AP-2

Classe : BTS SIO 25.1A

Nom : Anthony, Smail & Rayan

- Contexte de la situation professionnelle

La Maison des Ligues (La M2L), établissement du Conseil Régional de Lorraine, a pour mission de fournir des espaces et des services aux différentes ligues sportives régionales et à d'autres structures hébergées. La M2L, doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées.

- Besoin

Constamment sur ses gardes en matière de lutte contre les virus, la M2L nous demande de permettre de surveiller le trafic sur le réseau afin de protéger les utilisateurs de la M2L.

Recensement et identification des ressources numériques :

Réseau interne M2L

- 1 modem

Réseau interne (rose) :

- 2 appareille (PC)
- 1 serveur
- 2 switches
- 1 borne
- 1 routeur

Réseau DMZ (jaune) :

- 1 switch
- 1 Serveur

Réseau internet (bleu) :

- 1 modem
- 1 cloud operateur
- 1 routeur
- 2 serveurs
- 1 PC

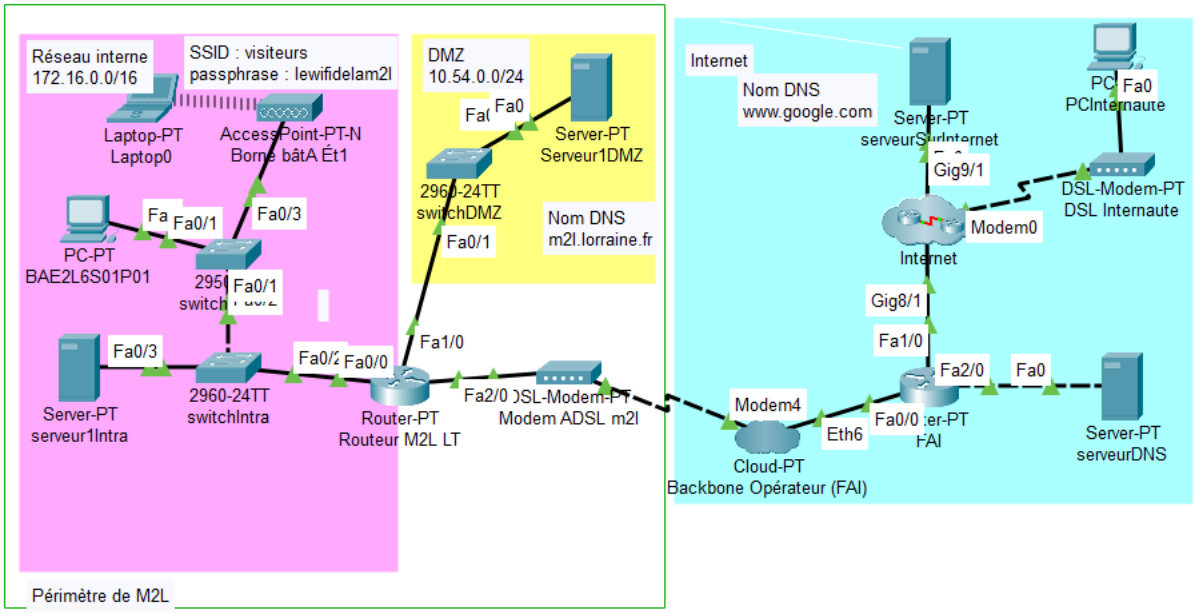


Table des matières

1- Problématique

Problématiques auxquelles les solutions doivent répondre :

Surveillance du parc :

Comment maintenir à jour et surveiller un parc informatique ?

Cette mission consiste à exploiter un ensemble de logiciels de configuration afin de :

- Vérifier que l'ensemble des postes (et notamment ceux des ligues) sont bien à jour au niveau de la sécurité (applications, système et antivirus).
- Répertorier les logiciels nécessitant une licence payante et vérifier l'existence de celle-ci.
- Lister les différentes versions des logiciels bureautiques installées sur les postes administratifs et procéder, dans la mesure du possible, à une homogénéisation des versions.
- Repérer les matériels en fin de garantie.
- Gérer les incohérences dans le parc comme un même nom d'hôte ou une même adresse IP.
- Vérifier si les postes installés dans la salle multimédia permettent de répondre aux nouveaux besoins (matériels et logiciels).
- Repérer les éléments d'interconnexion réseau et leur attacher de la documentation.

Pare-feu :

Comment protéger un réseau d’entreprise interne ?

Cette mission consiste à exploiter un ensemble de logiciels de configuration afin de :

- Sécurisation du réseau : Utilisez pfSense pour protéger votre réseau contre les menaces en configurant des règles de pare-feu, en bloquant les ports non utilisés et en mettant en place un filtrage de contenu.
- VPN (Virtual Private Network) : Configurez un serveur VPN avec pfSense pour permettre aux utilisateurs distants de se connecter de manière sécurisée au réseau interne, offrant ainsi un accès sécurisé aux ressources réseau même depuis l'extérieur.
- Bilan de bande passante : Surveillez l'utilisation de la bande passante sur votre réseau grâce aux outils intégrés de surveillance de trafic de pfSense. Identifiez les applications ou les périphériques qui consomment le plus de bande passante et ajustez en conséquence.
- Filtrage de contenu : Utilisez pfSense pour mettre en place des politiques de filtrage de contenu, que ce soit pour limiter l'accès à certains sites web ou pour

bloquer des types spécifiques de contenu, comme les annonces ou le contenu potentiellement malveillant.
- Sécurisation des connections Wi-FI : Configurez PfSense pour gérer l'accès Wi-Fi à votre réseau en mettant en place des réseaux VLAN (Virtual LAN) pour séparer le trafic, en utilisant WPA2-Enterprise pour une authentification sécurisée, et en appliquant des règles de pare-feu spécifiques aux réseaux sans fil.
- Surveillance et journalisation : Utilisez les fonctionnalités de journalisation de Pfsense pour surveiller l'activité du réseau, identifier les tentatives d'intrusion et générer des rapports sur l'utilisation et les performances du réseau.

2- Prérequis

Le matériel nécessaire pour la mise en place de Zabbix sera :

- Un serveur

Prérequis pour la mémoire

ZABBIX requiert à la fois de la mémoire physique et de la mémoire disque. 128 MB de mémoire physique et 256 MB d'espace disque libre peuvent être suffisant. Cependant, la valeur de la mémoire disque requise dépend évidemment du nombre d'hôtes ainsi que des paramètres qui seront supervisé.

Pour la sécurité du parc informatique, un pare feu sera mis en place ainsi qu'un système de prévention d'intrusion IPS/IDS et une solution contre les antivirus et antimalware.

Le Matériel nécessaire pour la mise en place de Nagios sera :

- Nagios XI nécessitee l'installation de certaines dépendances logicielles telles que PHP, Apache, MySQL/MariaDB etc

- Licence Nagios XI

- Système d'exploitation : Nagios XI est compatible avec plusieurs distributions Linux, notamment CentOS, RHEL (Red Hat Enterprise Linux) etc.

- Processeur

- Mémoire RAM

- Pour les petites installations : Au moins 4 Go de RAM.

- Pour les installations moyennes à grandes : Entre 8 Go et 16 Go de RAM.

- Une quantité d'espace disque de 20 Go ou plus est généralement recommandée

Mise en place d'un pare-feu (pfsense) :

Attention à avoir le matériel nécessaire (RAM ET CPU) selon notre charge de trafic, une zone internet et externe (DMZ)
Il faudra aussi configurer minutieusement les règles du pare-feu pour une bonne sécurité du réseau
Et faire des mises à jour constante pour éviter les failles de sécurité (Maintenance)

Le matériel nécessaire sera :

Un Routeur Cisco (Pare-feu matériel)
Routeur Cisco (Pare-feu logiciel pfsense)
Processeur compatible amd64 (x86-64) 64 bits
1 Go ou plus de RAM
Disque dur de 8 Go ou plus (SSD, disque dur, etc.)
Une ou plusieurs cartes d'interface réseau compatibles
Clé USB amorçable ou lecteur optique haute capacité (DVD ou BD) pour l'installation initiale

Mise en place d'un pare-feu (Checkpoint Firewall) :

Prérequis de checkpoint :

- CPU Intel Pentium Processor E2140

- Memory 4 GB

-Available Disk Space 2 GB

3- Solutions proposées

- Proposition de solution

Nous souhaitons mettre en place des moyens de surveillance du parc réseau (logiciel tel que Zabbix ou pare-feu/système d'exploitation comme pfSense) pour surveiller les trames, le matériel et pouvoir être alerter de problème via des notifications.

Surveillance du parc :

L'utilisation de zabbix un outil de surveillance open-source sera utilisé, celui-ci nous permettra de surveiller les serveurs et les réseaux.
Zabbix nous permettra de surveiller
- LE CPU
- La mémoire (RAM)
- L'espace disque
- Le trafic réseau

Celui-ci nous permettra de mettre en place un système de notification pour nous alertez en cas de problème.

Avec Nagios XI : Surveillance de l'infrastructure : Nagios XI permet de surveiller l'état et les performances des serveurs, des commutateurs, des routeurs, des appliances réseau, des périphériques de stockage et d'autres composants matériels.

Il offre la possibilité de surveiller les services critiques tels que les serveurs de messagerie, les bases de données, les applications web, les services cloud, etc., en vérifiant régulièrement leur disponibilité et leurs performances.

nagios XI peut envoyer des notifications d'alerte en temps réel via divers canaux tels que le courrier électronique, les SMS, les messages instantanés, etc., dès qu'une anomalie est détectée, ce qui permet aux administrateurs de prendre des mesures correctives rapidement.

Il permet de planifier et de gérer les périodes de maintenance pour éviter les fausses alertes pendant les opérations de maintenance planifiées.

La particularité de pfsense :

Le rôle du pare-feu permettra le filtrage du trafic, la protection contre les menaces informatique, la journalisation et rapports (log) et la segmentation du réseau.
Dans le réseau nous mettrons un pare-feu matériel CISCO ASA (première ligne de défense entre LAN ET WAN) et un pare-feu logiciel pfsense (qui gérera le trafic interne)

- Filtrage de trafic
- VPN
- Système de prévention/détection d'intrusion IDS/IPS
- Haute disponibilité
- Equilibrage de charge
- Portail captif
- Reporting et monitoring

Les avantages de pfsense :

- Flexibilité
- Personnalisation

L'avantage d'un pare-feu matériel et d'un pare-feu logiciel :

- Sécurité accrue
- Redondance
- Filtrage fin
- Gestion des politiques de sécurité.

Checkpoint FireWall :

Checkpoint Next Generation Firewall (NGFW) : Il offre une protection contre les menaces avancées grâce à des fonctionnalités telles que l'inspection en profondeur des paquets, la prévention des intrusions, le contrôle d'accès et la gestion unifiée des menaces.

Cette solution offre une protection avancée contre les menaces les malwares et les attaques ciblées en utilisant une analyse avancée

Une solution de sécurité unifiée qui intègre la protection des terminaux, du réseau, des applications et des données pour offrir une visibilité et un contrôle complets sur toutes les menaces.

4- Détails de l’intervention

- Démarche pour la mise en place :

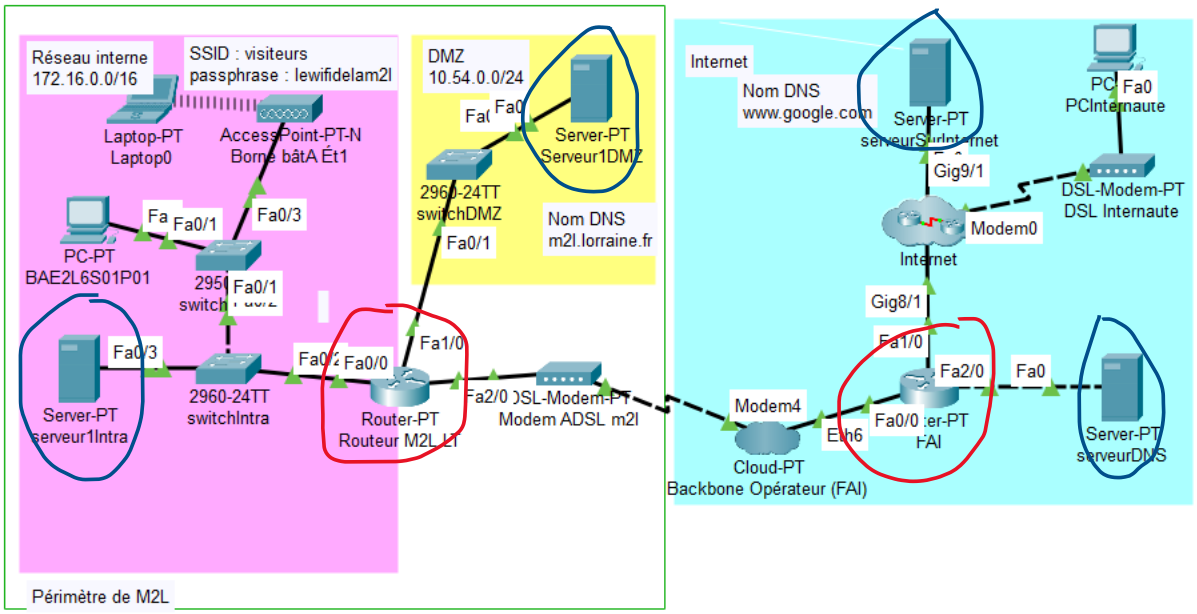
Prérequis :

- Plan du parc réseau de la M2L/ Maquette sous Packet Tracer
- Deux routeurs (un routeur M2L et un autre routeur FAI pour l’accès à internet)
- 3 serveurs situés dans la DMZ

Pour l’intervention nous procéderons à l’analyse du parc réseaux afin de vérifier l’état du système et des machines puis une maintenance et une remise à niveau de l’équipement ensuite nous installerons sur tous les routeurs le système d’exploitation/par feu Pfsense et enfin nous formerons les clients à l’utilisation et à la maintenance de Pfsense

Pour l’intervention nous procéderons à l’analyse du parc réseaux afin de vérifier l’état du système et des machines puis une maintenance et une remise à niveau de l’équipement ensuite nous installerons sur tous les serveurs le logiciel Zabbix et enfin nous formerons les clients à l’utilisation et à la maintenance de Zabbix

5- Emplacement sur le réseau



PFSENSE & Fortigate

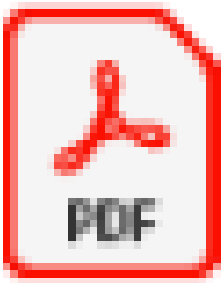
ZABBIX & NAGIOS

6- Solutions proposées

Caractéristique	**Pfsense**	**Checkpoint Firewall**
Type de License	Open source	Commercial
Coût	Gratuit (avec support payant optionnel)	Plus basique interface web moins moderne
Configuration	Principalement via l'interface GUI	Payant, dépendant du modèle et des services souscrits
Interface utilisateur	Interface web simple et fonctionnelle	Interface web avancée et console de gestion centralisée
Performance	Bonne pour les petites à moyennes entreprises	Haute performance, adaptée aux entreprises de toutes tailles
Fonctionnalités de sécurité	Firewall, VPN, NAT, trafic shaping	Firewall, VPN, prévention des intrusions, anti-bot, anti-virus, et plus
Support	Communauté active, support commercial optionnel	Support professionnel complet et services gérés disponibles
Idéal pour	PME, utilisateurs techniquement avertis	Grandes entreprises nécessitant une solution de sécurité robuste et intégrée

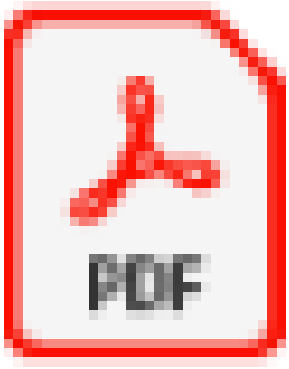
Critère	Zabbix	Nagios
Type de License	Open source (GPLc2)	Nagios XI commercial
Interface utilisateur	Moderne et bien intégré	Plus basique interface web moins moderne
Configuration	Principalement via l'interface GUI	Principalement par fichiers de configuration textuels
Découverte automatique des réseaux	Oui supporte la découverte automatique des réseaux	Limitée, principalement manuelle ou via des plugins
Surveillance	Active et passive, avec un large éventail de protocoles supportés	Principalement active, avec des plugins nécessaires pour différents protocole
Rapports	Rapports détaillés et personnalisables	Les rapports sont avancés
Alertes	Système d'alerte avancé et personnalisable	Système d'alerte flexible mais peut nécessiter plus de configuration
Communauté et support	Large communauté, avec beaucoup de documentation et de forums. Support commercial disponible	Très large communauté, nombreuse ressources et documentation disponible. Support commercial via Nagios XI

7- Devis

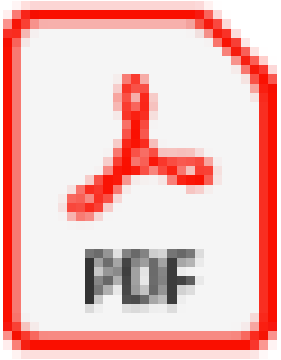


Devis_N1_-_Morrow_Sodali_1 (Zabbix).pdf

Devis_N1_-_Morrow_Sodali_2 (PFSENSE).pc



Devis_N1_-_Morrow_Sodali_5 (Nagios XI).p



Devis_N1_-_Morrow_Sodali_6 (CheckPoint F