Documentation de la configuration et des équipements du réseau de la maquette du cluster

Introduction : La maquette est composée de 4 zones : le LAN, la DMZ, le WAN et la ZS. Ces 4 zones sont interconnectées grâce à pfSense comme le montre le schéma réseau de la maquette que vous pouvez retrouver ici. La maquette comporte plusieurs serveurs et services dans les différentes zones que nous allons détailler dans cette documentation.

pfSense

pfSense est un routeur/pare-feu open source basée sur le système d'exploitation FreeBSD. Dans la configuration de la maquette, celui-ci jouera un rôle très important avec notamment l'utilisation des nombreux services qu'il propose. Il a été installé sur une machine virtuelle dédiée à partir de son ISO d'installation.
Site officiel de pfSense : https://www.pfsense.org/
La version du pfSense de cette maquette est la 2.3.4. Cette machine comporte 5 interfaces :

Interface	Adresse IP	VLAN
WAN	10.30.20.220	VLAN : 20
LAN	172.30.20.254	VLAN : 27
DMZ	172.30.30.254	VLAN : 21
ZS	172.30.10.254	VLAN : 22
SYNC	10.0.0.1/30	VLAN : 22

- -

Théoriquement :
Le pfSense est théoriquement un cluster pfSense en utilisant notamment les services High Availability Synchronisation (aussi appelé pfSense failover) et CARP de pfSense. Le service High Availability Synchronisation sert à synchroniser les configurations entre le pfSense MASTER et le pfSense SLAVE en utilisant une interface dédiée (SYNC) pour transiter les données en utilisant le protocole pfsync. Le service CARP sert quant à lui à la création des IP Virtuels et au basculement du MASTER au SLAVE en cas de détection d'un problème sur une interface. C'est le système de pfSense qui permet de créer un cluster de pfSense et donc d'assurer une haute disponibilité. J'ai voulu faire un cluster de pfSense car dans ma maquette, le pfSense est un SPOF (Single Point Of Failure ou Point individuel de défaillance en français) car c'est lui qui centralise toutes les connexions et qui fait office de passerelle par défaut dans toutes les zones de la maquette. Un problème ou une défaillance de l'une des interfaces du pfSense peut alors entraîner l'arrêt complet du réseau. J'ai donc créé un deuxième pfSense, le SLAVE et l'ai configuré pour mettre en place le cluster pfSense dont voici les configurations :

pfSense MASTER :

Interface	Adresse IP	VLAN
WAN	10.30.20.220	VLAN : 20
LAN	172.30.20.253	VLAN : 27
DMZ	172.30.30.253	VLAN : 21
ZS	172.30.10.253	VLAN : 22
SYNC	10.0.0.1/30	VLAN : 22
VIP LAN	172.30.20.254	VLAN : 27
VIP WAN	10.30.20.222	VLAN : 20
VIP DMZ	172.30.30.254	VLAN : 21
VIP ZS	172.30.10.254	VLAN : 22

pfSense SLAVE :

Interface	Adresse IP	VLAN
WAN	10.30.20.221	VLAN : 20
LAN	172.30.20.252	VLAN : 27
DMZ	172.30.30.252	VLAN : 21
ZS	172.30.10.252	VLAN : 22
SYNC	10.0.0.2/30	VLAN : 22
VIP LAN	172.30.20.254	VLAN : 27
VIP WAN	10.30.20.222	VLAN : 20
VIP DMZ	172.30.30.254	VLAN : 21
VIP ZS	172.30.10.254	VLAN : 22

Le mot de passe utilisé pour la synchronisation entre les deux pfSense est :pfsense_cluster1452

Voici les différents éléments du pfSense Master qui se synchronisent avec le pfSense SLAVE :

- User manager users and groups
- Authentification servers (LDAP, RADIUS)
- Certificate Authorities, Certificates and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration

- Ipsec configuration
- OpenVPN configuration
- DHCP Server settings
- WoL Server settings
- Static Route configuration
- Load Balancer configuration
- Virtual Ips
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwader and DNS Resolver configurations
- Captive Portal

Les services qui proviennent de paquets que l'on installe manuellement comme Squid ne sont pas synchronisés, toutefois avec tous les services synchronisés, on peut faire fonctionner le réseau dans un mode dégradé.

Les synchronisations entre les deux pfSense fonctionnaient parfaitement et le système CARP qui transférait les interfaces défaillantes (en stoppant manuellement les interfaces sur le MASTER) vers les interfaces du SLAVE fonctionnait aussi parfaitement.
Malheureusement il y avait un problème avec les IP Virtuels car celles-ci n'émettaient ni ne recevaient aucune donnée. Autrement dit, seules les interfaces réelles fonctionnaient, après plusieurs recherchent il s'avère que c'est un problème de pfSense quand il est utilisé sur des ESX car il faut que les interfaces sur lesquelles sont les IP Virtuels soient des interfaces en mode Distribué. Ces interfaces Distribuées doivent être rattachées à des interfaces physiques par interface Distribuée, hors avec le Cluster, nous ne disposons que d'interface Standard.
J'ai donc du renoncer au Cluster de pfSense tel que je viens de le décrire mais j'ai conservé le pfSense SLAVE car le service de synchronisation High Availability Synchronisation fonctionne très bien et en cas de problème sur le pfSense MASTER, je n'aurais qu'à changer manuellement les adresses IP des interfaces du SLAVE pour rétablir un mode de fonctionnement dégradé du réseau le temps de remettre en service le pfSense MASTER.
Voici la configuration réelle des interfaces du pfSense SLAVE :

Interface	Adresse IP	VLAN
WAN	10.30.20.221	VLAN : 20
LAN	172.30.20.252	VLAN : 27
DMZ	172.30.30.252	VLAN : 21
ZS	172.30.10.252	VLAN : 22
SYNC	10.0.0.2/30	VLAN : 22

- -

Pour accéder à l'interface WEB de pfSense, il faut y accéder à partir de cette adresse URL : https://pfsense.flo.bts/
OU à partir de l'IP : https://172.30.20.254/
On utilise les logins/password suivants :
User: admin

Password : pfsense

J'ai crée un compte d'accès spécialement dédié pour faire de la supervision de pfSense en utilisant l'interface principale de pfSense (dashboard) avec notamment des personnalisations de cette interface qui permettent d'avoir un état des services et de l'utilisation de pfSense, de ses interfaces, des utilisateurs connectés, des logs du firewall...

Le compte de supervision utilise les logins/password suivant :
User : view_dashboard
Password : @1ROOTview.bts

Les services de pfSense :

- Le service firewall :

Le service firewall (parefeu) est l'un des plus importants services de pfSense, il permet d'autoriser ou de refuser des flux en fonction des règles qui ont été précédemment établies. Les règles sont établies par interface, on autorise ou non les flux qui ont pour origine les IP de l'interface WAN et qui ont pour direction la DMZ par exemple. On peut aussi spécifier les protocoles et les ports par lesquels les flux sont autorisés à passer pour garantir une meilleure sécurité.

- Le portail captif :

Le portail captif est défini dans la zone du LAN et oblige ainsi à chaque utilisateur du LAN à s'authentifier sur le portail captif en utilisant la page WEB d'authentification du portail captif. Cette authentification est gérée grâce au serveur RADIUS de l'Active Directory (172.30.20.2). Il utilise le protocole MSCHAPv1.

- Le serveur DHCP :

Le serveur DHCP est défini dans la zone du LAN et permet ainsi une configuration automatique et dynamique des adresses IPs du LAN.
Le réseau est 172.30.20.0/24
La plage d'adresse IP est : de 172.30.20.10 à 172.30.20.253
Les serveurs DNS sont 172.30.10.2 et 172.30.20.254
La passerelle par défaut est 172.30.20.254
Le suffixe DNS est flo.bts
Le bail est de 86400 s

- Le service d’autorité de certification :

Le service d'autorité de certification permet de faire des certificats signés et approuvés par l'autorité de certification, il suffit alors d'installer le certificat de l'autorité de certification sur les postes du LAN pour que l'on puisse accéder de manière sécurisé aux ressources locales comme owncloud ou pfSense par exemple.

- Le service de proxy filtrant (Squid + SquidGuard + ClamAV)

Le service de proxy filtrant permet d'enregistrer les flux des utilisateurs du LAN lorsqu'ils se connectent sur des sites Internet. Il joue le rôle de filtre avec l'utilisation de SquidGuard qui permet alors de mettre en place des ACLs qui interdisent les sites dans la blacklist (http://www.shallalist.de/Downloads/shallalist.tar.gz). Squid est configuré en mode

transparent pour que les utilisateurs n'aient pas de configuration particulière à rentrer pour pouvoir naviguer. Il utilise l'authentification du portail captif, ainsi dans les logs de Squid, on peut identifier les utilisateurs avec leurs comptes Active Directory. Le proxy est cumulé avec l'antivirus open source ClamAV qui scannent les fichiers et les pages WEB qui font l'objet d'une requête par un client. Lorsqu'un fichier malveillant est détecté, il est mis en quarantaine sur le pfSense et il n'atteint donc pas l'utilisateur ni la zone LAN.

- Le service snort :

Le service snort est un service qui utilise l'IDS (Intrusion Detection System ou Systèmes de détection d'intrusion en français) SNORT pour détecter les menaces potentieles du réseau. Il utilise des bases de données qui lui permettent de détecter un comportement suspect dans le réseau, comme un spoofer par exemple. Dans le cas d'une détection d'intrusion du réseau il alerte l'administrateur. C'est un système qui vise à améliorer la sécurité du réseau en surveillant son utilisation.

- Le service OpenVPN

Le service OpenVPN est un service qui permet de faire une connexion privée distante à l'aide d'un VPN. Dans notre cas, le mode d'utilisation du VPN est site-à-site, c'est à dire que l'on va faire en sorte que le PC distant puisse être reconnu comme un PC appartenant à la LAN. De cette façon, le PC distant pourra, en passant par le portail captif et le proxy, accéder aux ressources du réseau (DMZ + ZS) comme s'il était dans la LAN.

- Le service Backup & Restore :

Le service Backup & Restore permet de faire des sauvegardes des configurations de pfSense dès que des éléments sont modifiés dans pfSense de la même manière que GIT (il met en évidence les différences, ajouts et suppression entre deux configurations). On peut ainsi reprendre la précédente configuration dans le cas d'une erreur de manipulation ou de configuration.

PfSense utilise les DNS : 172.30.10.2 8.8.8.8 8.8.4.4

Centreon

Centreon est un outil de supervision open source qui se base sur l'utilisation de Nagios pour recueillir les informations relatives à la supervision des équipements. Il est très utilisé comme solution gratuite ou à moindre frais (coût des plugins spécifiques) dans les entreprises.
Site officiel de Centreon : https://www.centreon.com/fr/

Centreon est installé sur une distribution CentOS, voici sa configuration :

Interface	Adresse IP	Route par défaut	VLAN	ZONE
eth0	10.30.10.5	172.30.10.254	VLAN : 22	ZS

Les serveurs DNS renseignés dans le resolv.conf sont 172.30.10.2 et 172.30.10.254

Pour accéder à l'interface WEB de Centreon, on utilise l'URL :

http://supervision.flobts
OU avec l'adresse IP http://172.30.10.5/Centreon
On se connecte à l'aide des logins/password suivant :
User: admin
Password : centreon

Les logins/password du compte root de CentOS sont :
User: root
Password : centreon

note : Pour faire une mise à jour de CentOS : yum update -y

GLPI

CLPI est une solution open source de gestion de parc informatique. Il permet la gestion de l'inventaire des composantes matérielles ou logicielles d'un parc informatique ainsi que la gestion de l'assistance aux utilisateurs.
Site officiel de GLPI : http://glpi-project.org/

GLPI est installé sur une distribution Debian 8 (Jessie), voici sa configuration :

Interface	Adresse IP	Route par défaut	VLAN	ZONE
eth0	172.30.10.4	172.30.10.254	VLAN : 22	ZS

Les serveurs DNS renseignés dans le resolv.conf sont 172.30.10.2 et 172.30.10.254

Pour accéder à l'interface WEB de GLPI, on utilise l'URL :
http://glpi.flo.bts/
OU avec l'adresse IP http://172.30.10.4/GLPI
On se connecte à l'aide des logins/password suivant :
User: root
Password: root

GLPI utilise apache2 + php5 + mysql

MOODLE

MOODLE est une solution de plate forme collaborative initialement destinée aux enseignants.
Site officiel de MOODLE: https://moodle.org/

MOODLE est installé sur une distribution Debian 8 (Jessie), voici sa configuration :

Interface	Adresse IP	Route par défaut	VLAN	ZONE
eth0	172.30.30.7	172.30.30.254	VLAN : 21	DMZ

Les serveurs DNS renseignés dans le resolv.conf sont 172.30.10.2 et 172.30.30.254

Pour accéder à l'interface WEB de GLPI, on utilise l'URL :
http://moodle.flo.bts/
OU avec l'adresse IP http://172.30.30.7
On se connecte à l'aide des logins/password suivant :
User: admin_moodle
Password: @1ROOTmoodle.bts

MOODLE utilise apache2 + php5 + mysql

OpenMediaVault

OpenMediaVault est une solution open source destinée aux serveurs de stockage en réseau NAS, il est basé sur Debian.
Site officiel de OpenMediaVault : http://www.openmediavault.org/

OpenMediaVault est installé sur une distribution Debian 8 (Jessie), voici sa configuration :

Interface	Adresse IP	Route par défaut	VLAN	ZONE
eth0	172.30.10.3	172.30.10.254	VLAN : 22	ZS

Les serveurs DNS renseignés dans le resolv.conf sont 172.30.10.2 et 172.30.10.254

Pour accéder à l'interface WEB de OpenMediaVault, on utilise l'URL :
http://nas.flo.bts/
OU avec l'adresse IP http://172.30.10.3/openmediavault
On se connecte à l'aide des logins/password suivant :
User: admin
Password: openmediavault

Les logins/password du compte root de OpenMediaVault sont :
User: root
Password: root

OWNCLOUD

Owncloud est une plateforme open source de services de stockage et partage de fichiers et d'applications diverses. Il est utilisé comme service de Cloud pour le réseau local, ainsi on obtient le total contrôle des accès aux ressources héberger par ce Cloud privé.
Site officiel de Owncloud: https://owncloud.org/

Owncloud est installé sur une distribution Debian 8 (Jessie), voici sa configuration :

Interface	Adresse IP	Route par défaut	VLAN	ZONE
eth0	172.30.30.8	172.30.30.254	VLAN : 21	DMZ

Les serveurs DNS renseignés dans le resolv.conf sont 172.30.10.2 et 172.30.30.254

Pour accéder à l'interface WEB de Owncloud, on utilise l'URL :
https://owncloud.flo.bts/
OU avec l'adresse IP https://172.30.30.8
On se connecte à l'aide des logins/password suivant :
User: root_owncloud
Password: @1ROOTowncloud.bts

Les logins/password du compte root de Owncloud sont :
User: root
Password: root

Les logins/password du compte pour Mariadb sont :
User: root
Password: root

Owncloud utilise nginx + php5-fpm + php5 + mariadb

Windows Server (serveur DNS + Active Directory + RADIUS)

Windows Server est installé avec la version 2008 R2, voici sa configuration :

Interface	Adresse IP	Route par défaut	VLAN	ZONE
eth0	172.30.10.2	172.30.10.254	VLAN : 22	ZS

Les serveurs DNS renseignés dans la configuration Ipv4 de l'interface sont 127.0.0.1 et 172.30.10.254

Les logins/password du compte admin sont :
User: Administrateur
Password: template

Les logins/password du compte admin (en réseau) sont :
User: administrateur
Password: @1ROOTwindows

Windows Serveur a les rôles Active Directory, DNS, NPS (Network Policy Server, utilisé pour faire RADIUS).

Active Directory :
L'Active Directory gère les comptes des utilisateurs du LAN.
Le domaine utilisé est : flo.bts
Les comptes enregistrés dans l'Active Directory sont :
- User : Flo MDP : @1ROOTflo.bts
- User : Tim MDP : @1ROOTtim.bts
- User : Tom MDP : @1ROOTtom.bts

DNS :
La configuration du DNS sur le Windows Serveur est nécessaire pour le fonctionnement d'Active Directory mais elle est aussi nécessaire pour l'utilisation locale de nom DNS pour les serveurs du réseau de la maquette.
Les paramètres suivants sont configurés :

Name	Type	Data
pfsense	Host (A)	172.30.20.254
supervision	Host (A)	172.30.10.5
owncloud	Host (A)	172.30.30.8
moodle	Host (A)	172.30.30.7
glpi	Host (A)	172.30.10.4
nas	Host (A)	172.30.10.3
ad	Host (A)	172.30.10.2

NPS :
Configuration du client RADIUS de Liaison :
nom : client_liaison
Adresse IP : 172.30.30.254
secret partagé : liaison
nom de la Stratégie réseau associé : portail captif
Nom convivial : Radius
Secret partagé : RADIUS

LAN

La LAN (Local Area Network) est la zone consacrée aux utilisateurs, elle n'y contient aucun serveur et assure une certaine sécurité grâce au portail captif dont l'authentification se fait par le serveur RADIUS, le proxy et son antivirus intégré ainsi que le pare feu pfSense. La LAN est associée au VLAN 27, les adresses IP sont distribuées via un serveur DHCP.
Les clients du LAN dans la maquette sont des clients Windows 7, Slitaz et Debian 8 (Jessie).
Les serveurs DNS associés aux équipements de la LAN sont 172.30.10.2 et 172.30.20.254.
La passerelle par défaut est 172.30.20.254. Son adresse de réseau est 172.30.20.0/24.

DMZ

La DMZ (DeMilitarized Zone ou zone démilitarisée en français) est la zone consacrée aux serveurs qui pourront être accessibles depuis Internet. Ainsi, les serveurs Owncloud et Moodle sont placés dans la DMZ car il seront accessibles depuis l'interface WAN, donc depuis internet. La DMZ est associée au VLAN 21.
La passerelle par défaut est 172.30.30.254. Son adresse de réseau est 172.30.30.0/24.

ZS

La ZS est une Zone Sécurisée consacrée aux serveurs qui ne seront pas accessibles depuis Internet, on y retrouve ainsi les serveurs : Windows Server, OpenMediaVault, GLPI et Centreon. Ils ne doivent pas être accessibles depuis Internet pour une raison de sécurité mais, ne doivent pas non plus être dans la zone LAN, la zone ZS est donc spécialement faite pour ces serveurs qui de par leurs contenu, leurs services et leur vocation n'ont pas à être accessibles depuis Internet. Toutefois, on peut y accéder depuis Internet en utilisant un Client VPN qui nous rendra alors dans la LAN et en passant le portail captif puis le proxy, nous seront à même d'accéder aux serveurs de la ZS. C'est une manière de sécuriser l'accès des serveurs grâce à une authentification.
La ZS est associée au VLAN 22.
La passerelle par défaut est 172.30.10.254. Son adresse de réseau est 172.30.10.0/24.

PC ADMIN

Le PC ADMIN est le PC de l'administrateur, c'est un poste sous Windows 7, il a tous les droits sur tous les équipements du réseau et possède un accès partout. Il peut changer de VLAN s'il en a besoin, mais il est initialement situé dans la LAN avec une IP fixe qui n'est pas dans la plage IP du serveur DHCP. Son IP fixe est 172.30.20.1, il utilise l'adresse par défaut 172.30.20.254 et les serveurs DNS : 172.30.10.2 et 172.30.30.254.
Pour se connecter à la session du PC ADMIN, on utilise les logins/password :
User: Admin
Password: template
Le PC ADMIN étant un PC d'administrateur réseau, il possède un certain nombre de logiciel pour mener à bien sa mission dont voici la liste :
- nmap
- chrome
- firefox
- wireshark
- notepadd++
- openvpn
- putty
- winscp
- pentestbox
- python