Master 2 Informatique - Cybersécurité

Tp PARE-FEU Cisco

Abdel-Malik FOFANA
ID: 22218511

November 1, 2024

Contents

1 Exercice 1

1.1 Question 1 : C'est quoi un proxy inverse ? Quels sont les avantages d'un tel proxy?

- Un proxy inverse (reverse proxy) est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur proxy qui permet à un utilisateur d'accéder au réseau Internet, le proxy inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes

- Avantages : il cache l'adresse des serveurs internes pour plus de sécurité, répartit le trafic entre les serveurs (load balancing) pour améliorer les performances, et peut gérer la mise en cache pour accélérer les temps de réponse. Il permet aussi de filtrer le trafic et de centraliser l'authentification.

1.2 Question 2 : Classer les différentes zones de cette architecture de la zone la plus sécurisée à la zone la moins sécurisée.

- PC/Mail/Webmail (derrière FW2)

- DMZ Proxy (dans DMZ, derrière FW1)

- DMZ Web (dans DMZ, derrière FW1)

- Internet

1.3 Question 3 : L'ordre des règles de filtrage dans un pare-feu est-il important ? Justifier votre réponse.

En effet il est important

Les règles de pare-feu sont commandées séquentiellement, de la priorité la plus haute à la plus basse dans la liste des règles. Si la première règle ne spécifie pas comment traiter un paquet, le pare-feu examine la deuxième règle.

Ce processus se poursuit jusqu'à ce que le pare-feu trouve une correspondance. Si le pare-feu trouve une correspondance, le pare-feu prend l'action que la règle spécifie. Les règles de priorité plus faible suivantes ne sont pas examinées. Par exemple, si une règle qui bloque tout le trafic est répertoriée en premier et est suivie d'une règle qui autorise tout le trafic, le client bloque tout le trafic.

1.4 Question 4 : En appliquant la démarche d'organisation de règles de filtrage, écrire les règles de filtrage pour le pare-feu externe avec mémoire (FW1).

Règles de filtrage pour FW1

Autoriser HTTP vers Proxy HTTP : Source : Internet, Destination : 198.168.10.80, Port : 80, Action : Autoriser

Autoriser SMTP vers Proxy SMTP : Source : Internet, Destination : 198.168.10.25, Port : 25, Action : Autoriser

Autoriser DNS vers Proxy DNS : Source : Internet, Destination : 198.168.1.53, Port : 53, Action : Autoriser

Autoriser HTTP vers Serveur Web : Source : Internet, Destination : 10.0.0.2, Port : 80, Action : Autoriser

Bloquer tout le reste : Source : Internet, Destination : Tout, Action : Bloquer

Règles de filtrage pour FW2

Autoriser HTTP vers Serveur Web : Source : Internet, Destination : 10.0.0.2, Port : 80, Action : Autoriser

Autoriser SMTP vers PC Mail : Source : Internet, Destination : 198.168.10.25, Port : 25, Action : Autoriser

Autoriser Webmail : Source : Internet, Destination : (PC Webmail), Port : 443, Action : Autoriser

Autoriser DNS vers Proxy DNS : Source : Internet, Destination : 198.168.1.53, Port : 53, Action : Autoriser

Bloquer tout le reste : Source : Tout, Destination : Tout, Action : Bloquer

1.5 Question 5 : Pourquoi placer l'IDS entre l'Internet et le pare-feu? Quel est l'avantage principal ? Quels sont les inconvénients (nommez-en deux) ?

Placer un IDS (Intrusion Detection System) entre l'Internet et le pare-feu FW1 permet de surveiller et d'analyser le trafic entrant avant qu'il n'atteigne le pare-feu. Cela aide à détecter les menaces potentielles avant qu'elles ne puissent affecter le réseau interne.

Avantage principal : Détection précoce des intrusions. L'IDS peut identifier et alerter sur des activités suspectes ou malveillantes, permettant ainsi une réponse rapide avant que les attaques ne soient bloquées par le pare-feu.

Inconvénients :

- Faux positifs : L'IDS peut générer de nombreux faux positifs, entraînant une surcharge d'alertes et potentiellement une perte d'attention sur des menaces réelles.
- Charge de travail accrue : Comme le trafic n'est pas encore filtré par le pare-feu, l'IDS doit analyser un volume plus important de paquets, nécessitant ainsi plus de ressources (temps, personnel, configuration) et augmentant la complexité opérationnelle du réseau.

2 Exercice 2

2.1 Question 1 : Le NAT est un mécanisme qui limite le problème de la pénurie des adresses IPv4 mais qui a aussi des avantages en termes de sécurité. Quels sont les avantages du NAT du point de vue sécurité, coût et maintenance ?

- **Sécurité renforcée :** Cache le réseau interne, prévient les attaques ciblées et limite l'accès à des sites malveillants.
- **Meilleure vitesse :** Réduit le nombre de paquets à acheminer, améliorant ainsi la communication réseau.
- **Flexibilité :** Permet de modifier la configuration du réseau sans changer les adresses IP.
- **Multi-homing :** Connecte des appareils à plusieurs réseaux publics, offrant redondance et disponibilité accrue.
- **Économies :** Diminue le besoin en adresses IP, réduisant les coûts associés.
- **Administration simplifiée :** Facilite la gestion du réseau en réduisant le nombre d'adresses IP à attribuer.

2.2 Question 2 : C'est quoi le problème rencontré si les deux utilisateurs (les deux pairs) pratiquent le NAT dynamique ?

Si deux utilisateurs pratiquent le NAT dynamique, ils peuvent rencontrer les problèmes suivants :

1. **Conflit d'adresses :** Les deux utilisateurs pourraient essayer d'utiliser la même adresse IP publique à différents moments, entraînant des collisions et des échecs de connexion.

2. **Difficultés de communication :** Les connexions directes entre les utilisateurs sont compliquées, car leurs adresses IP privées ne sont pas routables sur Internet, ce qui empêche les communications P2P efficaces.

2.3 Question 3 : C'est quoi la différence entre le mécanisme de redirection de port et le mécanisme du NAT ?

La redirection de port (port forwarding) et le NAT (Network Address Translation) sont deux mécanismes de gestion du trafic réseau, mais ils servent des objectifs différents :

1. **Redirection de port :**
   - Permet de rediriger des paquets destinés à un port spécifique d'une adresse IP vers une autre adresse IP et un port différent.
   - Utile pour exposer des services internes (comme un serveur web) à l'extérieur en spécifiant quel port doit être redirigé.
2. **NAT :**
   - Modifie l'adresse IP source ou destination des paquets traversant un routeur ou un pare-feu.
   - Utilisé pour masquer les adresses IP internes derrière une seule adresse IP publique, permettant à plusieurs appareils de partager une seule adresse IP.

La redirection de port fonctionne à la couche 4 (Transport) en redirigeant des paquets selon leur port, tandis que le NAT opère à la couche 3 (Réseau) en modifiant les adresses IP

2.4 Question 4 : Comment utiliser le mécanisme de redirection de port pour résoudre le problème du pair-à-pair lorsque les deux pairs sont derrière un NAT dynamique ?

La redirection de port est une solution pour permettre la communication directe entre deux pairs derrière un NAT dynamique en suivant ces étapes :

1. **Configurer le NAT :** Associer un port externe spécifique au port local de chaque pair.
2. **Échanger les informations de port :** Utiliser un serveur de signalisation pour partager l'IP publique et le port.
3. **Établir la connexion :** Les pairs se connectent en utilisant les informations échangées.