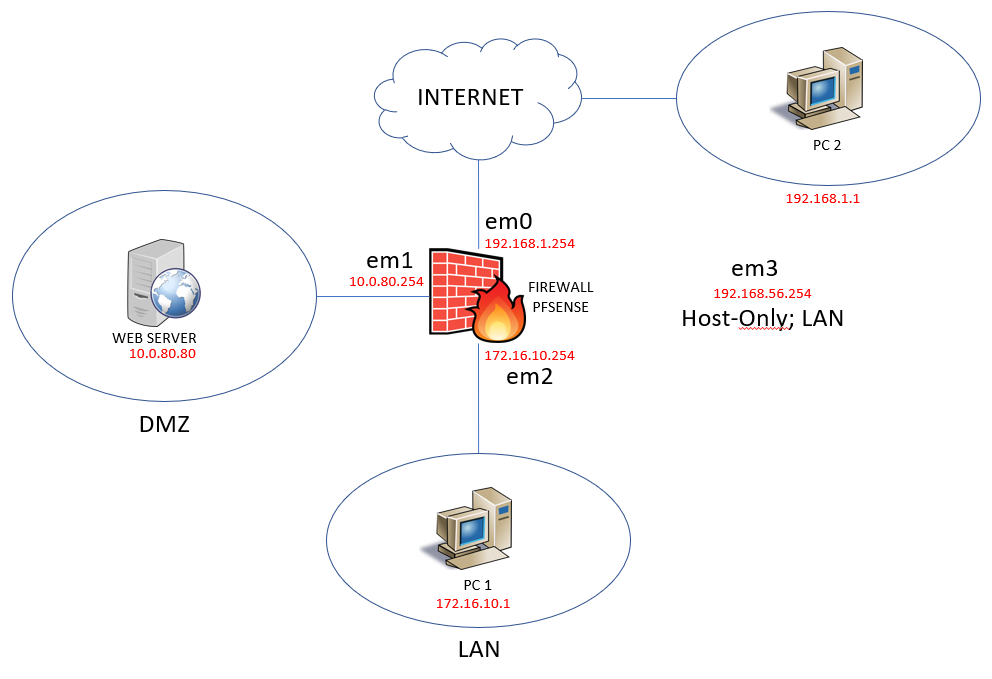
***TADJER Badr | TRAN Leo | ARRADI Naoufal***

***M1-APP-LS1***

**TP2 - Pare-Feu**

|  |
| --- |
|  |

1. Monter la maquette de la figure 1 en proposant un plan d’adressage de votre choix.



1. Écrire les règles du pare-feu pour satisfaire les contraintes suivantes :
   1. Il doit permettre l'accès à Internet des utilisateurs, mais uniquement vers un serveur http ou https (n’oublier pas d’autoriser DNS).

|  |
| --- |
| Ajout des 3 règles autorisant l’accès aux serveurs HTTP, HTTPS et aux DNS |
|  |

|  |
| --- |
| Teste d’une communication HTTP |
|  |

* 1. Il doit permettre le Ping d'une machine interne vers un serveur sur Internet. L’inverse est interdit.

|  |
| --- |
| Nous avons ajouté 2 règles, une interdisant tous Ping en destination du réseau LAN, et une autre, autorisant tous Ping vers un serveur internet. |
|  |

|  |
| --- |
| essaye de ping vers le DNS de Google |
|  |

* 1. Les machines du réseau LAN ne doivent pas être visible d'Internet (SNAT)

|  |
| --- |
| Par défaut sur pfsense les machines du réseau LAN ne sont pas visible d’internet |
|  |

* 1. Le serveur WEB dans la DMZ est accessible depuis le réseau LAN.

|  |
| --- |
| La règle permettant les communications de type HTTP vers n’importe quelle destination a été ajoutée à la question 2.a |
|  |

* 1. Le serveur WEB dans la DMZ n’est pas accessible directement depuis Internet (Utiliser le port forwarding).

|  |
| --- |
| Dans un premier, nous autorisons les accès TCP/UDP en destination du serveur Web |
|  |

|  |
| --- |
| Ensuite on configure l’accès au serveur Web en indiquant qu’il faut passer par l’interface du WAN |
|  |

|  |
| --- |
| Maintenant nous pouvons accéder à notre serveur en passant par l’adresse **192.168.56.80** |
|  |

* 1. Le pare-feu est accessible en utilisant SSH.

|  |
| --- |
| Nous devons activer la Secure Shell sur pfsense et nous avons laissé le port 22 par défaut pour les connexions en SSH |
|  |

|  |
| --- |
| Nous testons si la connexion SSH est possible en tapant sur l’invité de commande Windows, la commande : **ssh -p 22 root@192.168.56.254** |
|  |

1. Configurer le pare-feu pour qu’il puisse détecter et bloquer les scans réseau (nmap).

|  |
| --- |
| Afin de bloquer les scans réseau, nous avons installé le package **Snort**, qui s'occupe de détecter et bloquer les scans réseau. |
|  |

|  |
| --- |
| Nous avons ensuite configuré les paramètres sur service **Snort** et bloqué tous les hosts qui génère une alerte. |
|  |

1. Ajouter les règles qui permettent de protéger le pare-feu et les services internes des attaques DoS. Plusieurs solutions sont possibles. Effectuez une recherche et implémenter celle qui vous paraît la plus pertinente.

|  |
| --- |
| Afin de se prémunir des attaques DoS, nous avons ajouté les règles suivantes dans Snort :  **emerging-dos.rules**  **snort\_ddos.rules**  **snort\_dos.rules** |
|  |

1. Écrire des règles de protection contre les attaques par usurpation (spoofing).

|  |
| --- |
| Par défaut pfSense block les attaques par usurpation |
|  |

1. Le pare-feu est accessible par SSH. Faites le nécessaire afin de bloquer une adresse IP pour une heure après 5 tentatives de connexions SSH échouées.

|  |
| --- |
| Nous indiquons ici, qu’après 5 tentatives de connexion, l’adresse IP sera bloquée pendant 3600 secondes. |
|  |