

BTS Services Informatique à l'Organisation

Option : Solutions d'Infrastructure, Systèmes et Réseaux



Epreuve E5 : Conception et maintenance de solution informatique

Document technique

Projet #3 - Mise en place d'un pare-feu pfSense sécurisant un réseau local

SOMMAIRE

1. Introduction

- 1.1. Présentation de l'entreprise Kalo-Brazza
- 1.2. Objectifs du projet
- 1.3. Contexte et enjeux

2. Présentation de pfSense

- 2.1. Définition et fonctionnalités
- 2.2. Avantages de l'utilisation de pfSense
- 2.3. Matériels compatibles

3. Spécifications Techniques

- 3.1. Infrastructure réseau actuelle
- 3.2. Configuration matérielle requise
- 3.3. Schéma réseau prévu

4. Plan de Déploiement de pfSense

- 4.2. Installation du système
- 4.1. Configuration des interfaces réseau

5. Tests de connectivité et coûts d'installation

1. Introduction

1.1. Présentation de l'entreprise Kalo-Brazza

Kalo-Brazza est une entreprise spécialisée dans les services numériques variés, allant du développement d'applications web à la gestion de données en cloud. Pour assurer la sécurité et l'efficacité de ses opérations, l'entreprise vise à renforcer son infrastructure réseau en déployant pfSense.

1.2. Objectifs du projet

L'objectif principal est d'assurer la sécurité du réseau local (LAN) de Kalo-Brazza en installant et configurant pfSense pour filtrer et contrôler les échanges sur le réseau. Cela inclut la mise en place d'un pare-feu robuste, d'un système de routage efficace, et d'un portail captif pour une gestion avancée des utilisateurs.

1.3. Contexte et enjeux

Avec l'augmentation des cybermenaces et la complexité croissante des infrastructures réseau, la sécurisation des systèmes d'information est devenue une priorité stratégique pour Kalo-Brazza. L'entreprise traite quotidiennement des données sensibles, notamment des informations confidentielles liées aux projets clients et des données internes cruciales.

Pour répondre à ces enjeux, Kalo-Brazza a décidé de renforcer sa politique de sécurité en intégrant **pfSense**, une solution open-source reconnue pour sa fiabilité et sa flexibilité. Ce choix s'inscrit dans une démarche proactive visant à protéger les actifs numériques de l'entreprise tout en garantissant une connectivité rapide et stable.

2. Présentation de la solution attendue : pfSense

2.1. Définition et fonctionnalités

pfSense sécurise les systèmes d'information en contrôlant l'ensemble des échanges effectués sur le réseau.

Réalisée à partir d'une distribution BSD (FreeBSD) lui garantissant ainsi un niveau élevé de sécurité informatique et de fiabilité, la distribution pfSense permet le déploiement d'un pare-feu, d'un routeur, ainsi que d'un portail captif complet et adaptés aux professionnels.

De plus, il s'installe aussi bien sur du matériel professionnel (serveurs) que sur du matériel informatique courant tel qu'un simple PC client, ou bien encore une machine virtuelle...

2.2. Avantages de l'utilisation de pfSense

Sécurité accrue grâce à un contrôle strict des échanges réseau.

Flexibilité dans la configuration et les mises à jour.

Compatibilité avec différents matériels, y compris les machines virtuelles.

2.3. Matériels compatibles

pfSense peut être installé sur des serveurs dédiés, des PC standard, ou des plateformes virtualisées, assurant ainsi une grande flexibilité pour répondre aux besoins spécifiques de Kalo-Brazza.

3. Spécifications Techniques

3.1. Infrastructure réseau actuelle

L'infrastructure actuelle comprend des segments LAN et WAN avec plusieurs points d'accès sans fil et des postes de travail.

3.2. Configuration matérielle requise

Processeur : Intel/AMD 64-bit

Mémoire : Minimum 2 GO

Stockage : 16 GO

Interfaces réseau : WAN et LAN

3.3. Schéma réseau prévu

Le réseau sera segmenté en deux principales interfaces :

WAN : Connecté à l'Internet, configuration via DHCP. LAN :

Configuration IP manuelle, adressage 192.168.1.1/24.

Passons à la configuration de pfSense :

Après l'installation de la machine, vous devriez avoir une page identique.

Sur cette page, nous pouvons configurer le pare-feu ou tester sa connectivité.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 43678a0341d7683bd348

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.24.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █

```

L'option 1 permet d'assigner les interfaces à leurs cartes réseaux respectives, dans notre cas em0 correspond à l'interface WAN et em1 à l'interface LAN.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 43678a0341d7683bd348

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.24.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 1█

```

Après avoir assigner vos interfaces, il faut leur attribuer une adresse IP, l'interface WAN récupèrera la sienne via DHCP mais l'interface LAN quant à elle devra être configuré manuellement.

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.24.128/24
LAN (lan)      -> em1      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y
```

```
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

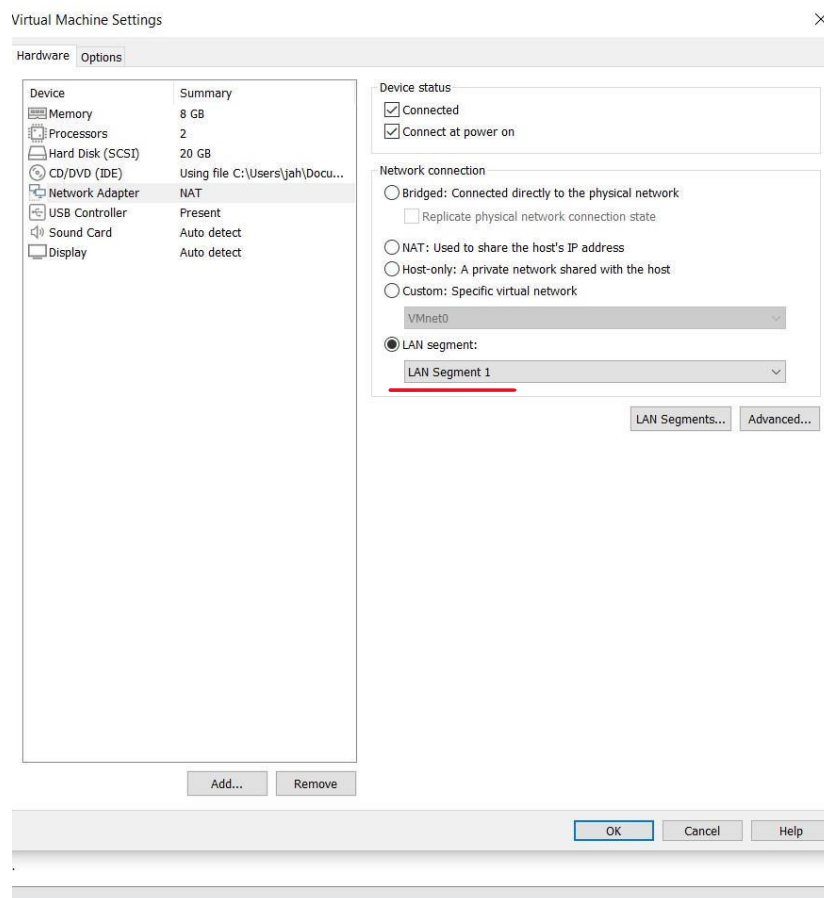
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 WAN address has been set to dhcp
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://dhcp/

Press <ENTER> to continue.
```

Après avoir configuré votre pare-feu, assignez la carte réseau LAN à une VM afin de tester le service DHCP.



5. Test de connectivité et coûts d'installation

Testez votre connectivité avec internet.

```

1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

```

Enter an option: 7

Enter a host name or IP address: 8.8.8.8

```

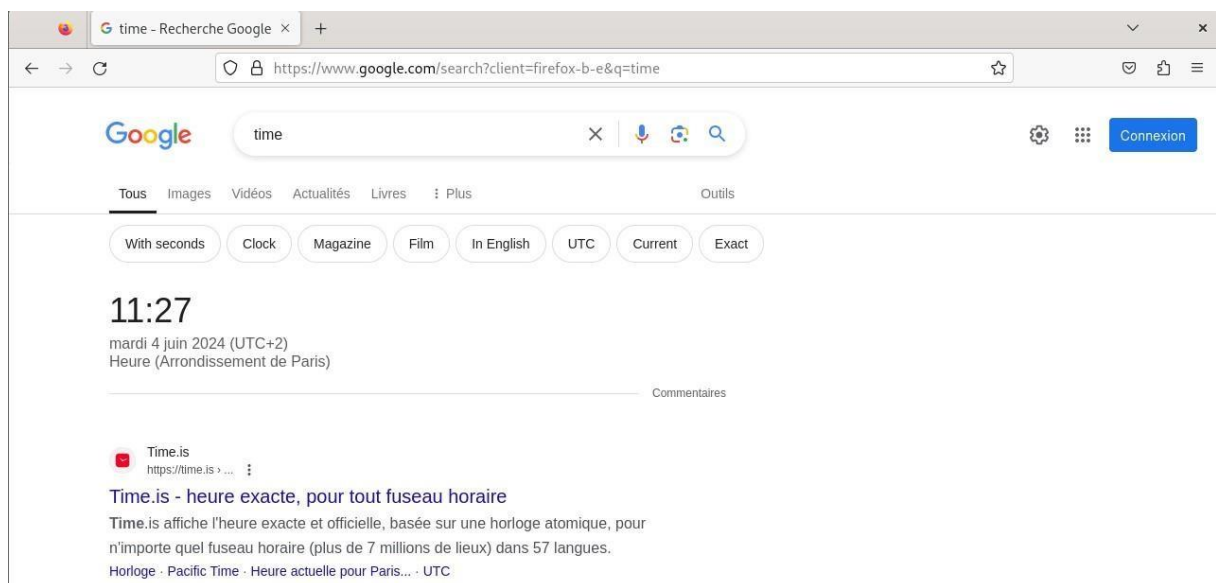
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=6.159 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=6.384 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=6.522 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.159/6.355/6.522/0.150 ms

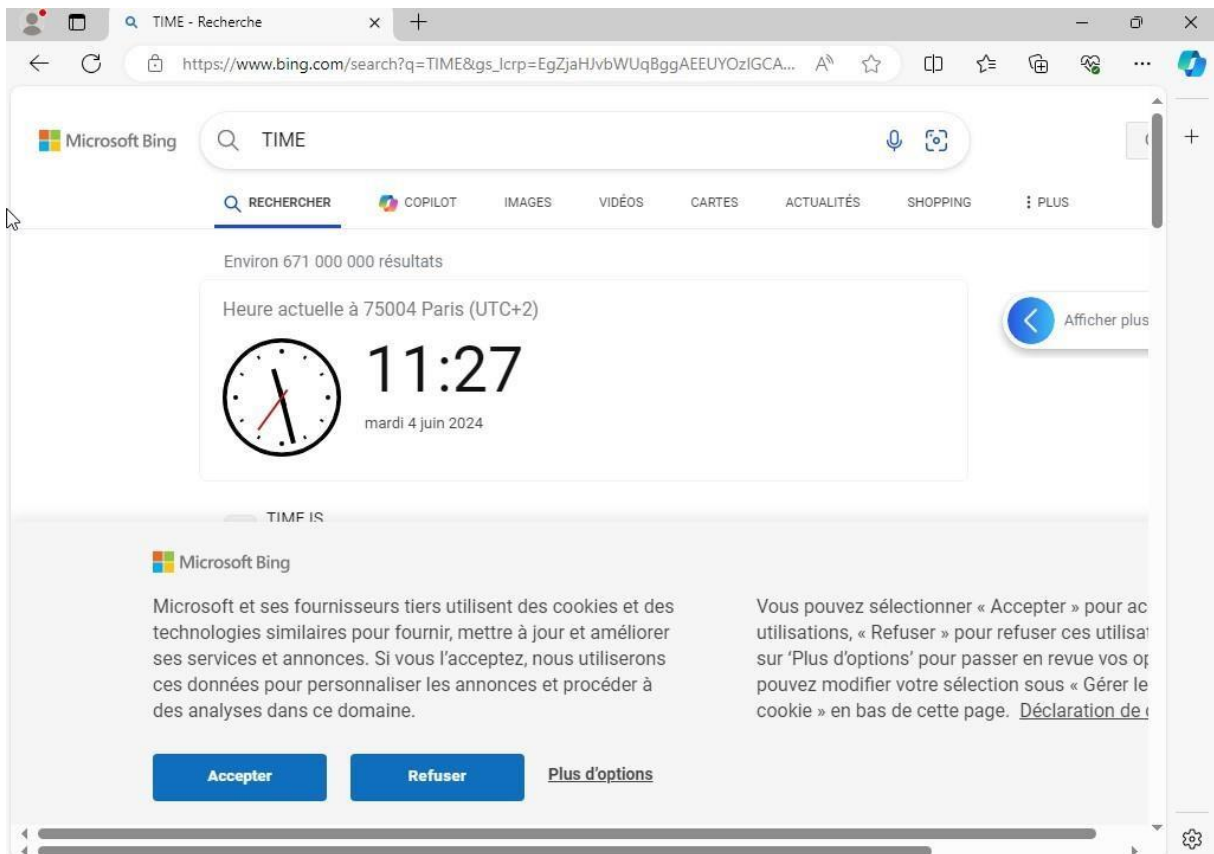
Press ENTER to continue.

```

Il ne semble pas y avoir de problème, essayez de faire une recherche sur internet et si la recherche aboutit c'est qu'il n'y a pas de problème.



Et le tour est joué vous avez internet sur vos machines associées !



Pour ce qui est des coûts :

1. Matériel : - Serveur dédié : 800 €
2. Logiciel : - pfSense (open source) : Gratuit
- Packages et extensions : Gratuits
3. Main d'œuvre : - Installation et configuration de pfSense (3 jours x 450 €/jour) : 1350 €
- Formation de l'équipe IT à la gestion de pfSense (1 jour x 450 €/jour) : 450 € Total estimé pour l'installation : 2600 €