Configuration et Utilisation de VM 1 - Serveur DHCP OpenBSD

Introduction

Le serveur **VM 1** est configuré pour gérer les adresses IP sur les réseaux privés de l'entreprise, en jouant le rôle de passerelle et serveur DHCP. Il attribue dynamiquement des adresses IP aux hôtes des trois réseaux privés et assure leur connectivité interne ainsi qu'un accès sécurisé à Internet. Ce serveur est installé sous **OpenBSD**, un système d'exploitation reconnu pour sa sécurité. Nous allons détailler les étapes d'installation de **OpenBSD** sur VirtualBox, ainsi que la configuration complète du serveur DHCP, des règles de sécurité et des réseaux internes.

Détails de la Configuration de VM 1

1. Installation d'OpenBSD sur VirtualBox

- **Téléchargement de l'ISO d'OpenBSD** :
    - Allez sur le site officiel d'OpenBSD (https://www.openbsd.org) et téléchargez la dernière image ISO (généralement l'image **amd64**).
- **Création de la VM sur VirtualBox** :
    - Lancez VirtualBox et créez une nouvelle machine virtuelle.
    - Donnez un nom à la VM, par exemple **VM1-DHCP**.
    - Choisissez **BSD** comme type de système d'exploitation, et **OpenBSD (64-bit)** comme version.
- **Configuration des ressources**:
    - Par défaut
- **Configuration des cartes réseau** :
    - La VM doit avoir trois cartes réseau internes (NIC) :
        - **LAN-1 (Administration)**, **LAN-2 (Serveur)** et **LAN-3 (Employés)**.
        - Pour chaque carte, choisissez le type **Réseau interne (Internal Network)** dans les paramètres réseau de VirtualBox.

- **Lancement de la VM** :
    - Lancez la VM avec l'ISO d'OpenBSD monté dans le lecteur CD pour démarrer l'installation.

- **Installation d'OpenBSD** :
    - Suivez les instructions d'installation à l'écran.
    - Choisissez les options par défaut pour le partitionnement du disque et configurez la langue et le fuseau horaire.
    - Créez un utilisateur `root` pour les privilèges administratifs
    - Configurez les paramètres réseau avec des adresses statiques pour chaque carte réseau (voir plus bas pour la configuration spécifique des cartes).

- **Configuration des cartes réseau avec IP statiques** :
    - Configurez les cartes réseaux internes pour qu'elles obtiennent des IP statiques et configurez la lan Nat sur dhcp:
        - **LAN-1 (Administration)** : `192.168.42.1`

        -> echo 'inet 192.168.42.1 255.255.255.192' | sudo tee -a /etc/hostname.em1 <-

        - **LAN-2 (Serveur)** : `192.168.42.65`

        -> echo 'inet 192.168.42.1 255.255.255.192' | sudo tee -a /etc/hostname.em2 <-

        - **LAN-3 (Employés)** : `192.168.42.130`

        -> echo 'inet 192.168.42.130 255.255.255.192' | sudo tee -a /etc/hostname.em3 <-

        - **NAT**

            -> echo 'dhcp' | sudo tee -a /etc/hostname.em0 <-

        Appliquez la configuration en redémarrant le réseau

        -> sh /etc/netstart <-

2. Configuration des Réseaux et des Masques de Sous-Réseau

Une fois OpenBSD installé et démarré, il est nécessaire de configurer les sous-réseaux pour assurer la bonne segmentation du réseau interne. Pour chaque LAN, nous allons définir une plage DHCP et un masque de sous-réseau adapté.

- **LAN-1 (Administration)** :
    - **Plage d'adresses** : 192.168.42.0 - 192.168.42.63
    - **Masque de sous-réseau** : 255.255.255.192 (/26)
    - **Broadcast** : 192.168.42.63
    - **Plage DHCP** : 192.168.42.40 - 192.168.42.60
- **LAN-2 (Serveur)** :
    - **Plage d'adresses** : 192.168.42.64 - 192.168.42.127
    - **Masque de sous-réseau** : 255.255.255.192 (/26)
    - **Broadcast** : 192.168.42.127
    - **Plage DHCP** : 192.168.42.70 - 192.168.42.110
- **LAN-3 (Employés)** :
    - **Plage d'adresses** : 192.168.42.128 - 192.168.42.191
    - **Masque de sous-réseau** : 255.255.255.192 (/26)
    - **Broadcast** : 192.168.42.191
    - **Plage DHCP** : 192.168.42.140 - 192.168.42.180

Ces masques de sous-réseau sont tous configurés en `/26`, ce qui permet une gestion efficace des adresses IP tout en assurant suffisamment d'adresses pour les clients DHCP.

3. Configuration du Serveur DHCP

Le serveur **OpenBSD** gère les adresses IP pour les trois réseaux internes via le serveur DHCP. Voici les étapes à suivre pour configurer le service DHCP :

1. **Installation et activation du serveur DHCP** :
    - Le serveur DHCP est déjà inclus dans OpenBSD. Il vous suffit de modifier le fichier de configuration **dhcpd.conf** en y ajoutant les plages d'adresses, le masque de sous-réseau, le broadcast et la plage DHCP

-> echo 'subnet 192.168.42.0 netmask 255.255.255.192 {

range 192.168.42.40 192.168.42.60;

option routers 192.168.42.1;

option broadcast-address 192.168.42.63;

}

subnet 192.168.42.64 netmask 255.255.255.192 {

range 192.168.42.70 192.168.42.110;

option routers 192.168.42.65;

option broadcast-address 192.168.42.127;

host webserver {

hardware ethernet 00:1a:2b:3c:4d:5e; # MAC address of the web server fixed-address 192.168.42.70; # Reserved IP for the web server

}

}

subnet 192.168.42.128 netmask 255.255.255.192 {

range 192.168.42.140 192.168.42.180;

option routers 192.168.42.129;

option broadcast-address 192.168.42.191;

}' | sudo tee -a /etc/dhcpd.conf <-

2. **Configuration de l'écoute dhcp** pour chaque LAN:

   nano /etc/rc.conf

   la ligne dhcpd_flags doit être dhcpd_flags = "em1 em2 em3"

3. **Configuration de l'activation au démarrage** pour chaque LAN:

   rcctl enable dhcpd

   rcctl start dhcpd

4. Configuration du Filtrage des Paquets et des Règles de Sécurité

Le filtrage des paquets est crucial pour sécuriser les communications entre les LANs et l'accès à Internet. Les règles de filtrage doivent être définies comme suit :

- **LAN-1 (Administration)** :
  - **Accès complet** aux serveurs et autres réseaux via le serveur LAN-2. Aucune restriction sur les ports.
- **LAN-3 (Employés)** :
  - **Accès limité** : Le réseau des employés ne peut accéder aux serveurs que via HTTP (port 80) et HTTPS (port 443).
- **Communication entre réseaux** :
  - Tous les LANs (administration, serveur et employés) doivent pouvoir communiquer entre eux via la passerelle VM 1.
  - **Ping** : Tous les sous-réseaux doivent être capables de se pinguer mutuellement.
  - **Accès à Internet** : Tous les LANs doivent pouvoir sortir sur Internet.

nano /etc/pf.conf

puis remplissez le fichier avec les règles firewall dans une logique de whitelist pour ne laisser passer que les paquets nécessaires

```
# Define the interfaces and networks

nat = "em0"             # Replace with your NAT interface

admin = "em1"           # Replace with your admin interface

server = "em2"          # Replace with your server interface

employee = "em3"        # Replace with your employee interface



# Block all traffic by default

block all

match out on $nat from {$admin:network, $server:network, $employee:network} to any nat-to $nat

pass in quick on $nat inet proto tcp from any to any

#dhcp request

pass in on {$admin,$server,$employee} proto udp from  {$admin,$server,$employee} to $nat port 67

#dhcp receive

pass out on {$admin,$server,$employee} proto udp from $nat to {$admin,$server,$employee} port 68

# dns traffic

pass out on {$admin,$server,$employee} proto udp from  {$admin,$server,$employee} to any port 53

pass in on {$admin,$server,$employee} proto udp from any to {$admin,$server,$employee} port 53

# internet access

pass in on {$admin, $server, $employee} from {$admin_network, $server_network, $employee_network} to any
```

```
# valider le traffic sortant des machines allant vers les machines des réseaux internes

pass out on {$admin, $server, $employee} to {$admin, $server, $employee}


# Accés ping entre les machines du réseaux

pass inet proto icmp from $admin_network to $server_network

pass inet proto icmp from $admin_network to $employee_network

pass inet proto icmp from $server_network to $admin_network

pass inet proto icmp from $server_network to $employee_network

pass inet proto icmp from $employee_network to $admin_network

pass inet proto icmp from $employee_network to $server_network


# règles admin, accés total serveur

pass in on $server from $admin:network to $server:network

pass out on $server from $server:network to $admin:network


# règles employées accès serveur

pass in on $server proto tcp from $employee:network to $server:network port {80, 443} keep
state

pass out on $server proto tcp from $employee:network to $server:network port {80, 443}
keep state


# Accept nat traffic

pass out on $nat proto {tcp, udp, icmp} from all modulate state
```

5. Routage IPV4

nano /etc/sysctl.conf

net.inet.ip.forwarding doit être égal à 1

Conclusion

L'installation et la configuration de **VM 1** en tant que serveur **DHCP OpenBSD** permet une gestion centralisée des adresses IP pour les réseaux internes de l'entreprise. Grâce à la segmentation des réseaux, à la mise en place d'un filtrage des paquets strict et à l'accès sécurisé à Internet, cette configuration assure à la fois flexibilité, sécurité et efficacité dans la gestion des ressources réseau.