisation («Organisationnal Units (OUs)») et les bons groupes, entretien et gestion de la transformation de l'infrastructure réseau existante et future (par exemple maintenance du brassage des prises réseau en fonction des dynamiques des utilisateurs finaux ainsi que maintenance du bon état des baies, migration «Autocom» et ToIP, etc.), mise en place réseau et serveurs selon les besoins avec gestion des stocks en matière d'équipements réseaux et des équipements serveurs, etc.) ; le BENT sera davantage chargé de l'allocation en équipements terminaux auprès des utilisateurs finaux ainsi que du bon fonctionnement de la flotte (par exemple

allocation en matière de stations de travail locales et/ou distantes (dispositif d'ordinateurs portables et stations d'accueil «NOeMI») ainsi que préparations préliminaires nécessaires (chiffrage, accès VPN, etc.), dépannage auprès des utilisateurs finaux des problèmes signalés avec réparation(s) physique(s) au besoin, gestion des stocks en matière de périphériques terminaux, etc.). Le BIN, quant à lui, sera plutôt responsable du développement de nouveaux outils en ligne et de la maintenance ainsi que du développement côté serveur (ou «backend») des applications déjà existantes (par exemple, développement de l'outil interne «Priam» permettant de récapituler les différents points à remplir par les différents Bureaux lors de nouvelles arrivées (créations de comptes AD et messagerie ainsi que compte devant servir de modèle pour le BI, allocation en matériel pour le BENT, etc.)); et le BSRU aura à sa charge le Standard de la Préfecture (joignable 24h/24-7j/7, le Standard de la Préfecture est une ligne dédiée servant à prendre en charge le public dans les périodes où le bâtiment ne peut pas recevoir de public).

À contrario d'une entreprise privée traditionnelle, il est préférable de parler ici de «missions» ou encore de «public visé» plutôt que de «clients» : en effet, rappelons que le SINSIC, service public directement sous l'autorité du Préfet, fait partie des «services supports» transversaux destinés à assister les autres services d'administration publique d'État dans le Département des Bouches-du-Rhône et n'a donc aucun objectif lucratif comme dans le cas d'une entreprise privée. Chaque agent a conscience de travailler par extension pour le Ministère de l'Intérieur et de manipuler des données pouvant être sensibles (par exemple, le réseau ministériel que nous allons étudier dans la partie «Travail réalisé dans les différents projets» est un réseau de sécurité A+ : dévoiler son adressage IP réel ainsi que sa numérotation VLAN exacte est donc prohibé), cela allié au caractère officiel de l'Institution et à l'importance de certains acteurs ou certains services présents entre les murs (par exemple, toute interruption réseau peut perturber l'activité d'un service donné (aussi vitale soit-elle : par exemple, le SGAR gère des fonds régionaux provenant des différents Ministères ainsi que de l'Union Européenne), ou encore une éventuelle faille dans la sécurité du réseau pourrait dévoiler jusqu'aux données confidentielles du Cabinet du Préfet) fait que rigueur, discipline, efficacité et discrétion sont évidemment de mise en plus de disponibilité, adaptabilité et autonomie, formant la «culture d'entreprise» de l'Institution entière.

3 Cadre Théorique et Technique Général

3.1 Objectifs en Amont et Réalisation Effective

Comme mentionné précédemment, les objectifs personnels que j'avais fixé comme devant être impérativement remplis par ce stage étaient «[l'application des] concepts théoriques appris au cours de mes deux premières années de BUT et [l'acquisition d'] une expérience professionnelle concrète, tout en remplissant efficacement les tâches confiées au BI et en offrant mon soutien aux membres de l'équipe». Pour formuler de manière plus exhaustive, en plus de la familiarisation avec le milieu professionnel et avec le travail en équipe (ce qui inclut également l'intégration à ladite équipe et l'assimilation de la «culture d'entreprise» : c'est-à-dire l'assimilation des valeurs, des normes, des comportements, et des pratiques spécifiques à l'Institution comme discuté plus haut), le développement de nouveaux savoirs et compétences techniques ainsi que la pratique concrète des savoirs théoriques et compétences techniques acquises antérieurement à ce stage représentait un objectif majeur devant être rempli (à travers le travail fourni dans la réalisation de différents projets, que nous étudierons dans la partie «Travail réalisé dans les différents projets»), afin d'obtenir une expérience professionnelle tangible en lien avec mon domaine d'étude.

À l'issue de ce stage, nous pouvons dire que ces différents objectifs prévus ont été pleinement remplis (comme peut par exemple en attester la fiche de suivi remplie et signée par mon tuteur en entreprise). Premièrement, en ce qui concerne l'ensemble des objectifs de savoirs-être (c'est-à-dire la familiarisation avec le milieu professionnel à travers l'intégration dans une équipe ou l'assimilation de la «culture d'entreprise») : tandis que «Travailler en équipe» a été inscrit dans la rubrique «Principaux acquis», les lignes «Est intégré, adapté à la culture d'entreprise», «S'adapte aux circonstances et aux autres […]» et «Contribue à la résolution de problèmes collectifs» ont toutes été notées à hauteur de 9/10. Deuxièmement, en ce qui concerne l'ensemble des objectifs de savoirs et savoirs-faire (c'est-à-dire le développement de nouveaux savoirs et compétences techniques, tout en consolidant et/ou pratiquant concrètement les savoirs théoriques et compétences techniques acquises antérieurement) : tandis que l'ensemble des projets ont été menés à bien (tous les projets inscrits dans «Objectifs et Résultats attendus» ont également été inscrits dans «Réalisations effectives»), la ligne «Apprend rapidement, sait mobiliser ses connaissances» a également été notée à hauteur de 9/10. En termes d'objectifs additionnels, nous pouvons dire que d'autres objectifs non-prévus en amont ont également été remplis en matière de savoirs-être : ma personnalité en matière de ponctualité et rigueur au travail a pu être démontrée comme fiable (les lignes «Travaille bien (fiabilité et rigueur)», «Présentation, ponctualité, assiduité» et «Maturité, attitude professionnelle, sens des responsabilités» ont respectivement été notées à hauteur de 9/10, 10/10 et 9/10).

3.2 Savoirs Théoriques Accumulés Antérieurement et Postérieurement au Stage

Tout au long de mes deux premières années de BUT, un ensemble de savoirs théoriques (et autres compétences techniques ne pouvant être travaillées que dans un cadre pédagogique bien précis et en-dehors de tout environnement de production, comme par exemple le réseau virtuel universitaire QAMU) a pu être mis à ma disposition afin d'être compris et assimilé. Ces savoirs théoriques englobent par exemple les compétences en matière de tests de pénétration (ou «tests d'intrusion» ou encore «pentesting» : il s'agit là de la recherche de vulnérabilités (en prenant directement le point de vue d'un éventuel cybercriminel attaquant) sur un réseau informatique cible) ne pouvant pas être pratiquées sur des cibles autres que des machines virtuelles dédiées à l'entraînement pour des raisons juridiques évidentes (rappelons que l'article 323-1 du Code Pénal stipule que «le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un [réseau ou système informatique] est puni de trois ans d'emprisonnement et de 100 000€ d'amende» ou que d'après l'article 323-2 «le fait d'entraver ou de fausser le fonctionnement d'un [réseau ou système informatique] est puni de cinq ans d'emprisonnement et de 150 000 € d'amende», et que l'entièreté du trafic réseau provenant du réseau informatique de l'université est surveillé par ses administrateurs), ou encore les compétences en matière de configuration, de déploiement, d'administration, de maintenance, de sécurisation et de

dimensionnement d'infrastructures réseaux (incluant également la sécurisation par pare-feu ou «firewalling») qui ont pu certes être pratiquées durant mon cursus sur du matériel réseau réel mais, pour des raisons évidentes de sécurité et de possibles répercussions en cas d'erreur (à titre d'exemple, rappelons que le protocole de routage BGP («Border Gateway Protocol»), protocole de routage de l'Internet, est extrêmement puissant et qu'une erreur concernant celui-ci pourrait avoir des conséquences sur le réseau réel (faussage des tables de routage de certains équipements réseau réels entraînant une perte de connectivité momentanée, etc.)), n'ont été pratiquées qu'en-dehors de tout environnement de production, hors de toute réelle menace de cyberattaque et en simulant entre élèves en salle de Travaux Pratiques l'interconnexion entre sites distants, sièges d'entreprise(s), etc.

Pas ou peu de nouveaux savoirs théoriques ont été ajoutés à travers ce stage à ceux déjà acquis antérieurement (mes différents projets ayant pu être réalisés dans un cadre concret (utilisation d'un réseau de production ou étude d'intervention sur un réseau en production et d'entretien sur un réseau en production, etc.), nous pouvons donc dire comme nous l'étudierons dans la sous-partie suivante que des compétences techniques ont été développées ou consolidées plutôt que des savoirs théoriques); toutefois, une solide expérience concrète de la réalité du terrain a pu être apportée à une partie des savoirs théoriques acquis précédemment (par exemple les compétences en matière de configuration, de déploiement, d'administration, de maintenance, de sécurisation et de dimensionnement d'infrastructures réseaux (et, par extension, celles en matière de sécurisation par pare-feu ou «firewalling»); celles en matière de tests d'intrusion n'ont malheureusement pas ou peu été concernées par les projets qui m'ont été affectés), les transformant donc en compétences techniques concrètes plutôt qu'en savoirs théoriques.

3.3 Compétences Techniques Requises Antérieurement et Consolidation

Tout au long de mes deux premières années de BUT, un ensemble de compétences techniques pratiques (allant de l'administration système et réseaux avec GNU/Linux ou Windows Server (sur machines virtuelles «basées sur le noyau» («Kernel-based Virtual Machine» ou KVM) ou Oracle VirtualBox ou bien directement sur machines physiques) avec configuration et sécurisation des services nécessaires, au développement d'applications Python communicantes avec bases de données relationnelles MariaDB, en passant par la configuration, le déploiement, l'administration, la maintenance, la sécurisation et le dimensionnement d'infrastructures réseaux (réseaux locaux Ethernet comme réseaux locaux sans-fil («Wireless Local Area Network» ou WLAN)) redondantes sous IPv4 comme IPv6 (sur matériel réseau majoritairement CISCO)) a pu être mis à ma disposition afin d'être compris et assimilé. Parmi toutes ces compétences, celles requises afin d'accéder à ce stage étaient l'administration système et réseaux Windows Server ainsi que la connaissance de l'AD, la capacité à pouvoir déployer et/ou manipuler des équipements réseau Hewlett-Packard (HP) sans interface utilisateur autre qu'une connexion console (les compétences acquises sur matériel CISCO étant facilement transposables sur d'autres constructeurs) et à pouvoir comprendre et administrer une infrastructure réseau déjà en place, ainsi que la connaissance des grands principes fondamentaux de la sécurité réseau ainsi que les bonnes pratiques à mettre en place (sécurisation par pare-feu ou «firewalling», sécurité des services, VPN, etc.).

La totalité de ces compétences requises afin d'accéder à ce stage ont été concernées par les projets qui m'ont été affectés et ont donc pu être consolidées (nous le verrons plus en détail dans la partie «Travail réalisé dans les différents projets», mais mes projets ont consisté en l'étude de l'infrastructure réseau en place afin de cartographier les baies de brassage et coordonner leur «nettoyage», en le diagnostic et la réinitialisation d'équipements réseau (commutateurs multicouches HP) inutilisés afin de constituer une réserve, en le choix d'un outil (avec appréhension de son utilisation, avec la distribution de l'outil auprès des agents le réclamant et avec la documentation de son utilisation) destiné à faciliter l'administration système des machines dont les mots de passe de sessions Windows ont été égarés, en l'élaboration d'un équipement réseau sous pfSense ainsi que de son écosystème de production, et en la sécurisation du modèle de station blanche réalisé par Maël LESAICHERRE (alternant au sein de l'Institution provenant également du BUT dans lequel il fait partie la promotion 2024 précédant la mienne)). De plus, à ces compétences requises consolidées peuvent s'ajouter de toutes nouvelles compétences développées par le stage, comme la manipulation

d’équipements serveurs dédiés qui est un aspect non-encore abordé dans le programme des deux premières années de BUT (nous verrons que l’un de mes projets en plus de ceux décrits plus haut était la mise à niveau et la configuration selon un cahier des charges d’un serveur HP (modèle précis *HPE ProLiant DL380*) destiné à devenir un nouveau serveur «Autocom» au sein de l’infrastructure de Téléphonie sur IP («Telephony over Internet Protocol» ou ToIP) (infrastructure séparée de l’infrastructure réseau traditionnelle par un pare-feu, se trouvant dans une de ses «Zones Démilitarisées» («De-Militarised Zones» ou DMZs))), le chiffrement et déchiffrement de supports de stockage avec le logiciel Windows Cryhod ou l’utilitaire Linux CryptSetup (permettant de configurer le chiffrement «Configuration Unifiée des Clés pour Linux» («Linux Unified Key Setup» ou LUKS)), la technologie Microsoft Deployment Toolkit, ou encore la manipulation matérielle (ou «manipulation du hardware» : intervenir physiquement sur des machines m’est fréquemment arrivé durant mon stage (notamment, comme nous le verrons plus en détail, pour des problématiques de création de nouvelles machines ou encore de clonage de disques durs internes)) et a pu me faire progresser sur ce point sur lequel je me sentais très peu à l’aise à titre personnel.

4 Travail Réalisé dans les Différents Projets

4.1 Projets secondaires

4.1.1 Étude de l'Infrastructure Réseau en Place, Coordination du «Nettoyage» des Baies de Brassage

La surveillance réseau (ou «monitoring» réseau, c'est-à-dire le processus de surveillance continue et systématique de l'activité et des performances du réseau (dispositifs connectés, services et applications, trafics de données, etc.) via la collecte par un outil spécialisé de données en temps réel (utilisation de la bande passante, latences, taux de perte de paquets, etc.) afin de garantir la disponibilité, la fiabilité, et l'efficacité du réseau en détectant et en analysant les éventuels problèmes ou anomalies) est un aspect primordial pour les réseaux informatiques de toutes tailles. L'outil spécialisé utilisé concernant les réseaux gérés par le BI est le logiciel TelemetroBox-NG (développé par le SGAMI Ouest (Secrétariat Général pour l'Administration du Ministère de l'Intérieur, service déconcentré du ministère de l'Intérieur chargé en matière de Systèmes d'Information et de Communication (SIC) d' «assurer au bénéfice des services locaux […] l'ingénierie, l'installation et la maintenance des SIC de sa compétence», les SIC sous compétence du SGAMI étant ceux de la Police Nationale et «les Services Interministériels Départementaux Systèmes d'Information et de Communication (SIDSIC)») à la DZSIC (Direction (Zonale) des Systèmes d'Information et de Communication) de Rennes) : celui-ci permet une supervision complète (état et détail de chaque équipement réseau en fonction, encombrement réseau, etc.) des réseaux gérés par le BI. Le logiciel TelemetroBox-NG ayant donc été conçu par une entité à part entière, nous ne discuterons donc pas ici de son fonctionnement interne (par exemple, comment les informations sont récoltées auprès des différents équipements et remontées à un hypothétique serveur de centralisation (hypothétiquement en utilisant des interrogations du Protocole Simple de Gestion Réseau («Simple Network Management Protocol» ou SNMP)), etc.) mais plutôt de son utilisation et des actions réalisées au moyen de ce logiciel de «monitoring».

Il est important de souligner que, comme évoqué précédemment, les réseaux gérés par le BI (qui sont, par extension, le réseau du Ministère de l'Intérieur) sont classés A+ concernant leur sécurité : aucun adressage IP réel ainsi que numérotation VLAN exacte ne seront dévoilés dans le présent rapport (la présentation de sa topologie générale et des matériels utilisés (comme nous le verrons dans la sous-partie suivante) sont toutefois possibles).

[Merci de se référer à la Fig. A1 trouvable en Annexes (page 6), ainsi qu'à sa légende]

[Merci de se référer à la Fig. A2 trouvable en Annexes (page 6), ainsi qu'à sa légende]

Ce logiciel est entre autres utilisable afin d'obtenir un récapitulatif de l'état des interfaces réseau de chaque baie de brassage (du site principal, en l'occurrence). C'est ce qui a été fait depuis l'onglet *Interfaces* de la rubrique *Gestion*, afin de cartographier l'une après l'autre les 18 baies de brassage du site (notons également que chaque baie de brassage est représentée par un symbole de commutateur réseau sur la schématisation : en réalité, chaque baie est composée de 2 ou 3 commutateurs reliés par une double liaison fibre optique afin d'offrir entre eux une double liaison redondante à haute vitesse).

[Merci de se référer à la Fig. A3 trouvable en Annexes (page 7), ainsi qu'à sa légende]

[Merci de se référer à la Fig. A4 trouvable en Annexes (page 7), ainsi qu'à sa légende]

Le critère afin de déclarer une interface comme «non-utilisée» était le suivant : celle-ci devait être en état «down» depuis au moins 12 mois (c'est-à-dire que celle-ci avait été précédemment brassée (raccordée à une prise murale) pour une utilisation passée et nécessitait d'être débrassée afin de libérer de la place sur les commutateurs des baies ainsi que pour libérer des câbles, en plus

d’améliorer la sécurité du réseau en réduisant les points d'entrée au minimum planifié et en facilitant la gestion des ressources réseau). Celles-ci étaient au nombre de 254, avant que le critère ne soit revu comme «supérieur ou égal à 10 mois» (augmentant légèrement leur nombre).

Une fois la cartographie terminée, une intervention physique dans chaque baie était donc nécessaire afin de retirer les câbles des interfaces précédemment repérées et/ou s’assurer qu’aucun câble ne s’y trouvait (cette étape de débranchement physique dans toutes les baies à été réalisée en collaboration avec Maël LESAICHERRE).

4.1.2 Diagnostic et Réinitialisation d’Équipements Réseau Inutilisés

Les commutateurs précédemment évoqués comme partie intégrante des baies de brassage du site peuvent éventuellement présenter des pannes et défaillances, selon leur temps et degré d’utilisation, en cas de surtensions électriques, etc. (défaillance de l’alimentation électrique, défaillance de composants internes, défaillance de ports Ethernet et/ou fibre optique, etc.) : constituer une réserve de matériel réseau de rechange est donc un aspect primordial pour les réseaux informatiques de toutes tailles.

Un ensemble de 21 commutateurs de niveau 2 et 3 (tous dans des états inconnus, il s’agissait majoritairement de modèles de niveau 3 ayant été réservés afin de servir de matériel de secours mais dont les identifiants de connexion console avaient été oubliés (il s’agissait précisément de modèles *3COM 5500-EI*, *HP A3600*, *HP FlexNetwork 5130*, *CISCO Catalyst 2950*, *CISCO SF-220* et *H3C S5500*)) était présent et devait être diagnostiqué ainsi que trié afin de constituer ladite réserve : se connecter en console sur chacune des machines (voire utiliser le Menu de Démarrage («Boot Menu») afin de contourner le fichier de configuration lorsque l’appareil demandait des identifiants de connexion pour l’interface console, comme montré et détaillé plus bas) puis utiliser une suite de commandes afin de diagnostiquer la santé des composants matériels et consulter (voire écraser par un fichier de configuration d’usine) le fichier de configuration stocké en mémoire était donc nécessaire et a été fait.

[Merci de se référer aux Figs. B1, B2 et B3 trouvables en Annexes (page 8), ainsi qu’à leur légende]

Cette opération m’a permis de me familiariser avec un nouveau jeu de commandes que le jeu de commandes CISCO (ainsi qu’une nouvelle logique : les commutateurs de famille HP (dont font partie les 3 modèles majoritaires montrés ci-dessus), en plus de partager le même jeu de commandes syntaxiquement différent, ne possèdent qu’un unique mode de configuration (avec un prompt constitué du nom de machine («hostname») de l’appareil), ce qui est assez désarçonnant lorsque l’opérateur est habitué à une logique CISCO davantage sécurisée constituée de 3 modes de configuration différents (un mot de passe supplémentaire au mot de passe de connexion console est demandé sur les modèles CISCO afin d’accéder au mode de configuration privilégiée («Privileged EXEC») correspondant au deuxième niveau de modes de configuration, là où les modèles de famille HP ne demandent donc que le mot de passe de connexion console : c’est donc en cela que nous pouvons dire que la logique HP, orientée simplicité de configuration, est moins sécurisée que la logique CISCO)), ainsi qu’avec un nouveau jeu de commandes CISCO non-encore abordé dans le programme des deux premières années de BUT : le jeu de commandes concernant le diagnostic de la santé du matériel, dont les principales commandes sont visibles dans les images suivantes en ce qui concerne le matériel HP.

[Merci de se référer à la Fig. B4 trouvable en Annexes (page 8), ainsi qu’à sa légende]

[Merci de se référer à la Fig. B5 trouvable en Annexes (page 9), ainsi qu’à sa légende]

[Merci de se référer aux Figs. B6 et B7 trouvables en Annexes (page 9), ainsi qu’à leur légende]

Suite au diagnostic de chacun des appareils, ceux dont le matériel était sain ont été remis à zéro et mis en réserve, tandis que ceux présentant des défaillances ont été triés et doivent partir en maintenance auprès de la DSIC du SGAMI Sud.

4.1.3 Mise à Niveau et Configuration du Futur Serveur Autocom

À chaque poste de travail installé dans les locaux de la Préfecture et ses sites dépendants est en théorie associé un téléphone IP répertorié par un numéro unique. Ce service interne de ToIP doit être hébergé et centralisé sur un serveur dit «Autocom» (également désigné comme «autocommutateur privé» ou PABX («Private Automatic Branch Exchange»), ce type de serveur permet la gestion des appels téléphoniques internes (communication entre différents postes téléphoniques au sein de l'Institution sans avoir à passer par le réseau téléphonique public) et externes (communication entre le réseau de téléphonie interne et les lignes téléphoniques traditionnelles ou numériques de l'extérieur) au sein d'une organisation en assurant leur routage (commutation automatique vers des extensions ou départements concernés) ainsi que diverses fonctionnalités avancées (contrôle d'accès, gestion de file d'attente, messagerie vocale, etc.)). Ce service «Autocom» était jusqu'ici hébergé sur un serveur de marque TERRA qui commençait malheureusement à présenter des dysfonctionnements physiques : un nouveau serveur capable d'endosser ce rôle était donc requis.

Nous ne nous intéresserons pas ici à la mise en œuvre concrète du service «Autocom» sur la machine mais seulement aux étapes préliminaires à son installation et configuration : après une étude de compatibilité, la remise à niveau du serveur (l'appareil récupéré en réserve était un HP *HPE ProLiant DL380 Gen9* hébergeant nativement Windows Server 2012R2, or, la version de Windows Server standardisée sur toutes les machines dans le SI du du Ministère de l'Intérieur étant Windows Server 2019, un changement de système d'exploitation s'imposait donc) avec la reconstruction RAID (nous étudierons en détail ci-dessous le concept de RAID), l'installation des logiciels de gestion serveur HP, ainsi que l'installation et la configuration des services demandés.

[Merci de se référer à la Fig. C1 trouvable en Annexes (page 10), ainsi qu'à sa légende]

La première étape à suivre après avoir collecté les informations nécessaires auprès du système d'exploitation natif de la machine (telles que numéro de série, date de sortie d'usine, version du Firmware BIOS, modèle exact de processeur, etc. ; ces informations peuvent facilement être récupérées au moyen de commandes PowerShell dédiées) afin de réaliser une étude de compatibilité avec Windows Server 2019 (en l'occurrence, la documentation communautaire officielle HP peut nous apprendre que ce modèle précis est effectivement compatible avec Windows Server 2019) et nous être assurés que tous les supports de stockage de la baie (quatre, en l'occurrence) sont sains, était la création du bon type de Regroupement Redondant de Disques Indépendants («Redundant Array of Independent Disks» ou RAID) à l'aide d'un utilitaire présent par défaut dans le Firmware BIOS de ce modèle de serveur HP, représenté ci-dessous.

[Merci de se référer aux Figs. C2, C3 et C4 trouvables en Annexes (page 11), ainsi qu'à leur légende]

La technologie de Regroupement Redondant de Disques Indépendants («Redundant Array of Independent Disks» ou RAID) est une technologie de stockage extrêmement puissante non-encore abordée au programme des deux premières années de BUT, permettant de combiner plusieurs supports de stockage afin d'améliorer les performances (c'est-à-dire maximiser l'espace de stockage et/ou la vitesse de lecture/écriture) et/ou d'améliorer la fiabilité (c'est-à-dire maximiser la redondance afin de minimiser les chances de pertes de données en cas de défaillance d'un support de stockage). Plusieurs «niveaux» de RAID existent, chacun offrant un compromis différent entre performance et fiabilité :

- Le RAID 0 (également appelé «striping»), maximise les performances au dépit de la fiabilité (les données sont réparties sur x supports de stockage sans système de redondance (par exemple, un RAID 0 mis en place entre 3 disques de 500Go chacun aura pour résultat un disque virtuel de 1,5To, sauf que des pertes de données auront donc lieu en cas de défaillance de l'un de ces trois disques)).
- Le RAID 1 (également appelé «mirrorring», fonctionne de l'exacte même manière que le «mirrorring ZFS» que nous étudierons dans la sous-partie «Élaboration d'un Équipement Réseau

sous pfSense et de son Écosystème de Production») maximise la fiabilité au dépit des performances (les données sont copiées sur *x* supports de stockage sans qu'aucune maximisation de l'espace de stockage ne soit prévue (par exemple, un RAID 1 mis en place entre 2 disques de 500Go chacun (le «mirrorring» est principalement conçu pour fonctionner entre deux supports mais est également envisageable entre plus de deux) aura pour résultat un disque virtuel de 500Go (mais le système sera capable de survire à une défaillance de disque, 2 copies identiques existant en tout de ce disque dur virtuel))).
- Les RAIDs 5 et 6, plus complexes, offrent des compromis entre performance et fiabilité au moyen de la réservation sur chaque disque d'une part dédiée à contenir des bits de parité (ces bits de parité servant, en cas de panne de disque(s), à pouvoir reconstruire («deviner») les données perdues par une opération de «OU exclusif» avec les données restantes) : le RAID 5 (très utilisé avec un.des disque.s inactif.s de rechange («spare») venant remplacer automatiquement un.des éventuel.s disque.s défectueux), devant être mis en place entre 3 disques minimum, réserve sur chaque disque une part dédiée aux bits de parité (toutes les parts accumulées faisant la taille du plus petit disque du RAID) de façon à ce que la perte de l'un des disques n'entraîne pas de perte de données (un RAID 5 n'est toutefois pas capable de garantir la récupération des données en cas de défaillance de plus d'un disque) (par exemple, un RAID 5 mis en place entre 3 disques de 500Go chacun aura pour résultat un disque virtuel de 1To, sauf que l'un des disques au maximum pourra subir une défaillance sans qu'aucune donnée ne soit perdue) ; le RAID 6 (peu utilisé), devant être mis en place entre 4 disques minimum, réserve sur chaque disque une part plus élevée dédiée aux bits de parité (toutes les parts accumulées faisant deux fois la taille du plus petit disque du RAID) de façon à ce que la perte de deux des disques n'entraîne pas de perte de données (un RAID 6 n'est toutefois pas capable de garantir la récupération des données en cas de défaillance de plus de deux disques) (par exemple, un RAID 6 mis en place entre 4 disques de 500Go chacun aura pour résultat un disque virtuel de 1To, sauf que deux des disques au maximum pourront subir une défaillance sans qu'aucune donnée ne soit perdue).
- Le RAID 10 (aussi appelé «RAID 1+0»), quant à lui, combine les avantages du RAID 1 et du RAID 0 en offrant à la fois une haute performance et une excellente redondance des données : devant être mis en place entre un nombre pair de disques supérieur ou égal à 4, chaque paire de disques est mise en RAID 1 («mirrorring») avant d'être intégrée à une structure RAID 0 (par exemple, un RAID 10 mis en place entre 4 disques de 500Go chacun aura pour résultat un disque virtuel de 1To, sauf que chaque paire d'un système RAID 10 pourra toujours tolérer la défaillance de l'un de ses disques sans perte de données). Il s'agit toutefois d'une logique très coûteuse en raison de la multiplication du nombre de disques physiques utilisés.

Dans le présent exemple, la présentation très claire et concise du logiciel *Smart Storage Administrator* nous indique qu'à partir de 4 disques durs physiques («unités physiques») de 300Go chacun, un seul disque dur virtuel («unité logique») est créé, résultat d'un RAID 5 à la capacité de stockage belle et bien égale à la somme de tous les disques moins l'un d'entre eux (en l'occurrence, 900Go) : résultat d'un choix qui m'a été laissé, ce RAID 5 a été choisi pour cause d'un très bon compromis entre maximisation de l'espace de stockage tout en pouvant supporter la perte de l'un des supports de stockage. C'est ainsi sur ce disque dur virtuel créé que nous devons désormais travailler (installer Windows Server en y créant les partitions adéquates, etc.).

[Merci de se référer à la Fig. C5 trouvable en Annexes (page 12), ainsi qu'à sa légende]

[Merci de se référer à la Fig. C6 trouvable en Annexes (page 12), ainsi qu'à sa légende]

Une fois notre système opérationnel, l'étape suivante consiste donc en l'installation des logiciels spécialisés de gestion serveur HP. Rappelons toutefois que la machine hébergeait nativement Windows Server 2012R2 : la plupart des logiciels conseillés par la documentation officielle HP pour ce modèle précis de serveur n'étaient pas compatibles avec Windows Server 2019 et renvoyaient des erreurs au moment de tenter de les installer. Seuls le logiciel vu précédemment *Smart Storage Administrator* (dans sa version en ligne de commande comme dans sa version en interface graphique vue précédemment) (avoir ce logiciel installé dans le système d'exploitation

permet de supprimer le besoin de redémarrer le serveur afin d'accéder au Firmware BIOS pour modifier et/ou obtenir des informations sur l'architecture RAID mise en place), et le logiciel HPE *System Management Homepage* ont pu être installés.

[Merci de se référer à la Fig. C7 trouvable en Annexes (page 13), ainsi qu'à sa légende]

Une fois la totalité des logiciels spécialisés de gestion serveur HP compatibles installés, la prochaine et dernière étape consiste donc en l'installation et l'activation des fonctionnalités demandées (le cahier des charges stipulait que le service Windows de Bureau à Distance devait être activé, ainsi que le service DNS, et que la sauvegarde incrémentielle quotidienne à 21h des données devait être faite en plus des clichés instantanés («snapshots») quotidiens à 21h également (cette combinaison de sauvegarde et de clichés instantanés offre une solution très efficace pour prévenir la perte de données, en assurant à la fois une copie des fichiers et la possibilité de restaurer le système à un état antérieur)). La plupart de ces modifications peuvent se faire simplement via le Gestionnaire de Serveur Windows Server : tandis qu'un simple interrupteur doit être inversé dans la rubrique *Serveur Local* afin d'activer à l'écoute le service Bureau à Distance («Remote Desktop Protocol» ou RDP, permettant d'obtenir une session graphique à distance) sur cette machine, une simple case *Serveur DNS* est à cocher dans la rubrique *Rôles de Serveurs* de *Ajouter des rôles et des fonctionnalités* pour activer le service DNS (à ce stade, nous pouvons nous assurer que les ports 3389 et 53 (correspondant respectivement aux services RDP et DNS) sont bien ouverts via la commande PowerShell «Get-NetTCPConnection | Select-Object LocalAddress, LocalPort, RemoteAddress, RemotePort, State, OwningProcess»). De plus, en ce qui concerne l'outil de sauvegarde Windows Server, une simple case Sauvegarde Windows Server doit être cochée dans *Fonctionnalités* pour que l'application correspondante apparaisse dans le menu *Démarrer*, et la gestion des clichés instantanés est possible directement avec un clic droit dans l'Explorateur de fichiers sur l'un des lecteurs précédemment créés (C:\ ou D:\) :

[Merci de se référer aux Figs. C8 et C9 trouvables en Annexes (page 13), ainsi qu'à leur légende]

4.1.4 Choix et Mise en Œuvre d'un Outil d'Administration Système

Au-delà du fait qu'il est tout à fait possible que les utilisateurs finaux de périphériques terminaux oublient leur mot de passe, le fonctionnement de l'AD de l'Institution est tel que toute machine n'ayant pas été démarrée depuis plus de 3 mois est désactivée puis en est automatiquement supprimée au bout d'un an (la machine en elle-même fait alors référence à des mots de passe n'existant plus dans l'AD, voire à des comptes utilisateurs obsolètes). Une solution dans ce genre de cas peut être d'agir directement sur l'AD, mais le Service possédait également un outil (sous la forme d'une petite distribution «live» Linux pouvant être stockée sur 512Mo de mémoire sur un périphérique amovible) capable de contourner les mots de passe de sessions Windows, outil qui nécessitait toutefois d'être remplacé pour raison d'obsolescence (en effet, celui-ci ne fonctionnait qu'au maximum sous Windows 7, or la version de Windows standardisée sur toutes les machines de travail sous juridiction du Ministère de l'Intérieur est Windows 10). Étudier les différents outils disponibles était donc nécessaire et a été fait : parmi plusieurs autres possibilités, l'outil *Hiren's Boot CD PE*, système d'exploitation Windows 11 «Live» spécialisé dans l'administration système et/ou la récupération de données sous Windows, a été préféré pour sa spécialisation Windows et sa simplicité d'utilisation (au prix toutefois d'une taille plus élevée : «pesant» 3,07Go, celui-ci doit donc être hébergé sur un support amovible de 4Go minimum). Une documentation d'utilisation a été réalisée et plusieurs supports amovibles de démarrage ont été créés sur demande des services qui le nécessitaient.

[Merci de se référer à la Fig. D1 trouvable en Annexes (page 14), ainsi qu'à sa légende]

Toutefois, en ce qui concerne les limitations de l'outil (qui sont intrinsèques à cette catégorie d'outils de dépannage système via support amovible), celui-ci devient inopérant si le Firmware BIOS a été protégé par un mot de passe administrateur (le menu de démarrage (permettant de stipuler à la

machine de démarrer sur le support amovible plutôt que sur le disque interne) étant alors inaltérable par l'opérateur), et/ou si le disque interne a été précédemment crypté (les données se trouvant dessus, parmi lesquelles ladite base de données de comptes locaux, étant alors inaccessibles).

4.1.5 Sécurisation de Station Blanche

Une «station blanche» telle qu'imaginée dans le cahier des charges du Ministère de l'Intérieur et conseillée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est une machine dédiée à l'analyse antivirale de supports amovibles, afin d'agir comme un sas de décontamination et de prévenir tout risque d'infection au sein du réseau d'entreprise (rappelons que certains logiciels malveillants sont conçus pour être hébergés sur des périphériques de stockage amovibles et exécutés automatiquement au branchement de ceux-ci ; or, certains logiciels malveillants (tels que les vers informatiques ou «worms») étant tout à fait capables de se répliquer eux-mêmes sur les différentes machines du réseau, l'infection d'un réseau d'entreprise (qui plus est ministériel) pourrait avoir lieu à cause d'un support amovible et pourrait avoir des conséquences désastreuses (vol de données, mise en place de portes dérobées («backdoors») offrant des accès pérennes aux cybercriminels à travers le réseau, etc.)). Un modèle de station blanche fonctionnant sous Ubuntu (distribution Linux) et analysant automatiquement chaque support amovible branché au moyen de 2 antivirus différents (ClamAV, logiciel antivirus pour systèmes UNIX ; et Trellix, logiciel antivirus standardisé sur le réseau ministériel) venait d'être rendu opérationnel par Maël LESAICHERRE : toutefois, cette machine devait désormais pouvoir être sécurisée, c'est-à-dire faire en sorte que l'utilisateur de ladite station blanche ne puisse entreprendre aucune action pouvant porter atteinte au système d'exploitation de la machine ou bien au réseau en lui-même depuis ladite machine : tâche que j'ai assurée personnellement au moyen du jeu de commandes ci-dessous.

[Merci de se référer aux Figs. E1, E2, E3, E4, E5, E6, E7 et E8 trouvables en Annexes (page 15), ainsi qu'à leur légende]

4.2 Projet principal

4.2.1 Élaboration d'un Équipement Réseau sous pfSense et de son Écosystème de Production

Au sein de l'un des sites distants, une partie de l'infrastructure réseau (constituée notamment de deux équipements critiques devant impérativement bénéficier d'une connexion Internet pour fonctionner) dépend avant modification de la topologie décrite ci-dessous. La nature non-optimisée de cette topologie saute aux yeux (l'équipement réseau de secours doit être manuellement raccordé en cas de panne), c'est pourquoi le besoin pour un équipement réseau à 3 interfaces (LAN, WAN1 et WAN2) capable au minimum de réaliser l'équilibrage de charge entre lesdites Box (avec, en addition, le filtrage de flux selon une matrice prédéfinie afin de protéger davantage le LAN) est apparu.

[Merci de se référer à la Fig. F1 trouvable en Annexes (page 16), ainsi qu'à sa légende]

[Merci de se référer à la Fig. F2 trouvable en Annexes (page 16), ainsi qu'à sa légende]

En raison de problématiques de coût et de disponibilité rapide, il était impossible d'utiliser un matériel dédié (par exemple, un pare-feu STORMSHIELD qui serait en théorie tout à fait capable d'assurer l'équilibrage de charge précédemment décrit) : mais un équipement réseau peut tout à fait être créé à partir d'une station de travail obsolète aux spécifications matérielles revues (au moyen de systèmes d'exploitation gratuits, qu'ils soient polyvalents comme la distribution Linux Debian ou spécialisés dans la Protection par Pare-feu ou «Firewalling» comme la «distribution FreeBSD» pfSense), c'est ce qui a été fait à l'aide du matériel décrit ci-dessous (en plus d'une clé USB de démarrage pfSense requise pour l'installation, bien évidemment).

[Merci de se référer aux Figs. F3 et F4 trouvables en Annexes (page 17), ainsi qu'à leur légende]

Comme évoqué plus haut, dans l'optique de créer le matériel le plus résilient possible et avec le meilleur taux de survivabilité imaginable, les compétences acquises précédemment en matière de RAID ont été mises à profit de ce projet principal : l'équipement réseau, lors de son remontage, a été doté de deux disques distincts réglés lors de l'installation du système d'exploitation en «mirrorring ZFS» (exact équivalant du RAID 1 discuté précédemment, proposé nativement lors de l'installation de pfSense, et qui pourrait être étendu à davantage de disques pour une survivabilité encore meilleure) de façon à ce que le système reste opérationnel en cas de défaillance de l'un de ses supports de stockage (supports de stockage voués à être périodiquement vérifiés et au besoin remplacés par le personnel SIC du site, au moyen des commandes concernées inscrites dans la documentation utilisateur fournie avec les machines) ; en ce qui concerne le serveur TFTP, celui-ci a été doté lors de son remontage de 4 disques distincts (l'un hébergeant Debian et les trois autres mis en RAID 5 de façon à pouvoir héberger une grande quantité de sauvegardes de fichiers de configuration (afin de pouvoir au besoin revenir à n'importe quelle configuration précédente, comme décrit plus bas) tout en pouvant tolérer la panne de l'un des supports de stockage) (là encore, supports de stockage voués à être périodiquement vérifiés et au besoin remplacés par le personnel SIC du site, au moyen des commandes concernées inscrites dans la documentation utilisateur fournie avec les machines). Notons que l'idée initiale concernant le périphérique réseau (dont le système d'exploitation n'était au départ installé que sur un seul disque) était de créer, après avoir terminé sa configuration, une copie exacte de son disque dur au moyen de l'utilitaire Clonezilla, copie rebranchable manuellement à la place du disque initial en cas de défaillance de celui-ci ; toutefois, le système de fichiers ZFS utilisé par pfSense étant très spécifique et n'étant à priori pas pris en charge par Clonezilla, l'opération n'a eu pour seul effet que de corrompre le disque initial et de forcer le recommencement du projet (cette fois en «mirrorring ZFS» plus complexe à administrer mais beaucoup plus fiable).

Une fois la machine destinée à servir d'équipement réseau remontée, la prochaine étape consistait en sa sécurisation et en sa configuration, avant de s'intéresser aux problématiques de routage pour remplir le premier point du cahier des charges : le partage de charge entre les deux interfaces WAN.

[Merci de se référer aux Figs. F5, F6, F7, F8, F9, F10, F11 et F12 trouvables en Annexes (page 17), ainsi qu'à leur légende]

Parallèlement, à partir d'une Box Internet Orange Pro v3 de réserve identique à celles trouvables sur le site concerné, la procédure permettant de changer le réseau IP distribué en DHCP par celles-ci a due être étudiée et documentée (en effet, il était nécessaire que les deux interfaces WAN du nouvel équipement réseau soient sur des réseaux différents du réseau 192.168.1.0/24 déjà utilisé sur l'interface LAN du nouvel équipement réseau (les machines du LAN devaient impérativement rester sur cette plage IP, or le duplicata d'adresses sur un réseau IP est inimaginable car serait source de lourds problèmes de routage en plus d'une administration rendue drastiquement difficile) : la procédure de changement de réseau IP de l'interface LAN de la Box est très simple et requiert la configuration directe du DHCP, comme indiqué ci-dessous).

[Merci de se référer à la Fig. F13 trouvable en Annexes (page 20), ainsi qu'à sa légende]

Une fois le nouvel équipement réseau parfaitement capable de réaliser le routage des paquets comme indiqué précédemment, la prochaine étape consistait en la mise en place de règles de filtrage selon la matrice suivante incorporant les bonnes pratiques du «Firewalling» : «autoriser les connexions depuis le LAN sur les ports 22 TCP, 53 TCP/UDP, 80/81/443 TCP, 1883/8883 TCP et interdire les autres ; interdire toute connexion depuis les WANs», ce que qui a donné les tables de filtrage suivantes :

[Merci de se référer aux Figs. F14, F15, F16, F17 et F18 trouvables en Annexes (page 20), ainsi qu'à leur légende]

Une fois le filtrage de flux effectif, en addition, afin d'étoffer davantage le filtrage sur l'interface LAN (aucune connexion n'étant de toute façon permise depuis les interfaces WAN), le filtrage d'adresse IP de destination, de pays de destination et de contenu (c'est-à-dire de nom de domaine de destination) peut également être configuré via le paquet additionnel «pfBlockerNG» comme indiqué ci-après.

[Merci de se référer aux Figs. F19, F20, F21, F22, F23 et F24 trouvables en Annexes (page 22), ainsi qu'à leur légende]

[Merci de se référer aux Figs. F25 et F26 trouvables en Annexes (page 24), ainsi qu'à leur légende]

Une fois le paquet «pfBlockerNG» configuré de façon à assurer le filtrage additionnel au pur filtrage de flux configuré précédemment, la dernière étape avant d'obtenir une configuration solide, résiliente et répondant au cahier des charges imposé concernant notre équipement réseau et son écosystème de production, est l'automatisation de certaines tâches au moyen de l'utilitaire «Cron» sur notre équipement réseau ainsi que sur notre serveur de sauvegarde TFTP (dont la configuration est également décrite ci-dessous en même temps que les tâches «Cron» en elles-mêmes et la topologie finalement obtenue).

[Merci de se référer aux Figs. F27, F28, F29 et F30 trouvables en Annexes (page 24), ainsi qu'à leur légende]

[Merci de se référer à la Fig. F31 trouvable en Annexes (page 26), ainsi qu'à sa légende]

Finalement, en ce qui concerne les voies d'amélioration du projet, une configuration VPN permettant un accès distant au réseau interne du site pourrait s'avérer utile à des fins d'administration distante ; toutefois, ce point non-abordé dans le cahier des charges pourrait ajouter une vulnérabilité critique sur le nouveau réseau créé en plus de rajouter à coup sûr une nouvelle couche de complexité d'administration (complexité d'administration déjà prononcée en raison des nombreuses fonctionnalités physiques et logicielles ajoutées). De plus, l'ajout d'une fonctionnalité de Détection d'Intrusions / Prévention des Intrusions («Intrusion Detection System» / «Intrusion Prevention System» (IDS/IPS)) est disponible sur pfSense et tout à fait ajoutable sur le nouvel équipement réseau afin de sécuriser encore davantage le réseau interne (ceci n'a pas encore été fait par seuls problèmes de manque de temps et de rediscussion du cahier des charges initial). Enfin, l'ajout au réseau créé d'un clone de l'équipement réseau et leur fusion en un seul équipement virtuel à des fins de haute disponibilité (sur le même principe que le protocole HSRP étudié au programme de deuxième année de BUT) a été suggéré, mais refusé pour des raisons de hausse de complexité (un clone de l'équipement réseau sera donc créé et disposé à côté de l'équipement initial mais non raccordé au réseau et devant être branché manuellement en cas de panne du premier (sur le même principe que la redondance manuelle de Box Internet dans la topologie pré-modification)).

5 Conclusion

En conclusion, nous pouvons donc dire que ce stage a été une réussite sur tous ses aspects : m'ayant permis de développer de nouvelles compétences techniques (Administration serveurs et RAID, démontage et remontage matériel, etc.) comme comportementales (Intégration dans une équipe, Rapport à la hiérarchie, etc.), ou de renforcer durablement certaines déjà acquises (Administration systèmes et réseaux, configuration / déploiement / administration / maintenance / sécurisation / dimensionnement d'infrastructures réseaux, «Firewalling», etc. ; Assiduité, Rigueur, Ponctualité, etc.) ainsi que d'apporter une expérience concrète aux savoirs théoriques acquis au cours de mes deux premières années de BUT, ce stage s'est articulé autour de plusieurs projets (5 projets secondaires et 1 projet principal) de nature «touche-à-tout» et variés m'ayant permis de tester et développer ma nature polyvalente. Les objectifs ayant été fixés avant le stage comme devant impérativement être remplis par celui-ci (application des concepts théoriques et compétences techniques appris lors des deux premières années de BUT, développement de nouveaux savoirs et compétences techniques, assimilation d'une «culture d'entreprise», etc.) ont non seulement tous été remplis mais d'autres, non-prévus avant le départ en stage, ont également été complétés (mise à l'épreuve de la ponctualité, rigueur au travail, assiduité, etc.).

Première expérience professionnelle réelle permettant de découvrir en détail les rouages du fonctionnement d'une entreprise, ce stage aura indéniablement été d'une utilité sans pareille dans mon cursus, une étape cruciale de ma formation comme de mon développement. Sur le plan personnel, celui-ci m'aura permis d'apprendre énormément, que ce soit sur ma capacité à m'intégrer dans une entreprise et à m'adapter à un nouveau cadre, à travailler en équipe et à communiquer afin de maintenir une cohésion, à développer des qualités personnelles telles que la gestion du temps et des priorités, etc. ; tout en consolidant ma conviction d'avoir choisi la bonne voie professionnelle. Ce stage m'aura également permis d'ouvrir la porte à l'alternance de troisième année, d'autant plus riche en apprentissages et expériences que la longueur de l'immersion en entreprise est décuplée.

6 Remerciements

Premièrement, mes remerciements vont bien évidemment à Lionel MOURRE, qui a accepté de valider ma candidature et de me prendre en stage après un seul entretien en ne connaissant de moi que mon Curriculum Vitae (CV) et une lettre de motivation. Qui plus est, cette demande de stage s'est inscrite au cœur d'une période de forte tension tant sur le Service entier (Jeux Olympiques, élections, etc.) que sur lui-même (endossage temporaire du double rôle d'Adjoint au Chef de Service et de Chef du Bureau des Infrastructures), ce qui ne l'a toutefois pas non plus empêché d'accepter. Celui-ci a su faire confiance à des compétences techniques inscrites sur un CV et à une promesse tacite de rigueur et d'assiduité.

Deuxièmement, mes remerciements vont également à Maël LESAICHERRE, qui m'a épaulé dans mes projets et m'a permis de participer aux siens tout en m'apprenant chaque rouage de la machinerie préfectorale. Une collaboration qui me manquera indubitablement, et sans laquelle la période d'alternance sera incontestablement différente !

Troisièmement et plus largement, mes remerciements vont également bien sûr à l'ensemble de l'équipe du SINSIC, tous bureaux confondus. Tout a été fait afin que je sois à l'aise dans ce Service et que mon intégration y soit optimale, pour que ma compréhension des tâches réalisées (ainsi que de leurs tenants et aboutissants) soit claire et maximale (et, avec elle, le nombre de précieux enseignements que j'ai pu tirer de cette période de stage), pour que mes questions, interrogations et demandes d'assistance ne soient jamais sans réponse, pour que mes conditions de travail soient les plus faciles possibles (je pense notamment, concernant mon projet d'équipement réseau sous pfSense, à l'inépuisable réserve de matériel réformé du BENT ainsi qu'à leurs précieux conseils !). En bref, tous mes efforts se sont concentrés à être utile et efficace au sein de ce Service, et j'espère sincèrement que ceux-ci se sont avérés payants !

7 Glossaire

Active Directory et **Unités d'Organisation («Organisationnal Units (OUs)»)** : Service de gestion des identités et des accès développé par Microsoft, utilisé principalement dans les environnements Windows pour gérer et sécuriser les informations et les ressources réseau d'une organisation, facilitant ainsi l'administration et le contrôle des accès au sein d'un réseau d'entreprise. C'est une base de données centralisée permettant de stocker des informations sur les objets du réseau (utilisateurs, ordinateurs, groupes, etc.) et fournissant des fonctionnalités pour l'authentification, l'autorisation et la gestion des politiques de sécurité. L'Active Directory utilise une structure hiérarchique composée de domaines (collections d'objets tels que des utilisateurs, des groupes et des appareils, gérés par un même contrôleur de domaine et partageant une base de données de comptes et des politiques de sécurité), d'arbres (collections de domaines partageant un espace de noms contigu et étant liés hiérarchiquement), et de forêts (collections plus larges contenant un ou plusieurs arbres partageant une relation de confiance implicite), permettant une organisation logique et flexible des ressources. Au sein des domaines, les Unités d'Organisation (OUs) sont des conteneurs logiques utilisés pour structurer les objets de manière hiérarchique, facilitant la gestion et l'application de politiques spécifiques. Elles permettent aux administrateurs de déployer des politiques spécifiques, de déléguer des tâches administratives et de gérer efficacement les objets.

VPN («Virtual Private Network» ou «Réseau Privé Virtuel») : Technologie qui crée une connexion sécurisée et chiffrée entre un utilisateur et un réseau privé via Internet, permettant ainsi de masquer l'adresse IP de l'utilisateur et d'assurer la confidentialité des données transmises. Dans le cas des VPN d'accès distant, comme utilisés par les travailleurs distants de la Préfecture, cette connexion permet d'accéder à des réseaux distants comme s'ils étaient physiquement connectés. Contrairement aux VPN site-à-site, qui sont destinés à connecter des réseaux entiers, les VPN d'accès distant sont essentiels pour la sécurité des communications depuis des environnements publics ou non sécurisés, en protégeant les données des interceptions et en contournant les restrictions géographiques.

Développement «backend» ou «côté serveur» : Ensemble des activités de programmation et de gestion qui se concentrent sur les aspects non visibles d'une application, c'est-à-dire ceux qui se déroulent sur le serveur (création et gestion des bases de données, mise en œuvre de la logique métier, gestion des requêtes HTTP, authentification des utilisateurs, maintien de la sécurité des données, etc.) : assure le traitement des données et des services qui soutiennent les fonctionnalités de l'interface utilisateur tout en assurant la scalabilité et la performance de l'application en gérant efficacement les interactions entre le serveur, la base de données et l'interface utilisateur.

VLAN («Virtual Local Area Network» ou «Réseau Local Virtuel») : Technologie de réseau qui permet de segmenter un réseau physique en plusieurs réseaux logiques distincts au sein d'une même infrastructure matérielle. En créant des VLANs, les administrateurs réseau peuvent regrouper des équipements terminaux en fonction de leur fonction ou de leur emplacement sans tenir compte de leur position physique, ce qui améliore la gestion, la sécurité et l'efficacité du réseau. Les VLANs permettent d'isoler le trafic, limitant ainsi l'accès aux données sensibles et réduisant la congestion réseau en segmentant les domaines de diffusion.

Sécurisation par Pare-feu ou «Firewalling» : Technique de protection des réseaux informatiques consistant à utiliser un dispositif dédié nommé «pare-feu» (étant généralement dans les faits le même équipement que le routeur connectant le LAN concerné à Internet) pour filtrer le trafic réseau entrant et sortant en fonction de règles prédéfinies (un pare-feu analyse les paquets de données et bloque ou autorise les communications selon des critères de sécurité, empêchant ainsi les intrusions (accès non autorisés) et protégeant contre les cyberattaques).

Protocole de Routage : Ensemble de règles et de procédures utilisé par les routeurs pour échanger des informations sur la topologie du réseau et déterminer les chemins optimaux pour acheminer les paquets de données vers leurs destinations finales (permettent aux routeurs de communiquer entre

eux pour partager différentes informations (l'état et le statut des liaisons reliant les routeurs, les routes disponibles, etc.), ce qui leur permet de construire et de maintenir à jour des tables de routage dynamiques). De nombreux protocoles de routage existent, chacun possédant ses avantages et inconvénients selon les besoins spécifiques du réseau (taille, complexité, exigence en termes de rapidité, etc.).

Topologie Réseau : Disposition ou agencement physique et/ou logique (l'agencement physique désignant la disposition réelle des câbles et des équipements, tandis que l'agencement logique désigne la manière dont les données circulent et les dispositifs communiquent entre eux) des différents composants d'un réseau (les périphériques terminaux ainsi que les périphériques réseau, et les liens de communication qui les relient). Définit comment les différentes parties d'un réseau sont interconnectées et comment les données circulent entre lesdites parties.

Table de Routage : Base de données interne à un routeur qui contient des informations sur les routes réseau disponibles et les chemins vers différentes destinations (prochain routeur pour une certaine adresse de destination, coût de la liaison correspondante, etc.), afin de prendre des décisions sur l'acheminement des paquets de données (est mise à jour dynamiquement par les protocoles de routage ou configurée manuellement par les administrateurs réseau).

Administration systèmes et réseaux : Gestion et maintenance des systèmes informatiques et des infrastructures réseau d'une organisation : configuration, surveillance, mise à jour et sécurisation des serveurs, des postes de travail, des équipements réseau (comme les routeurs et les commutateurs), ainsi que des systèmes d'exploitation (les administrateurs système et réseau assurent également la gestion des utilisateurs et des permissions, la résolution des problèmes techniques, et l'optimisation des performances pour garantir une disponibilité continue et une efficacité opérationnelle des services informatiques).

Routeurs / Commutateurs : Équipements essentiels aux réseaux informatiques, aux rôles distincts mais complémentaires. Les routeurs sont des dispositifs qui connectent différents réseaux entre eux (parfois de différentes tailles : cas de la liaison entre réseaux locaux («Local Area Networks» ou LANs) et réseaux étendus («Wide Area Networks» ou WANs) au moyen de la translation d'adresses («Network Address Translation» ou NAT)) et dirigent le trafic de données entre ces réseaux en déterminant le chemin optimal pour chaque paquet de données à l'aide d'un adressage IPv4 ou IPv6. Les commutateurs (dans le cas des commutateurs de couche 2, contrairement aux commutateurs de couche 3 dont les ports peuvent agir au choix de l'administrateur comme des ports de routeur ou des ports de commutateur de couche 2), quant à eux, assurent la transmission efficace de trames de données entre les dispositifs connectés à un même LAN au moyen des adresses de Contrôle d'Accès au Support («Media Access Control» ou MAC) propres aux interfaces réseau de chaque appareil connecté. Sont respectivement représentés dans les schématisations réseau par les représentations suivantes :

Réseaux Locaux («Local Area Networks» ou LANs) / Réseaux Étendus («Wide Area Networks» ou WANs) : Types de réseaux informatiques différenciés par leur échelle et leur portée (les LANs couvrent une zone géographique restreinte, comme une maison, un bureau ou un campus, permettant la communication rapide et efficace entre les dispositifs connectés grâce à une infrastructure propre (qu'elle soit filaire ou sans-fil) en offrant des vitesses élevées et une faible latence pour le transfert de données internes ; tandis que les WANs s'étendent sur de vastes zones géographiques (interconnectant les LANs à travers des distances significatives pouvant aller jusqu'à l'échelle mondiale (au moyen de technologies de communication diverses comme les lignes téléphoniques, les

liaisons par satellite ou les fibres optiques) et étant donc essentiels à la communication entre réseaux éloignés) en offrant toutefois des vitesses plus lentes et avec une gestion de la latence plus complexe que les LANs.

Latence : Mesure généralement exprimée en millisecondes du temps écoulé entre l'émission d'une requête ou d'un signal et la réception de la réponse correspondante dans un système de communication (en d'autres termes, délai de propagation des données à travers un réseau ou un système pouvant être influencé par la distance physique entre les appareils, la congestion du réseau (en d'autres termes, la quantité de trafic), la qualité des équipements et des lignes de transmission, les protocoles utilisés, etc.) : critère essentiel pour évaluer la performance des réseaux informatiques, car influence directement la réactivité des applications et donc la qualité de l'expérience utilisateur.

Translation d'Adresses («Network Address Translation» ou NAT) : Technologie réseau utilisée pour modifier les adresses IP dans les paquets de données pendant qu'ils transitent entre un LAN et un WAN à travers un routeur : masque les adresses IP privées d'un réseau local en les remplaçant par une adresse IP publique unique lors des communications avec des réseaux externes. Technique largement utilisée pour conserver les adresses IP publiques et renforcer la sécurité en empêchant l'accès direct aux adresses internes depuis l'extérieur, tout en facilitant la connexion de multiples dispositifs internes à un réseau externe via une seule adresse IP publique (permet donc de pallier au problème de la restriction des adresses IPv4 disponibles).

Adresses de Contrôle d'Accès au Support («Media Access Control» ou MAC) : Identificateurs uniques attribués à chaque interface réseau ou périphérique réseau pour la communication sur les réseaux locaux (LANs) (chacune est codée en dur dans le matériel lors de la fabrication (et ne changera jamais ni ne sera obtenue dynamiquement à l'instar des adresses IP) et se compose de six paires de caractères hexadécimaux) : jouent un rôle crucial dans la transmission des données au niveau de la couche couche 2 du modèle OSI, permettant aux dispositifs de s'identifier et de communiquer directement entre eux sur un même LAN.

GNU/Linux : Système d'exploitation libre et open source (en d'autres termes, dont le code source est librement accessible, modifiable et redistribuable par tout utilisateur, favorisant ainsi la transparence, la collaboration et l'amélioration continue par la communauté) polyvalent (utilisé pour une large gamme d'applications, allant des serveurs aux ordinateurs personnels et aux appareils mobiles) composé du noyau Linux (le cœur du système d'exploitation responsable de la gestion des ressources matérielles et de l'exécution des tâches système tout en offrant une interface entre les logiciels et le matériel de l'ordinateur) et des logiciels du projet GNU.

Windows Server : Système d'exploitation spécialisé serveurs développé par Microsoft conçu pour gérer et administrer divers services (l'annuaire Active Directory, les services de fichiers, l'hébergement web, etc.).

Machines Virtuelles «Basées sur le Noyau» («Kernel-based Virtual Machine» ou KVM) : Technologie de virtualisation open source intégrée dans le noyau Linux permettant à celui-ci de fonctionner comme un hyperviseur (en d'autres termes, un logiciel qui permet de créer et de gérer des machines virtuelles («Virtual Machines» ou VMs) en isolant et en allouant les ressources matérielles d'un ordinateur physique pour permettre l'exécution simultanée de plusieurs systèmes d'exploitation sur une même machine).

Oracle VirtualBox : Logiciel de virtualisation open source qui permet aux utilisateurs de créer et de gérer des machines virtuelles de divers systèmes d'exploitation (Windows, Linux, Solaris, etc.) sur un ordinateur hôte, tout en offrant des fonctionnalités avancées en matière de clonage, de gestion des ressources réseau et de stockage, d'instantanés (ou «snapshots» : sauvegardes de l'état précis à un moment donné d'un système informatique permettant de revenir à cet état ultérieurement si nécessaire), etc.

Services (Réseaux) : Applications ou processus fournissant des fonctionnalités essentielles aux utilisateurs ou à d'autres systèmes via un réseau, et étant donc cruciaux pour le fonctionnement et l'interconnectivité des réseaux informatiques modernes (incluent par exemple le serveur web pour l'hébergement de sites internet, le serveur de messagerie pour la gestion des emails, le service de «serveur de noms» («Domain Name System» ou DNS) pour la résolution de noms en adresses IP, etc.).

Python : Langage de programmation interprété, de haut niveau et polyvalent, apprécié pour sa facilité d'apprentissage et sa flexibilité, connu pour sa syntaxe claire et concise qui facilite la lecture et l'écriture de code (est largement utilisé pour le développement web, l'analyse de données, l'automatisation des tâches, l'intelligence artificielle, etc.).

Bases de Données : Structures de données permettant de stocker, gérer et récupérer des données structurées de manière efficace : sont essentielles pour de nombreuses applications (de la gestion des informations d'entreprise à l'analyse des grandes quantités de données) et permettent de garantir l'intégrité, la disponibilité et la sécurité des informations.

Ethernet : Technologie de réseau local (LAN) standard qui permet la communication entre ordinateurs et autres périphériques sur un réseau filaire, via un média cuivré torsadé (ou à fibres optiques) capable de donner aux LANs leurs caractéristiques de grande vitesse de transmission de données et de faible latence.

Réseau Local Sans-Fil («Wireless Local Area Network» ou WLAN) : Technologie de réseau local (LAN) utilisant des ondes radio pour connecter les périphériques terminaux aux appareils réseaux (bornes sans-fil, le plus souvent elles-mêmes connectées au réseau Ethernet) plutôt que le média cuivre ou fibre d'Ethernet, permettant une mobilité accrue et une meilleure flexibilité de connexion en comparaison avec Ethernet (tout en posant toutefois des problématiques de sécurité nouvelles).

Redondance (Réseau) : Technique de conception des infrastructures de réseau visant à garantir la disponibilité et la fiabilité des services en cas de panne ou de défaillance d'un composant (implique la duplication des chemins de données, équipements critiques et connexions de façon à ce qu'une panne dans une partie du réseau soit transparente du point de vue des utilisateurs finaux et/ou n'affecte pas l'ensemble du système).

IP (IPv4 et IPv6) : Protocoles de communication utilisés pour l'adressage et le routage des paquets de données entre réseaux indépendants (principalement afin de pouvoir router les paquets de données à travers Internet). IPv4 utilise des adresses sur 32 bits, limitant le nombre d'adresses disponibles et conduisant donc à l'épuisement des adresses disponibles et au besoin de recourir à de la translation d'adresses (NAT). IPv6, en revanche, utilise des adresses sur 128 bits, offrant un nombre quasi illimité d'adresses uniques, ce qui permet de répondre à la croissance continue des appareils connectés (tout en introduisant également des améliorations en termes de sécurité, de gestion des flux de données et de simplification du routage).

Connexion Console (pour Équipements Réseau Administrables) : Méthode d'accès direct à la configuration et à la gestion des équipements réseau (tels que les routeurs et les commutateurs de tous niveaux, via un port physique dédié sur l'appareil et un câble spécifique relié à un ordinateur utilisant un logiciel d'émulation de terminal) souvent utilisée lors de la configuration initiale ou de la résolution des problèmes : permet aux administrateurs réseau d'interagir avec le système d'exploitation de l'équipement en dehors des interfaces réseau normales, offrant un contrôle total même en cas de dysfonctionnement des interfaces réseau standard.

Téléphonie sur IP («Telephony over Internet Protocol» ou ToIP) : Technologie largement adoptée par les entreprises pour son efficacité et sa flexibilité, permettant de transmettre des appels

téléphoniques via des réseaux informatiques en utilisant le Protocole Internet (IP) plutôt que les réseaux téléphoniques traditionnels (convertit la voix en paquets de données numériques qui sont ensuite envoyés sur un réseau IP utilisant donc la commutation par paquets de données, plus rapide que les circuits commutés de la téléphonie classique).

«Zones Démilitarisées» («De-Militarised Zones» ou DMZs) (d'un Pare-Feu) : Sous-région d'un réseau informatique spécifiquement conçue pour ajouter une couche supplémentaire de sécurité en isolant certaines ressources (typiquement les serveurs partagés entre les réseaux interne sécurisé et externe non-sécurisé (comme Internet)) des réseaux internes sensibles : permet de limiter l'accès direct des utilisateurs extérieurs aux ressources critiques de l'entreprise tout en permettant un accès contrôlé aux services qui doivent être exposés à Internet (serveurs Web, de messagerie, de transfert de fichiers, etc.)

Chiffrement et Déchiffrement de Supports de Stockage : Transformation des données stockées sur des dispositifs tels que des disques durs, des SSD, des clés USB, ou d'autres supports de stockage, en une forme illisible sans la clé de déchiffrement appropriée (via des algorithmes cryptographiques pour protéger la confidentialité des données contre les accès non autorisés), ainsi que son opération inverse. Traitement automatiquement réalisé sur les ordinateurs portables affectés aux travailleurs distants (en effet, pour toute entreprise, le préjudice en cas de perte ou de vol d'un tel appareil va bien au-delà de la valeur du matériel : des données confidentielles ou à diffusion restreinte pouvant potentiellement être présentes sur le disque de la machine peuvent être vendues voire rendues publiques sur Internet).

Microsoft Deployment Toolkit (MDT) : Ensemble d'outils et de processus fournis par Microsoft pour automatiser et simplifier le déploiement de systèmes d'exploitation et d'applications sur des ordinateurs (permet aux administrateurs système de créer des images de déploiement standardisées qui peuvent être facilement déployées via le réseau sur plusieurs machines, et donc d'automatiser l'installation d'OS comme Windows ainsi que de suites de logiciels prédéfinies).

Bande Passante : Quantité maximale de données en bits par seconde (bps) qui peut être transférée de manière efficace d'un point à un autre dans un réseau (indicateur clé de la performance du réseau : certaines applications requièrent une haute capacité de transfert de données (diffusion de vidéos en streaming et jeux en ligne, transferts de fichiers volumineux, etc.) et la bande passante disponible influencera directement l'expérience utilisateur sur ces applications). Peut être affectée par divers facteurs (qualité des équipements de réseau, type et qualité du câblage reliant ceux-ci, encombrement du réseau, etc.).

Taux de Perte de Paquets : Pourcentage de paquets de données qui sont envoyés mais ne parviennent pas à atteindre leur destination dans un réseau, par rapport au nombre total de paquets transmis : mesure essentielle pour évaluer la qualité et la fiabilité des communications réseau (une perte de paquets excessive peut entraîner des dégradations notables de la performance (interruptions de service, temps de réponse accrus, mauvaise qualité de transmission audio ou vidéo, etc.)) pouvant être influencée par divers facteurs (congestion du réseau, erreurs de configuration des équipements, interférences (concernant les transmissions sans-fil) ou diaphonie (concernant les transmissions filaires Ethernet), etc.).

Diaphonie : Phénomène d'interférence électromagnétique où un signal transmis sur un circuit électrique ou une ligne de communication (tels qu'un câble Ethernet) génère des perturbations indésirables dans un autre circuit physiquement proche, principalement à cause de la mécanique d'induction électromagnétique (possibilité de passage d'un premier conducteur à un second du courant généré dans un premier conducteur, à cause du champ magnétique généré autour du premier conducteur lors du passage dudit courant) : raison pour laquelle les câbles Ethernet blindés par une feuille d'aluminium («Foiled Twisted Pair» ou FTP) existent, et pour laquelle les paires de fils à l'intérieur des câbles Ethernet sont torsadées (le phénomène d'induction électromagnétique indésiré

entraîne une dégradation de la qualité du signal (introduction de bruit et de distorsions qui altèrent la clarté et la fiabilité des transmissions de données) pouvant affecter les lignes téléphoniques comme les réseaux informatiques).

Protocole Simple de Gestion Réseau («Simple Network Management Protocol» ou SNMP) : Protocole de communication standardisé utilisé pour surveiller et gérer les périphériques sur un réseau informatique (permet aux administrateurs de réseau de collecter des informations, de configurer des paramètres et de surveiller les performances des appareils réseau) : un logiciel Gestionnaire SNMP sur une machine d'administration envoie des requêtes (demandes d'informations précises) à Agent SNMP sur le périphérique à surveiller (suit donc une architecture respectivement client-serveur).

Cœurs de Processeur ou cœur de CPU («Central Processing Unit») : Unité de calcul indépendante au sein d'un processeur (chaque cœur peut avoir accès à des ressources partagées (telles que la mémoire cache) mais est capable d'exécuter des instructions et de traiter des tâches de manière autonome, ce qui permet à un processeur d'effectuer plusieurs opérations simultanément).

Firmware BIOS : Logiciel configurable intégré dans la mémoire non volatile de la carte mère d'une machine (assure le démarrage initial de celle-ci avec le chargement du système d'exploitation depuis le disque dur après l'auto-test et l'initialisation des composants matériels, assure la reconnaissance des périphériques connectés tels qu'un clavier, etc.). Bien que le terme «BIOS» soit souvent utilisé, les machines modernes peuvent également utiliser des alternatives telles que l'UEFI (Unified Extensible Firmware Interface), offrant des fonctionnalités étendues et un démarrage plus rapide.

PowerShell : Environnement de script et shell de ligne de commande développé par Microsoft, conçu pour la gestion et l'automatisation des tâches d'administration système et réseau et l'écriture de scripts avancés (intègre des «cmdlets» («command-lets») qui sont des commandes spécialisées pour effectuer des tâches administratives courantes (gestion des processus, manipulation de fichiers, configuration de systèmes, etc.)) : se distingue par sa capacité à utiliser des objets pour échanger des données entre les commandes, offrant ainsi une approche plus sophistiquée et flexible que les shells traditionnels basés sur le texte.

Bits de parité et opération «OU Exclusif» («XOR») en RAID : Les bits de parité sont des informations redondantes stockées sur les disques d'un système RAID, spécialement conçus pour assurer l'intégrité des données et permettre la reconstruction des informations en cas de défaillance de l'un des disques (ils sont calculés pour chaque ensemble de données réparties sur les disques selon l'opération «XOR» appliquée aux bits de données (cette opération est un type d'addition binaire où le résultat est 1 si le nombre de 1 est impair parmi les bits de données et 0 sinon), et permettent de reconstruire les bits de données perdus en cas de défaillance de disque grâce à une deuxième opération «XOR» entre eux et les bits de données restants).

Sauvegarde Incrémentielle : Méthode de sauvegarde des données qui ne sauvegarde que les modifications apportées depuis la dernière sauvegarde ayant eu lieu (réduit le temps nécessaire pour effectuer la sauvegarde et économise de l'espace de stockage, en comparaison de la sauvegarde complète qui sauvegarde toutes les données à chaque fois).

Ports (Réseaux) : Numéros de canaux logiques (étiquetés de 0 à 65535 avec les numéros inférieurs à 1024 réservés aux services système bien connus et aux protocoles spécifiques) utilisés pour identifier les applications et les services réseau à l'écoute de tentatives de connexions sur un périphérique hôte (sont essentiels pour permettre à plusieurs applications de fonctionner simultanément sur un même appareil). Les protocoles correspondants peuvent utiliser le protocole TCP (Transmission Control Protocol) pour les connexions fiables ou le protocole UDP (User Datagram Protocol) pour les connexions non fiables à faible latence.

Distribution Live (ou Système d'Exploitation Live) : Type de système d'exploitation qui peut être exécuté directement depuis un support amovible (CD, DVD ou clé USB), sans nécessiter d'installation préalable sur le disque dur de l'ordinateur (et donc l'effacement du système d'exploitation précédent) : est couramment utilisé pour la récupération de données, le diagnostic de matériel, les démonstrations de logiciels, etc.

Bombe à Processus («Fork Bomb») : Type d'attaque de déni de service qui exploite une vulnérabilité des systèmes d'exploitation multitâches, notamment sous UNIX et Linux (fonctionne en exécutant un script malveillant qui crée une chaîne de processus en boucle infinie, chaque processus générant d'autres processus à une vitesse exponentielle) : sature rapidement les ressources du système affecté, le rendant extrêmement lent ou totalement inutilisable et nécessitant souvent un redémarrage forcé pour rétablir son fonctionnement normal.

(Requête) «Ping» : Commande réseau qui permet de tester la connectivité entre deux périphériques au sein d'un réseau (fonctionne en envoyant une série de paquets-requêtes ICMP (Internet Control Message Protocol) «echo request» vers une adresse IP cible et en mesurant le temps qu'il faut pour recevoir une réponse «echo reply»).

Adresse de Diffusion ou «Broadcast» : Adresse réseau spéciale utilisée pour envoyer des paquets de données simultanément à tous les dispositifs d'un réseau local (permet de cibler tous les dispositifs dans un segment réseau spécifique, contrairement aux adresses IP qui identifient des hôtes individuels).

Équilibrage de Charge (ou «Load Balancing») : Technique de gestion du trafic réseau qui répartit efficacement les charges de travail ou les demandes de service sur plusieurs ressources ou serveurs pour optimiser les performances et garantir une haute disponibilité (permet de réduire le risque de surcharge d'une seule ressource en distribuant le trafic entrant de manière équilibrée) : permet notamment d'assurer une tolérance aux pannes en redirigeant le trafic vers des ressources disponibles en cas de défaillance d'une partie du système.

Matrice (de Flux) : Représentation structurée et organisée des flux de données à travers un réseau informatique (généralement définie comme un tableau ou une grille qui montre la direction et le volume des flux de données entre différents points du réseau) : permet d'analyser le trafic réseau, ce qui est notamment utile pour les administrateurs réseau et les spécialistes de la sécurité informatique lorsqu'un ensemble de règles de filtrage doit être défini.

FreeBSD : Système d'exploitation open source de type UNIX conçu pour fournir une base robuste, performante et sécurisée pour une large gamme d'applications (serveurs, postes de travail, etc.) et réputé pour sa stabilité et ses capacités réseau avancées ; inclut un noyau, des outils systèmes, ainsi qu'un ensemble complet de bibliothèques et d'applications. pfSense, au-delà d'être «une distribution spécialisée de FreeBSD», est une solution open source de pare-feu et de routeur basée sur ledit système d'exploitation FreeBSD (en d'autres termes, pfSense est construit sur FreeBSD et l'utilise donc comme noyau sous-jacent et tire parti de ses fonctionnalités de réseau et de sécurité).

Mémoire Vive («Random Access Memory» ou RAM) : Type de mémoire informatique essentielle au fonctionnement des systèmes électroniques (dite «mémoire volatile» : perd toutes les données qu'elle contient lorsque l'appareil est éteint, contrairement aux mémoires de stockage permanentes comme les disques durs), utilisée pour stocker temporairement les données et les instructions nécessaires au fonctionnement en cours des applications et du système d'exploitation, permettant un accès rapide et direct aux informations par le processeur.

Serveur de Protocole Trivial de Transfert de Fichiers («Trvial File Transfer Protocol» ou TFTP) : Serveur qui utilise le protocole TFTP (protocole réseau simple, conçu pour un transfert rapide et léger de fichiers, souvent utilisé pour le chargement d'images de démarrage ou la mise à

jour de firmware sur des périphériques réseau tels que les routeurs et les commutateurs ; fonctionne sans connexion persistante au moyen d'UDP) pour permettre le transfert de fichiers entre machines sur un réseau sans prise en compte de mécanismes de sécurité avancés tels que l'authentification ou le chiffrement (limite l'utilisation de TFTP à des environnements réseau sécurisés où la rapidité et la simplicité sont prioritaires).

SSH par Clé Publique : Méthode d'authentification sécurisée utilisée pour établir des connexions à distance via le protocole SSH (Secure Shell) reposant sur un système de cryptographie asymétrique utilisant une paire de clés publique et privée plutôt qu'un mot de passe demandé lors de la connexion (mot de passe sur lequel une attaque par force brute peut avoir lieu) : la clé publique est alors placée sur le serveur SSH et la clé privée conservée sur le client, puis, lorsqu'une connexion est initiée, le serveur utilise la clé publique pour générer un défi chiffré que seul le détenteur de la clé privée correspondante peut déchiffrer, prouvant ainsi son identité sans nécessiter de mot de passe.

Attaque par force brute (ou «bruteforce») : Méthode d'intrusion visant à accéder à des systèmes, comptes ou données protégés en essayant systématiquement toutes les combinaisons possibles de mots de passe ou de clés de chiffrement jusqu'à trouver la bonne (repose uniquement sur la puissance de calcul pour parcourir exhaustivement toutes les possibilités, contrairement aux formes d'attaques plus sophistiquées qui exploitent des vulnérabilités spécifiques ou des faiblesses logicielles), pouvant être extrêmement efficace contre les systèmes ou comptes utilisant des mots de passe faibles ou courts.

Service DHCP («Dynamic Host Configuration Protocol») : Protocole réseau permettant aux serveurs DHCP d'attribuer automatiquement et dynamiquement sur demande de machines clientes (périphériques terminaux, ressources partagées (imprimantes, etc.)) des informations de connexion réseau (adresse IP pour une durée («bail») défini et masque de sous-réseau associé, passerelle par défaut, etc.). Les adresses IP distribuables peuvent être extraites d'un ensemble («pool») ou bien définies statiquement par l'administrateur en cas de demande provenant d'une adresse MAC précise.

Fonctionnalité de Détection d'Intrusions / Prévention des Intrusions («Intrusion Detection System» / «Intrusion Prevention System» (IDS/IPS)) : Technologie de sécurité réseau conçue pour identifier, analyser et répondre aux menaces potentielles dans un système informatique (un IDS surveille les activités réseau ou système pour détecter des comportements suspects ou anormaux qui pourraient indiquer une tentative d'intrusion ou une attaque et alerte les administrateurs lorsqu'une menace est identifiée ; tandis qu'un IPS va plus loin en bloquant automatiquement les activités malveillantes identifiées, empêchant ainsi les intrusions en temps réel) utilisant des signatures de menaces connues et des analyses comportementales pour détecter et prévenir une large gamme d'attaques.

Protocole HSRP («Hot Standby Router Protocol») : Protocole de redondance conçu par Cisco pour garantir la disponibilité et la continuité de la connectivité réseau en cas de défaillance de routeur (permet la création d'un groupe de routeurs (vu par l'entièreté du réseau interne comme un seul et unique routeur virtuel) contenant un routeur principal actif et plusieurs autres routeurs en veille le surveillant et prêts à prendre sa place en cas de défaillance).

8 Bibliographie et Sitographie

Site officiel des Bouches-du-Rhône, mis à jour le 04/01/2023 «La zone de défense et de sécurité sud» [en ligne] [consulté le 18/06/2024] : https://www.bouches-du-rhone.gouv.fr/Services-de-l-Etat/La-zone-de-defense-et-de-securite-sud/La-zone-de-defense-et-de-securite-sud

Site officiel vie-publique.fr, mis à jour le 15/01/2024 «Quel est le rôle d'un préfet de région ?» [en ligne] [consulté le 18/06/2024] : https://www.vie-publique.fr/fiches/20170-quel-est-le-role-dun-prefet-de-region#:~:text=cumulant%20des%20pr%C3%A9rogatives%20r%C3%A9gionales,d%C3%A9concentr%C3%A9s%20r%C3%A9gionaux%20de%20l'%C3%89tat

Site officiel vie-publique.fr, mis à jour le 15/01/2024 «Quelle est la fonction d'un préfet ?» [en ligne] [consulté le 18/06/2024] : https://www.vie-publique.fr/fiches/20169-quelle-est-le-role-dun-prefet

Site officiel des Bouches-du-Rhône «Les sous-préfectures d'arrondissement» [en ligne] [consulté le 18/06/2024] : https://www.bouches-du-rhone.gouv.fr/Services-de-l-Etat/Les-sous-prefectures-d-arrondissement

Document CFDT du 30/04/2014 (PDF) [consulté le 15/06/2024] : https://smi-cfdt.fr/images/stories/Circulaire/SGAMI/fiche_SIC.pdf

Nicolas_W, le 05/10/2021 à 15:43 «Quels serveurs HPE ProLiant prennent en charge les différentes versions de Windows Server?» [en ligne] [consulté le 23/04/2024 et le 15/06/2024] : https://community.hpe.com/t5/blog-hpe-france/quels-serveurs-hpe-proliant-prennent-en-charge-les-diff%C3%A9rentes/ba-p/7133597?profile.language=fr