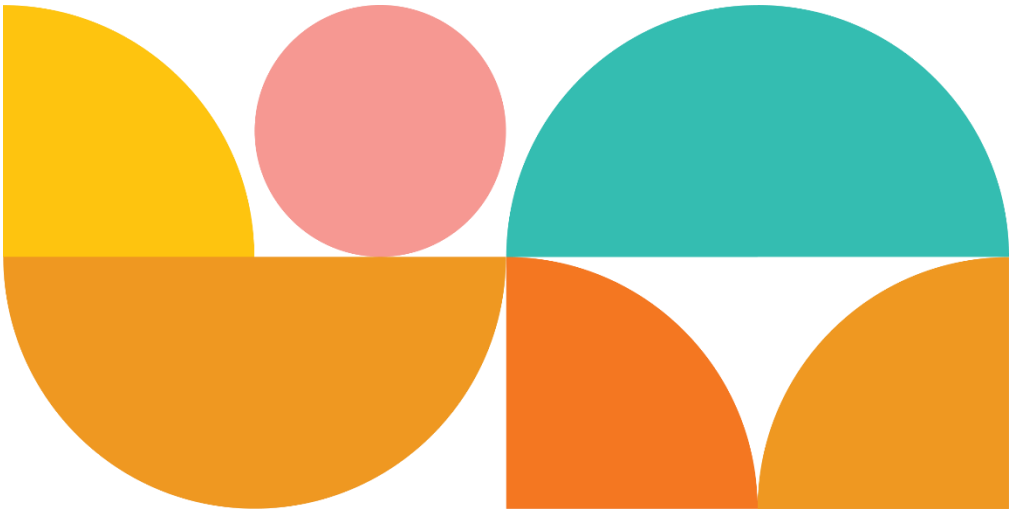
Cahier des charges

Projet simulation cyberattaque E5



BTS SIO Alternance 2ème année - option SISR

Sommaire :

Sommaire : 2

1. Contexte et Objectifs 4

1.1 Contexte 4

1.2 Objectifs 4

2. Expression des besoins 5

2.1 Entreprise ByteMeUp (BMU) 5

2.2 Entreprise Pare-Fouine 5

2.3 Entreprise Cloud Macronique 6

3. Solutions techniques pour répondre aux besoins exprimés 8

3.1 Entreprise ByteMeUp (BMU) 8

3.1.1 Schéma du réseau 8

3.1.2 Serveur de virtualisation 8

3.1.3 Contrôleur de domaine 9

3.1.4 Outil de Ticketing 9

3.1.5 Firewall 10

3.1.6 Sauvegardes 10

3.1.7 Wifi sécurisé public 10

3.1.8 Outil de supervision Zabbix 11

3.2 Entreprise Pare-Fouine (PF) 11

3.2.1 Équipements Réseaux et Sécurité 11

Pare-feu matériel Zyxel 11

Points d'Accès Wi-Fi Zyxel 12

NAS QNAP 12

Switch réseau gigabit administrable Planet XGS3-24042 12

Serveur de virtualisation 12

Serveur de Sauvegarde HyperV 12
3.2.2 Machines Virtuelles 13
Gestion du domaine et des utilisateurs 13
Supervision Zabbix 13
Déploiement centralisé WDS (Windows Deployment Service) 13
Hébergement du site web 13
Accès bureau à distance (Remote Desktop Service) 14
3.2.3 Logiciels et Outils 14
Zabbix 14
3.3 Entreprise CloudMacronique (CM) 15

1. Contexte et Objectifs

1.1 Contexte

Les entreprises ByteMeUp, Pare-Fouine et Cloud Macronique ont décidé de s'associer pour répondre à un appel à projet d'une agence gouvernementale de cybersécurité. Ce projet simulera une/des cyberattaques sur des infrastructures diverses. Chaque entreprise ayant son domaine de compétences, elles ont décidé de monter chacune une infrastructure spécifique à celles-ci. Ces infrastructures auront un accès sécurisé vers l'extérieur, les 3 infrastructures seront interconnectées entre elles.

- Pare-Fouine proposera une infrastructure avec des ressources accessibles depuis l'extérieur (serveur web et RDS) et un outil de supervision
- Cloud Macronique est spécialisé en réseau. Elle mettra en place une infrastructure avec un wifi sécurisé, un outil de supervision du réseau, un cœur de réseau et une segmentation réseau.
- ByteMeUp est spécialisée dans les infrastructures résilientes et les solutions de sauvegarde. Elle montera une infrastructure avec un serveur de production et un serveur de réplica qui inclura un outil de supervision, un accès wifi sécurisé.

L'objectif est de monter des infrastructures variées mais fonctionnelles afin tester la résilience et la sécurité de celles-ci. Cette attaque simulée doit évaluer leur capacité à réagir rapidement tout en minimisant les interruptions de service et la perte de données.

1.2 Objectifs

Pour chaque entité, il s'agit d'installer, configurer, mettre en service et sécuriser l'infrastructure informatique qu'elle est chargée de mettre en place en vue de la simulation de cyberattaque.

Les objectifs seront :

- De tester, d'un point de vue sécurité et résilience, les solutions habituellement mises en place chez les clients
- D'assurer la disponibilité de chaque infrastructure
- D'assurer l'interconnexion et la sécurité des échanges entre les infrastructures de chaque entité.

2. Expression des besoins

2.1 Entreprise ByteMeUp (BMU)

Dans le cadre de la simulation de cyberattaque, plusieurs composants clés de l'infrastructure de ByteMeUp seront testés. Le contrôleur de domaine est essentiel pour la gestion des identités et des droits d'accès. Il sera particulièrement visé par des tentatives de compromission d'administrateurs et d'escalade de privilèges, tests qui permettront de valider la robustesse des stratégies de sécurité. L'outil de ticketing sera évalué en termes de continuité des opérations et de gestion des incidents de sécurité, pour vérifier si les alertes sont correctement remontées et traitées. Le pare-feu sera mis à l'épreuve afin de mesurer sa capacité à bloquer les intrusions, à limiter les mouvements latéraux et à protéger les segments critiques du réseau. La solution de sauvegarde, avec des VM dans un VLAN DMZ et des sauvegardes externalisées, sera testée pour assurer une récupération rapide des systèmes critiques en cas d'attaque destructive ou de ransomware. Un réseau Wi-Fi sécurisé sera essentiel pour s'assurer qu'il n'est pas un point d'entrée facile pour les attaquants. Enfin, l'outil de supervision, comme Zabbix, jouera un rôle crucial dans la détection en temps réel des attaques et des anomalies sur le réseau, permettant une réaction rapide avant que les dégâts ne se propagent.

2.2 Entreprise Pare-Fouine

Dans le cadre du projet de simulation de cyberattaques Pare-Fouine plusieurs matériels essentiels sont mis en place pour garantir des infrastructures interconnectées, performantes et sécurisées. Le pare-feu Zyxel protégera les accès externes comme le serveur web et RDS grâce au filtrage de paquets, IDS/IPS et VPN, tout en défendant contre les attaques DDoS. Les points d’accès Zyxel offriront une connectivité Wi-Fi sécurisée avec WPA3, et leur gestion centralisée permettra de superviser le réseau sans fil, garantissant l'isolement des invités. Le NAS QNAP assurera le stockage sécurisé des données et des sauvegardes avec un accès à distance protégé et un support RAID pour éviter les pertes de données en cas de défaillance de disque. Le switch Planet XGS3-24042 segmentera le réseau via VLANs et optimisera le trafic critique grâce à la QoS, avec une sécurité renforcée par l’authentification 802.1X et les ACLs. Le serveur de virtualisation HyperV hébergera les VMs essentielles à l’infrastructure, avec redondance des disques et

clustering pour minimiser les interruptions. Le serveur de sauvegarde HyperV gérera les sauvegardes incrémentielles, assurant la restauration rapide des données après une attaque. Les VMs pour Active Directory et RDS permettront une gestion centralisée des utilisateurs, et la réplication d'AD garantira une continuité même en cas de panne. La VM Zabbix supervisera l'ensemble de l'infrastructure, détectant les anomalies de performance et générant des alertes en cas de menaces. La VM SRV-WDS facilitera le déploiement rapide des systèmes Windows après une attaque ou une panne. Le serveur web, hébergé dans la DMZ, assurera la gestion des services externes tout en étant isolé du réseau interne, renforçant ainsi la sécurité en limitant l'accès direct aux systèmes internes. Enfin, la VM pour RDS permettra un accès distant sécurisé aux bureaux des utilisateurs, un élément clé pour la continuité des opérations. Zabbix jouera un rôle central en surveillant l'infrastructure en temps réel, garantissant une réaction rapide aux incidents avant qu'ils ne causent des interruptions majeures.

2.3 Entreprise Cloud Macronique

Pour ce projet de simulation de cyberattaque, Cloud Macronique va proposer une infrastructure sécurisée spécialisée dans le réseau avec une segmentation, un cœur de réseau, un pare-feu, un wifi sécurisé, un outil de supervision réseau, un service de virtualisation, un service de contrôleur de domaine et d'un service de gestion de données.

La segmentation réseau servira à différencier et séparer la partie publique et administratif, pour permettre une meilleure sécurisation. La création d'un cœur de réseau garantira un routage efficace des données, assurant la haute disponibilité et la fiabilité du réseau. L'outil de supervision réseau jouera un rôle crucial pour prévenir les cyberattaques provenant de l'intérieur du réseau, permettant ainsi une intervention rapide. Un logiciel de surveillance réseau permettra aussi d'identifier rapidement les problèmes de performance, les pannes et les anomalies sur le réseau. En surveillant en temps réel l'état des équipements, le trafic et les connexions, il devient possible d'intervenir rapidement, de réduire les temps d'arrêt, et d'améliorer la fiabilité ainsi que la disponibilité du réseau.

Pour simuler une infrastructure d'entreprise nous mettrons en place un serveur centralisé grâce au service de virtualisation. Ce service accueillera le contrôleur de domaine qui attribuera automatiquement des adresses IP, les associera aux noms d'hôtes pour faciliter la communication interne et fera la gestion des utilisateurs. Le service de virtualisation intégra également une base de données dédié au stockage et au partage

des données, cela garantira la centralisation des données avec des droits d'accès spécifiques pour assurer confidentialité et sécurité. Le contrôleur de domaine et la base aurons une haute disponibilité grâce à la réplication de celle-ci.

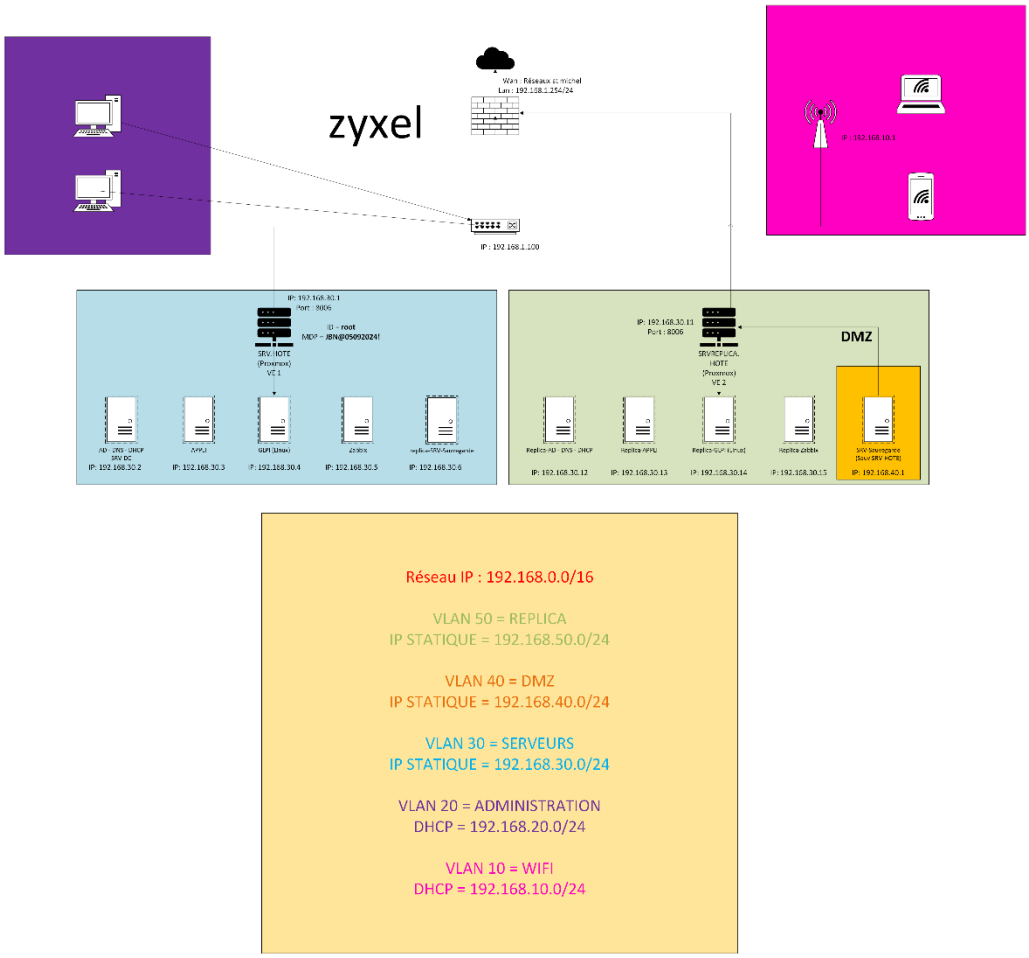
Un Wi-Fi sécurisé avec portail captif sera mis en place pour renforcer la protection du réseau contre les cyberattaques. Ce système exigera une authentification de chaque utilisateur avant l'accès au réseau, garantissant que seuls les utilisateurs autorisés pourront se connecter et accéder aux ressources internes, réduisant ainsi les risques d'intrusion.

En parallèle, un pare-feu performant sera installé pour filtrer les flux entrants et sortants, bloquant les menaces avant qu'elles ne puissent compromettre l'infrastructure. La surveillance continue du réseau permettra de détecter rapidement toute anomalie ou tentative d'intrusion, assurant ainsi une réponse rapide et efficace face aux cyberattaques extérieures.

3. Solutions techniques pour répondre aux besoins exprimés

3.1 Entreprise ByteMeUp (BMU)

3.1.1 Schéma du réseau



3.1.2 Serveur de virtualisation

Dans le cadre des solutions techniques pour le serveur de virtualisation, deux serveurs physiques seront utilisés : un HP ProLiant DL380p Gen8 pour le serveur hôte et un Dell PowerEdge R420 pour le serveur replica, tous deux exécutant Windows Server 2019 avec Hyper-V. Cette configuration permettra de créer des machines virtuelles (VM) pour

les différents serveurs nécessaires à l'infrastructure. Le serveur hôte sera situé sur le VLAN Serveurs, tandis que le serveur replica sera positionné sur le VLAN Replica. Cette architecture assurera une gestion efficace des ressources virtualisées tout en garantissant une redondance et une disponibilité accrues des services déployés.

3.1.3 Contrôleur de domaine

Pour répondre aux besoins de gestion centralisée des utilisateurs et des services réseau, la solution technique repose sur la mise en place d'un contrôleur de domaine hébergé sur une machine virtuelle (VM) sous Windows Server 2019. Cette VM intégrera plusieurs services essentiels, dont Active Directory pour la gestion des utilisateurs, des groupes et des permissions. Le service DNS assurera la résolution des noms de domaine, tandis que DHCP prendra en charge l'attribution dynamique des adresses IP. Enfin, Remote Desktop Services (RDS) sera utilisé pour permettre un accès distant sécurisé aux ressources de l'entreprise. Cette architecture VM sous Windows Server 2019 garantit une gestion efficace, une sécurité renforcée, et une haute disponibilité des services réseau.

3.1.4 Outil de Ticketing

L’outil de ticketing, GLPI sera hébergé sur une machine sous Linux, avec un système Ubuntu ou Debian. Pour assurer son fonctionnement optimal, un environnement LAMP (Linux, Apache, MySQL/MariaDB, PHP) sera mis en place, permettant à GLPI d'opérer en tant qu’application web. Cette configuration inclut Apache comme serveur web, MySQL/MariaDB pour la gestion de la base de données, et PHP pour le traitement des requêtes. De plus, l'intégration de GLPI avec l'Active Directory (AD) de l'entreprise sera mise en œuvre afin de synchroniser les utilisateurs et de faciliter l'authentification ainsi que la gestion des comptes. Enfin, le plugin FusionInventory sera installé pour automatiser la gestion de l'inventaire des équipements. Une GPO (Group Policy Object) sera également créée pour déployer automatiquement l’agent FusionInventory sur les postes utilisateurs, permettant ainsi une remontée efficace des informations sur le matériel et les logiciels dans GLPI. Cette approche garantira une gestion centralisée et efficace des incidents, tout en assurant une visibilité complète sur l'inventaire des ressources.

3.1.5 Firewall

Le pare-feu Zyxel USG 100 sera configuré pour assurer une protection robuste du réseau. La première étape consistera à configurer les interfaces WAN et LAN afin d'établir la connectivité réseau. Ensuite, des règles de filtrage seront créées en fonction des besoins spécifiques des serveurs, permettant de contrôler le trafic entrant et sortant de manière efficace. Pour renforcer la sécurité, une DMZ (zone démilitarisée) sera mise en place pour accueillir les sauvegardes d'une machine virtuelle. Cette configuration garantira une protection adéquate des données tout en permettant un accès contrôlé aux ressources nécessaires, réduisant ainsi le risque d'intrusion et améliorant la sécurité globale de l'infrastructure.

3.1.6 Sauvegardes

Dans le cadre des solutions de sauvegarde, une VM sera créée sur le serveur replica, utilisant OpenMediaVault comme système d'exploitation. Cette VM sera chargée de gérer les sauvegardes des machines virtuelles du serveur hôte. Pour renforcer la sécurité de l'infrastructure, la VM de sauvegarde sera positionnée dans une DMZ. Les sauvegardes seront également envoyées vers un NAS QNAP situé en externe. Cette configuration garantit non seulement la protection des données sensibles, mais aussi un accès contrôlé aux ressources de sauvegarde, tout en maintenant une séparation adéquate entre le réseau interne et les environnements externes.

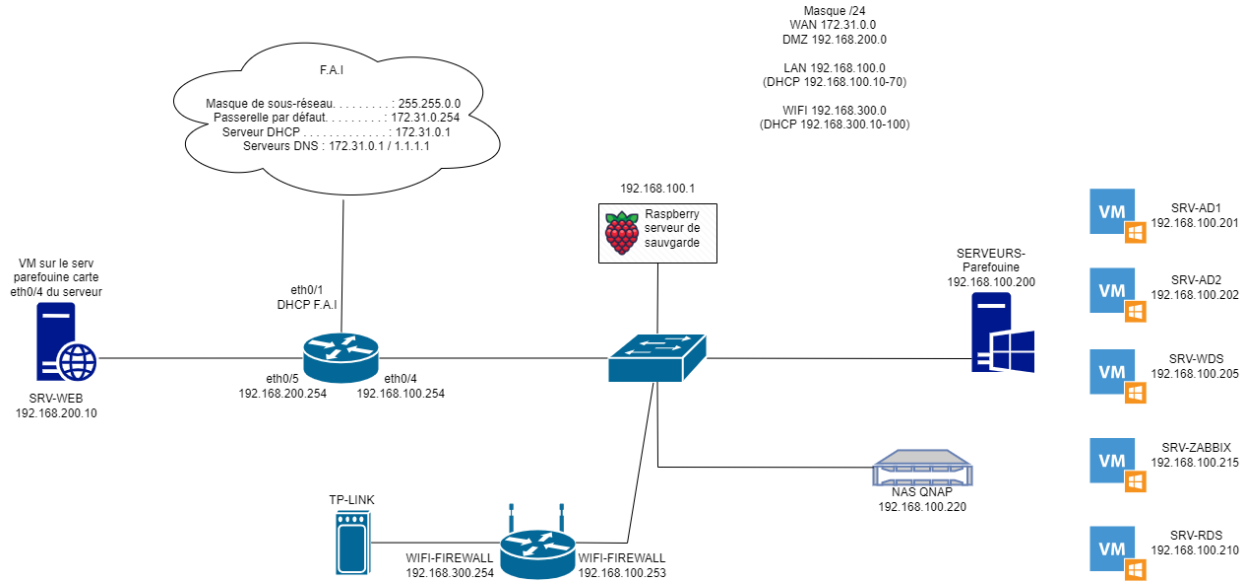
3.1.7 Wifi sécurisé public

Pour assurer un accès sécurisé au wifi public, un portail captif basé sur un serveur RADIUS sera mis en place. Il sera hébergé sur une machine virtuelle utilisant Windows Server. Ce serveur permettra de définir des utilisateurs avec des identifiants stockés dans sa base de données. Les utilisateurs se connecteront au réseau via un point d'accès Zyxel USG40W, où ils devront entrer leurs identifiants pour accéder au Wi-Fi. Cette approche garantira une authentification robuste et un contrôle d'accès efficace, tout en offrant une expérience utilisateur simplifiée pour les invités.

3.1.8 Outil de supervision Zabbix

L'outil de monitoring sera mis en place sur une machine virtuelle utilisant un système d'exploitation Linux. Les agents Zabbix seront installés sur les serveurs à surveiller, permettant une collecte efficace des données. Les hôtes seront ajoutés dans l'interface de Zabbix, et des templates de supervision adaptée seront appliqués pour personnaliser le suivi des performances. De plus, des déclencheurs et alertes seront configurés afin de notifier l'équipe en cas de problème détecté, garantissant ainsi une réactivité rapide et une gestion proactive des incidents. Cette approche permettra d'assurer une visibilité complète sur l'état de l'infrastructure et d'optimiser la disponibilité des services.

3.2 Entreprise Pare-Fouine (PF)



3.2.1 Équipements Réseaux et Sécurité

Pare-feu matériel Zyxel

Filtrage de paquets, IDS/IPS, gestion VPN, protection DDoS.
Interface web pour la configuration et les rapports.

Haute Disponibilité : Support de la configuration en cluster pour la redondance.

Points d’Accès Wi-Fi Zyxel

Gestion centralisée, réseaux invités, roaming.
Sécurité : WPA3, filtrage des adresses MAC.

NAS QNAP

Serveur de stockage en réseau (NAS).
QNAP avec support pour RAID et disques durs internes.
Capacité minimale de 4 To (extensible).
Partage de fichiers, sauvegardes, accès à distance.
Interface web, gestion des utilisateurs, et droits d'accès.

Switch réseau gigabit administrable Planet XGS3-24042

24 ports Gigabit Ethernet.
QoS, gestion VLANs, agrégation de liens.
Authentification 802.1X, ACLs.

Serveur de virtualisation

Serveur de Virtualisation HyperV rackable
CPU : Min. 8 cœurs.
RAM : Min. 48 Go.
Stockage : HDD/SSD, min. 500go.
Fonctions : HyperV, gestion LXC, clustering.
Connectivité : Réseau gigabit, redondance des disques.
OS : Windows Server 2019

Serveur de Sauvegarde HyperV

Serveur NAS.
Stockage : HDD, min. 5 To.
Fonctions : HyperV Backup Server, sauvegardes incrémentielles.

Intégration : Compatible avec HyperV pour gestion centralisée des sauvegardes.

3.2.2 Machines Virtuelles.

Gestion du domaine et des utilisateurs

2 VM Active Directory Répliqué sous HyperV VE avec les spécifications suivantes :

- CPU : 4 vCPU.
- RAM : 6 Go.
- Stockage : 130 Go.
- OS : Windows Server 2019.

Supervision Zabbix

1 VM sous HyperV VE avec les spécifications suivantes :

- CPU : 2 vCPU.
- RAM : 4 Go.
- Stockage : 100 Go.
- OS : Linux Debian 12.

Déploiement centralisé WDS (Windows Deployment Service)

1 VM sous HyperV VE avec les spécifications suivantes :

- CPU : 2 vCPU.
- RAM : 6 Go.
- Stockage : 130 Go.
- OS : Windows Server 2019.

Hébergement du site web

1 VM sous HyperV VE avec les spécifications suivantes :

- CPU : 2 vCPU.
- RAM : 4 Go.
- Stockage : 80 Go.
- OS : Ubuntu 24.04

Accès bureau à distance (Remote Desktop Service)

1 VM sous HyperV VE avec les spécifications suivantes :

- CPU : 2 vCPU.
- RAM : 6 Go.
- Stockage : 80 Go.
- OS : Windows Server 2019

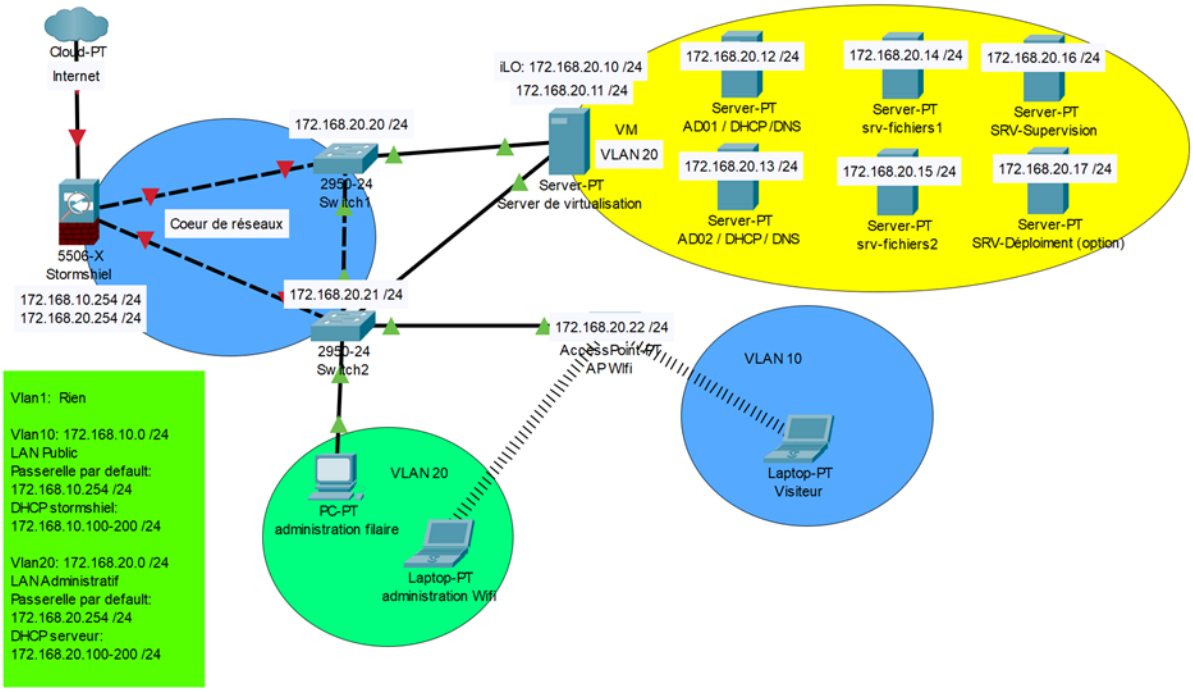
3.2.3 Logiciels et Outils

Zabbix

Surveillance en temps réel, alertes, collecte de performance.
Interface : Web pour gestion et configuration.
Intégration : Avec pare-feu, IDS/IPS, et autres équipements pour supervision complète et sous Linux.

3.3 Entreprise CloudMacronique (CM)

3.3.1 Schéma de l’infrastructure



3.3.2 Virtualisation

Les machines virtuelles nécessaires au fonctionnement de l’infrastructure seront hébergées sur un serveur de virtualisation HP… avec l’outil de virtualisation de Windows Server 2022 Hyper-V. Les machines virtuelles tourneront également sous Windows Server 2022.

3.3.3 Segmentation réseau

La solution consiste à mettre en place deux VLAN distincts : un VLAN Administration où se trouveront les serveurs avec l’AD, serveur de fichier etc … et un VLAN Visiteur avec un wifi mis en place ou ils auront accès qu’à internet, ceci servira à séparer les trafics et renforcer la sécurité du réseau. Deux switches seront déployés et configurés pour gérer ces VLAN, en assurant l'isolation des communications entre les deux segments.

Les switches seront interconnectés pour permettre la communication et assurer la redondance. Chaque switch sera ensuite relié au pare-feu, qui jouera le rôle de routeur entre les VLANs, gérant ainsi le routage des données et appliquant les règles de sécurité nécessaires. Cette solution garantira une segmentation efficace du réseau, une gestion optimisée du trafic, et une meilleure protection des ressources internes.

3.3.4 Surveillance réseau

La solution de surveillance réseau sera gérée à partir du logiciel Zabbix, installé sur une machine virtuelle en linux hébergée sur un serveur interne. Zabbix sera configuré pour surveiller les équipements réseau, tels que les switches, les serveurs, et le pare-feu, en collectant des données via SNMP ou ICMP. Des alertes en temps réel seront configurées pour signaler toute anomalie ou panne. Cette approche permettra d'assurer un suivi continu de la performance et de la disponibilité du réseau, facilitant ainsi la détection rapide des problèmes et l'optimisation de l'infrastructure réseau.

3.3.5 Wi-Fi sécurisé avec portail captif

Le **Stormshield SN900** permet de sécuriser l'accès au réseau Wifi en mettant en place un portail captif. Ce portail redirige les utilisateurs vers une page d'authentification avant qu'ils ne puissent accéder à Internet. Les sessions utilisateurs sont enregistrées dans des logs pour un suivi précis des connexions, et des comptes temporaires peuvent être créés.

3.3.6 Filtrage des flux

Le **Stormshield SN900** est configuré pour filtrer les flux entrants et sortants grâce à des règles précises basées sur les adresses IP, les ports et les protocoles. Il intègre un système IDS/IPS qui analyse le trafic en temps réel, détecte le s comportements suspects et bloque automatiquement les menaces potentielles, assurant une protection active contre les cyberattaques.

3.3.7 Supervision du réseau

Le **Stormshield SN900** offre des outils de monitoring en temps réel, permettant de suivre les activités réseau via un tableau de bord interactif. En cas d’anomalie, des alertes

automatiques sont générées pour permettre une réaction rapide. Les rapports d'audit et d'activité fournissent une vue détaillée du réseau, facilitant ainsi la gestion proactive de la sécurité.

3.3.8 Contrôleur de domaine

Les services AD, DHCP, et DNS seront installés sur le contrôleur de domaine. L'Active Directory (AD) permettra une gestion centralisée des utilisateurs et des groupes, avec des politiques de sécurité uniformisées qui sera mis en place avec des GPO (Stratégie de groupe) et une authentification renforcée. Le service DHCP attribuera automatiquement des adresses IP aux appareils, simplifiant la gestion réseau et évitant les configurations manuelles. Le DNS associera les adresses IP précédemment assigné à des noms d'hôtes (Nom de poste, serveur, imprimantes, ect...), facilitant ainsi la gestion interne entre les machines. Ces services seront répliqués sur une seconde machine virtuelle pour garantir une haute disponibilité et assurer la continuité des opérations en cas de panne d'une VM.

3.3.9 Serveur de fichiers partagés

Une VM sera dédiée au stockage, à la gestion et au partage des données au sein du réseau. Ce serveur centralisera tous les fichiers de l'entreprise, permettant un accès simplifié et une collaboration en temps réel entre les utilisateurs. Des droits d'accès spécifiques seront définis pour chaque utilisateur ou groupe lié au service AD afin de garantir que seules les personnes autorisées puissent consulter et/ou modifier les fichiers, assurant ainsi la confidentialité des informations sensibles. Des stratégies de sécurité, comme le chiffrement des données seront appliquées pour prévenir toute perte ou altération des fichiers et renforcer leur protection globale. Ce serveur de fichier sera répliqué sur une autre VM pour garantir ainsi une haute disponibilité et assurer la continuité des opérations en cas de panne d'une VM.

Délais

Les 3 infrastructures seront opérationnelles pour le début du projet de cyberattaque prévu en mai 2025.