Dossier d'Architecture Technique

Implémentation et configuration d'une infrastructure hautement disponible pour Train Commander

SUPINFO International University

Versions :

VERSION	DATE	OBJET DE LA MODIFICATION
1.0	01/06/2016	Création du document
1.1	03/06/2016	Mise en page des schémas
2.0	09/06/2016	Version finale

Vos interlocuteurs :

NOM	FONCTION	TELEPHONE	MAIL
Jérémy KOSTECKI	Chef de Projets / Architecte Réseau et Sécurité	+33 6 73 61 38 24	170262@supinfo.com
Jonathan MECHIN	Architecte Système / Linux / SAN	+33 6 58 57 97 48	171868@supinfo.com
Eliott VERNIERES	Architecte Microsoft Windows / Exchange	+33 6 23 85 36 65	169975@supinfo.com

Documents de référence :

VERSION	DOCUMENT
2.0	DAT_TC_2016.dox

Clause de confidentialité

Toute information contenue dans ce document strictement confidentiel est fournie à Train Commander dans le seul but de répondre à la requête de Train Commander et ne peut être utilisée à d'autres fins.

Train Commander s'engage à ne pas publier ni faire connaître tout ou partie de ces informations à quelque tierce partie que ce soit, sans l'autorisation préalable de SoftNet SAS.

Terminologie

Expression ou acronyme	Définition

1. Sommaire

1. Sommaire 3

2. Introduction 4

2.1. Objectif du document 4

2.2. Périmètre du document 4

3. Architecture Hautement Disponible 5

3.1. Choix technologiques 5

3.1.1. Serveurs 5

3.1.2. Réseau et Sécurité 5

3.1.3. SAN 6

3.2. Contraintes et exigences 6

3.3. Architecture cible 6

3.3.1. Vue d'ensemble de l'infrastructure 6

3.3.2. Redondance de l'infrastructure 7

3.3.3. Dimensionnement de l'infrastructure 9

3.3.4. Plan d'adressage IP 9

3.3.5. Matrice de flux 11

4. Annexes ..... **Erreur ! Signet non défini.**

2. Introduction

2.1. Objectif du document

Le présent document a pour objectif de présenter l'ensemble des spécifications détaillées et fonctionnelles de l'architecture cible hautement disponible à déployer chez Train Commander par SoftNet SAS.

Cette solution doit répondre aux exigences de Train Commander.

2.2. Périmètre du document

Dans ce document, les paramètres de configurations précisés sont ceux qui s'appliquent à Windows Server 2012R2, Ubuntu Server 16.04, PfSense 2.3.1, Exchange 2013 SP1, SQL Server 2014 et FreeNAS 9.10. Il s'agit des choix technologiques retenus pour ce projet.

Le document comprend :

- Une présentation de l'architecture globale
- Une présentation de la redondance de l'architecture
- Les décisions d'architectures retenues dans le contexte du projet

Le document ne comprend pas les procédures d'installation et de configuration détaillés des plateformes qui seront décrites dans des documents dédiés à cet effet.

3. Architecture Hautement Disponible

3.1. Choix technologiques

Différentes technologies ont été employées dans cette architecture, à la fois des technologies open source mais aussi des technologies propriétaires. Les technologies utilisées en sécurité et réseau sont entièrement open source, tout simplement parce que ce sont des outils fiables et qui ont fait leur preuve avec une grande granularité en termes d'options et de configuration. Pour ce qui est du stockage, les technologies utilisées sont aussi entièrement open source. Tout le reste repose sur des technologies propriétaires Microsoft.

Afin de limiter les coûts, cette architecture utilise des technologies de virtualisation grâce à l'utilisation de VMware ESXi.

3.1.1. Serveurs

Les serveurs utilisés dans cette architecture sont : Windows Server 2012 R2 et Ubuntu Server 16.04.

Les services Windows Server utilisés dans cette architecture sont : IIS, Active Directory, Exchange.

IIS est utilisé pour stocker l'intégralité du site internet sauf la base de données qui sera stockée à part dans le SAN. Le choix du serveur web s'est porté sur IIS à cause du fait que le langage de programmation utilisé pour développer la solution soit de l'ASP.NET.

Active Directory est utilisé pour gérer les administrateurs et utilisateurs du système ainsi que les objets Exchange.

Exchange est utilisé en tant que serveur de messagerie afin d'envoyer les emails de confirmation de commande, recevoir les mails de réclamation et gérer les mails internes.

Les services Ubuntu Server 16.04 sont : Proxy, Reverse Proxy et Cache.

Notre choix s'est porté sur Ubuntu Server pour ces services du fait de sa légèreté mais aussi de sa robustesse.

3.1.2. Réseau et Sécurité

Dans le cas du domaine du réseau et de la sécurité, nous avons choisi la solution PFsense basé sur FreeBSD qui nous sert à la fois de pare-feu, de passerelle VPN et de routeur. C'est une solution légère, gratuite et fiable, idéale pour un environnement virtualisé.

3.1.3. SAN

FreeNAS basé sur FreeBSD nous permet d'obtenir un fonctionnement proche d'un SAN pour un coût moins élevé grâce à sa gratuité.

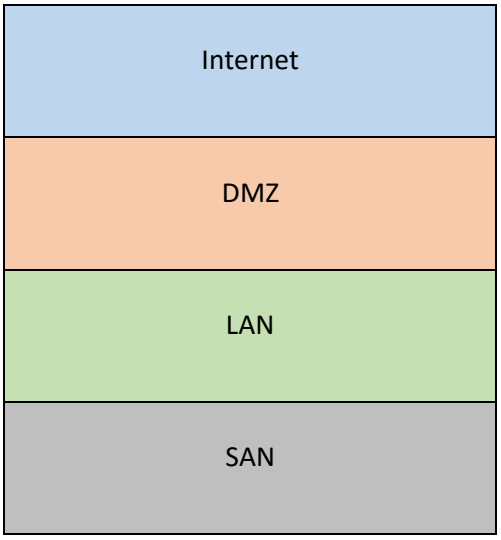
3.2. Contraintes et exigences

- Train Commander souhaite pouvoir proposer l'intégralité des trajets offerts par la SNCF. A cette fin, les serveurs devront pouvoir utiliser une API capable d'échanger avec l'API de la SNCF.
- L'architecture devra être réparti entre deux Datacenter en actif/passif avec un basculement immédiat en cas de défaillance du site principal.
- L'architecture devra pouvoir héberger l'intégralité des collaborateurs de Train Commander.
- L'architecture devra pouvoir support à minima un nombre de 100 000 utilisateur/jours et donc potentiellement 100 000 commandes/jours.

3.3. Architecture cible

3.3.1. Vue d'ensemble de l'infrastructure

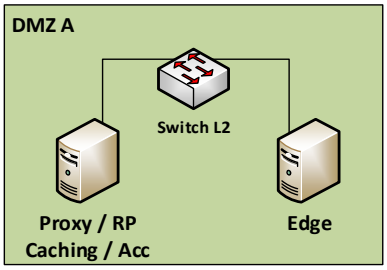
L'architecture cible se décompose en plusieurs blocs :



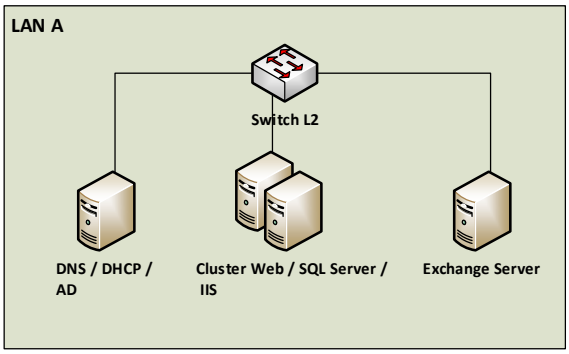
Internet : Un pool d'adresses publiques a été affecté par le fournisseur d'accès internet.

DMZ : Zone tampon entre le réseau interne et internet. Cette zone permet de sécuriser l'infrastructure tout en permettant aux visiteurs ou clients de pouvoir se connecter au serveur et

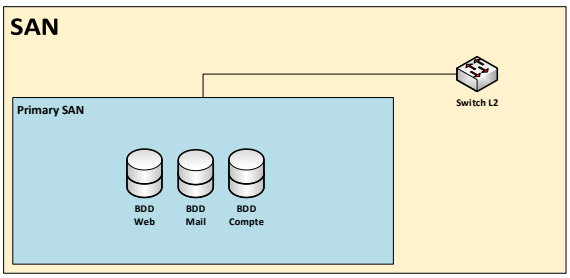
ainsi passer leur commande. La transition entre la zone DMZ et le LAN se fera au travers d'un reverse proxy.



LAN : Partie interne du réseau sur laquelle se trouve les serveurs.



SAN : Serveur de stockage de données en réseau.



Il est mis en place un pare-feu entre chacun des blocs afin d'étanchéifier chacun des blocs. Les flux sont filtrés au travers de règles de pare-feu précises.

3.3.2. Redondance de l'infrastructure

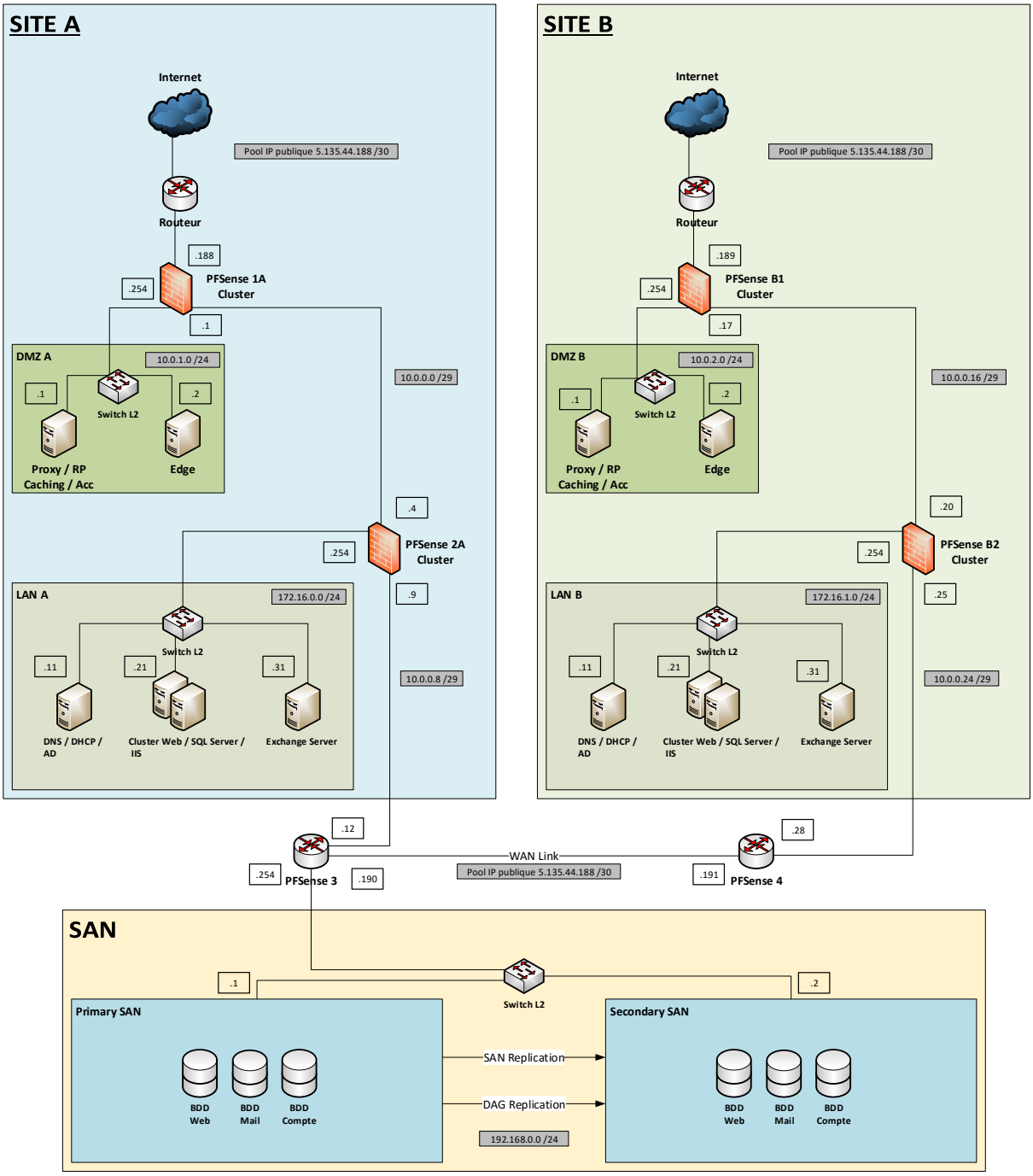
Afin d'assurer une disponibilité permanente du site Train Commander on s'appuiera sur deux Datacenter situés sur deux lieux géographiquement distincts. Ils fonctionneront en mode actif/passif, le second prenant le relais dès que le premier site rencontre des problèmes divers.

Afin de fiabiliser les sites, les éléments de chaque site seront redondés. Cela inclus entre autres les pare-feu, le serveur web ainsi que le SAN.

Afin de s'assurer que les données sont identiques entre les deux sites, leurs ressources seront communes et disponibles sur le SAN.

Le SAN se situant à proximité du Site A, l'interconnexion entre le site A et le site B se fera au travers d'un lien WAN dédié, les communications transitant à travers un VPN.

L'architecture finale ressemblera à cela :



3.3.3. Dimensionnement de l'infrastructure

L'infrastructure de compose de la manière suivante :

- 10 serveurs PFsense (dont 4 clusters de 2 serveurs)
- 2 serveurs Proxy
- 2 serveurs Edge
- 2 serveurs Active Directory
- 4 serveurs Web (2 clusters de 2 serveurs)
- 2 serveurs Exchange
- 2 serveurs FreeNAS

Le lien WAN vers l'extérieur pour chacun des sites doit être au minimum de 100Mo/s et l'interconnexion entre les sites A et B soit être aussi de 100Mo/s.

Les serveurs soivent être composés d'un processeur récent de type Intel Xeon et d'au minimum 1Go de RAM pour les serveurs Ubuntu et FreeBSD et d'au minimum 2Go de RAM pour les serveurs Windows Server. Les serveurs Web devront être équipés de 4Go au minimum afin de minimiser les ralentissements en période de forte affluence sur le site. Les serveurs Exchange seront composés d'au minimum 4Go comme préconisé par Microsoft.

3.3.4. Plan d'adressage IP

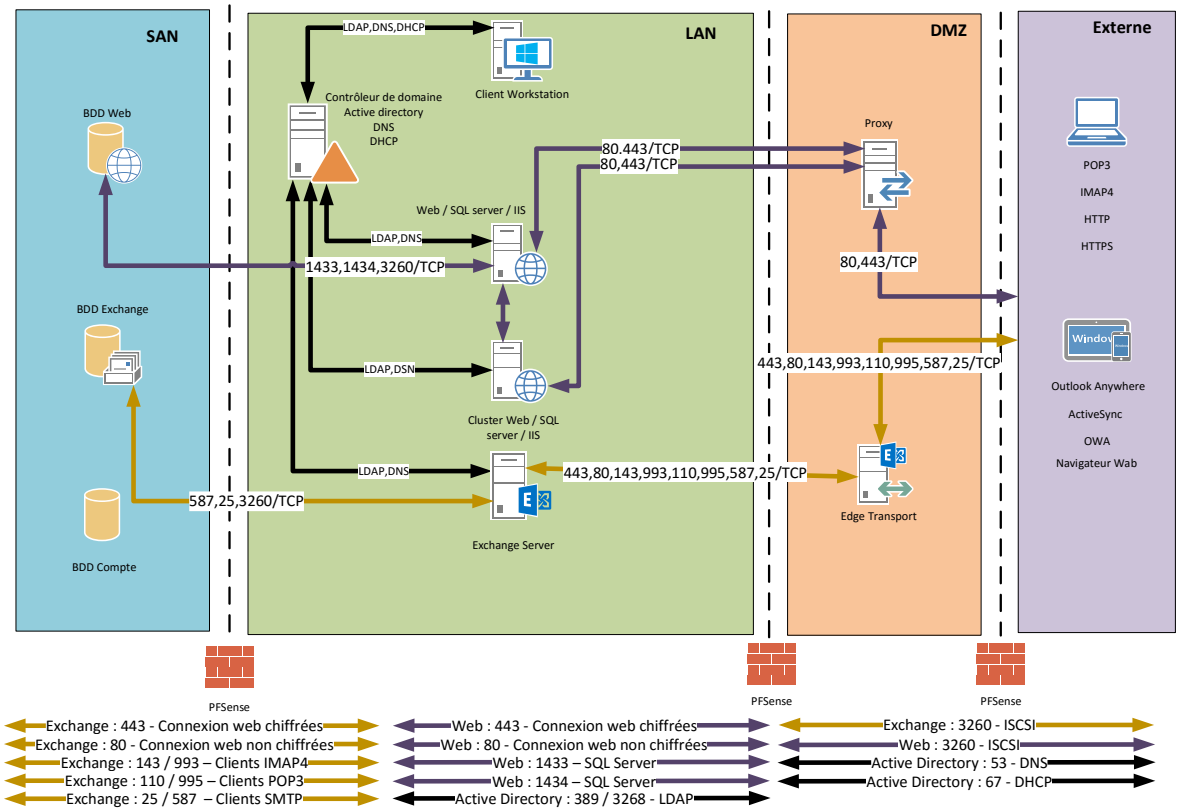
Liste des sous réseaux et VLAN associés :

Subnets	VLANs	Descriptions
10.0.0.0/29	10	Interco DMZ A – LAN A
10.0.0.8/29	11	Interco LAN A - SAN
10.0.0.16/29	12	Interco DMZ B – LAN B
10.0.0.24/29	13	Interco LAN B - SAN
10.0.1.0/24	20	DMZ A
10.0.2.0/24	21	DMZ B
172.16.0.0/24	30	LAN A
172.16.1.0/24	31	LAN B
192.168.0.0/24	40	SAN

Liste des équipements et IP associés :

Equipements	Adresses IP
PfSense 1A WAN	5.135.44.188
PfSense 1A DMZ	10.0.1.254 /24
PfSense 1A INTERCO DMZ LAN	10.0.0.1 /29
PfSense 1B WAN	5.135.44.189
PfSense 1B DMZ	10.0.2.254 /24
PfSense 1B INTERCO DMZ LAN	10.0.0.17 /24
PfSense 2A INTERCO DMZ LAN	10.0.0.4 /29
PfSense 2A INTERCO LAN SAN	10.0.0.9 /29
PfSense 2A LAN	172.16.0.254 /24
PfSense 2B INTERCO DMZ LAN	10.0.0.20 /29
PfSense 2B INTERCO LAN SAN	10.0.0.25 /29
PfSense 2B LAN	172.16.1.254 /24
PfSense 3 INTERCO LAN SAN	10.0.0.12 /29
PfSense 3 WAN VPN	5.135.44.190
PfSense 3 SAN	192.168.0.254 /24
PfSense 4 INTERCO LAN SAN	10.0.0.28 /29
PfSense 4 WAN VPN	5.135.44.191
Proxy / RP DMZ A	10.0.1.1 /24
Proxy / RP DMZ B	10.0.2.1 /24
Edge DMZ A	10.0.1.2 /24
Edge DMZ B	10.0.2.2 /24
DNS / DHCP / AD LAN A	172.16.0.11 /24
Cluster Web / SQL / IIS LAN A	172.16.0.21 /24
Cluster Web / SQL / IIS LAN A (1)	172.16.0.22 /24
Cluster Web / SQL / IIS LAN A (2)	172.16.0.23 /24
Exchange Server LAN A	172.16.0.31 /24
DNS / DHCP / AD LAN B	172.16.1.11 /24
Cluster Web / SQL / IIS LAN B	172.16.1.21 /24
Cluster Web / SQL / IIS LAN B (1)	172.16.1.22 /24
Cluster Web / SQL / IIS LAN B (2)	172.16.1.23 /24
Exchange Server LAN B	172.16.1.31 /24
Primary SAN	192.168.0.1
Secondary SAN	192.168.0.2

3.3.5. Matrice de flux



3.3.6. Evolutivité de l'architecture

L'architecture possède les brique d'une architecture évolutive :

- Un stockage solide en SAN, permettant via son protocole standard de s'adapter à toutes les technologies le rendant universelle de plus ajouter ou diminuer le volume de stockage est simplifié

- Des serveurs de dernières générations permettes une plus grande compatibilité entres eux, de plus l'intégration future de plusieurs technologies compatibles.