|  |  |  |  |
| --- | --- | --- | --- |
| F:\BTS cours\portfolio\logoIMC.jpg | **BTS SIO**  **Services Informatiques aux Organisations** | | F:\BTS cours\portfolio\logolaposte.jpg |
| **Option** | **SISR** |
| **Session** | **2015** |

|  |  |  |
| --- | --- | --- |
| **Costes Antoine** | **Activité professionnelle N°** | 8 |

|  |  |
| --- | --- |
| **NATURE DE L'ACTIVITE** | Projet personnel encadré réalisé en formation : Sécurité Pare-feu |
| **Contexte** | Les responsables M2L décident de faire évoluer les services WEB en améliorant la qualité et la sécurité du réseau interne.  Le projet s’étend aussi à la mise à disposition du public d’Internet, des services d’accès aux sites WEB des ligues et de téléchargement de documents ou de brochures diverses. Ces serveurs sont accessibles à travers une zone commune sécurisée DMZ.  Un Pare Feu sera configuré sur les interfaces permettant l’accès à Internet et à la DMZ pour règlementer et filtrer les communications. |
| **Objectifs** | Mise en place de règles de filtrages sur le routeur de la DMZ |
| **Lieu de réalisation** | IMC - Paris |

|  |
| --- |
| **SOLUTIONS ENVISAGEABLES** |
| Faire héberger ces services WEB, FTP par un prestataire. |

|  |  |
| --- | --- |
| **DESCRIPTION DE LA SOLUTION RETENUE** | |
| **Conditions initiales** | Routeur sans règles de filtrage des communications entre les différents réseaux |
| **Conditions finales** | Création et mise en place de règles de filtrage |
| **Outils utilisés** | Cisco Packet Tracer |

|  |  |
| --- | --- |
| **CONDITIONS DE REALISATION** | |
| **Matériels** | Routeurs, serveurs et machines virtuels sur Cisco Packet Tracer |
| **Logiciels** | Cisco packet tracer, putty |
| **Durée** | 1 mois |
| **Contraintes** | Respect des commandes CISCO |

|  |  |
| --- | --- |
| **COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE** | |
| A5.1.5  A5.1.3  A3.2.1  A3.1.1  A1.4.1  A1.3.4  A1.3.3  A1.2.4  A1.2.3  A1.1.3  A1.1.2  A1.1.1 | Évaluation d'un élément de configuration ou d'une configuration  Suivi d'une configuration et de ses éléments  Installation et configuration d'éléments d'infrastructure  Proposition d'une solution d'infrastructure  Participation à un projet  Déploiement d'un service  Accompagnement de la mise en place d'un nouveau service  Détermination des tests nécessaires à la validation d'un service  Évaluation des risques liés à l'utilisation d'un service  Étude des exigences liées à la qualité attendue d'un service  Étude de l'impact de l'intégration d'un service sur le système informatique  Analyse du cahier des charges d'un service à produire |

|  |
| --- |
| **DEROULEMENT DE L'ACTIVITE** |
| **DMZ, zone démilitarisé :**  La zone démilitarisée (delimitarized zone) est une troisième interface sur un Firewall (sous réseau séparé du réseau local) possédant des machines qui sont susceptible d’être accéder par internet, si la DMZ est piraté, le réseau local ne sera pas compromis.  C:\Users\Anto^n\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Demilitarized_Zone_Diagram.png  L’espace DMZ est gérer par un pare feu au travers de règles de filtrage. Les ressources accessibles depuis l’internet sont dissociées des ressources accessibles à l’intérieur du réseau. Ces ressources peuvent être :   * Serveur WEB ou FTP * Un intranet pour les employés * Serveur mail * Toute autre ressource permettant à la société de dialoguer avec internet.   **Firewall, règle de filtrage :**  Un pare-feu (coupe-feu ou firewall) est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu permet de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :   * une interface pour le réseau à protéger (réseau interne) ; * une interface pour le réseau externe   Un système pare-feu contient un ensemble de règles prédéfinies permettant :   * D'autoriser la connexion (allow) ; * De bloquer la connexion (deny) ; * De rejeter la demande de connexion sans avertir l'émetteur (drop).   L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :   * D'autoriser uniquement les communications ayant été explicitement autorisées : * D'empêcher les échanges qui ont été explicitement interdits.   La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.  **Mise en place de la table de filtrages :**   * Les sous réseaux des ligues et M2L ont accès à l’Internet mais il n’est pas possible pour le public Internet d’accéder à un des équipements du réseau interne. * Les serveurs de téléchargement (FTP) et WEB Extranet (HTTP) de la DMZ sont accessibles à la fois par les sous réseaux des ligues et par le public Internet. * Les sous réseaux de l’association M2L ne doivent pas accéder au serveur de téléchargement FTP de la DMZ sauf le sous réseau Informatique. * Seuls les 7 postes du sous réseau Informatique M2L possédant les 7 adresses les plus hautes (dont les 2 postes de l’administrateur réseau) peuvent effectuer les commandes de test ping et tracert vers tous les éléments du réseau des ligues et vers l’Internet. * Seul le serveur WEB de la DMZ peut effectuer des requêtes vers le serveur de base de données (sur le port 5430) situé dans le sous réseau informatique à l’adresse 172.16.2.57.   **Commandes sur le routeur M2L :**  On crée d’abord les règles de filtrage :  *conf t*  *access-list 101 permit tcp any 172.16.0.0 0.0.0.255 established*  *access-list 101 permit tcp any 192.168.0.12 0.0.0.15 eq 20*  *access-list 101 permit tcp any 192.168.0.12 0.0.0.15 eq 80*  *access-list 101 icmp permit any 172.16.2.48 0.0.0.7 echo-reply*  *access-list 102 permit tcp host 192.168.0.12 172.16.2.57 eq 5430*  On attribue les règles de filtrage au port concerné :  int fa1/0  ip access-group 101 in (in ou out pour le filter de packet en entré ou en sortie)  ex  int fa1/1  ip access-group 102 in  ex  C:\Users\Anto^n\AppData\Local\Microsoft\Windows\INetCache\Content.Word\dmz.png  Il sera nécessaire d’effectué un ensemble de test enfin de vérifier l’efficacité des règles de filtrage mis en place. |

|  |
| --- |
| **CONCLUSION** |
| La DMZ apporte une maitrise totale de ces serveurs, une isolation physique des zones intranet, internet et DMZ. De plus, la définition de règles de filtrage spécifiques à la DMZ augmente la sécurité. Toutefois, elle a un cout élevé et nécessite une infrastructure lourde. |

|  |
| --- |
| **EVOLUTION POSSIBLE** |
| Mise en place d’un serveur proxy pour renforcer la sécurité des connections vers l’extérieur du réseau de la M2L |