3TI - 2017-2018

Réseau d'entreprise

OKLN

Groupe B

---

7 Février 2018

1 Introduction

2 Infrastructure réseau

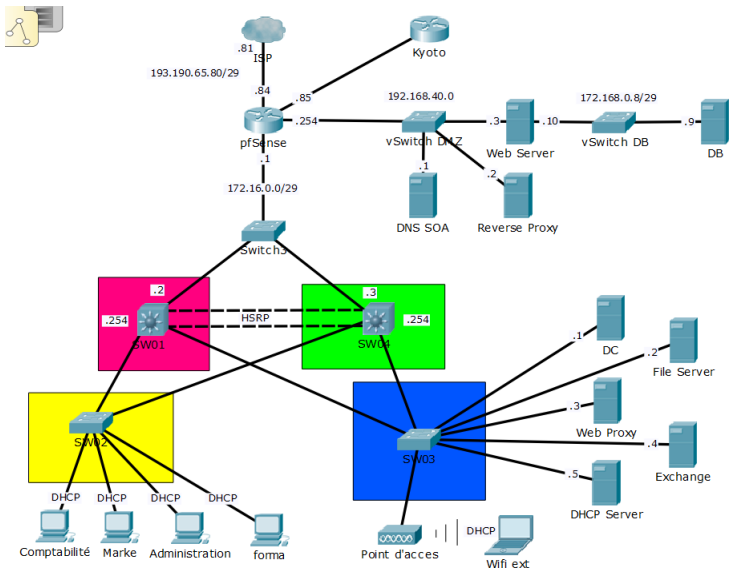
2.1 Tâches réalisées

— Finition de l'infrastructure
— Test de simulation packet tracer
— Reset stack number
— Configuration de vtp
— Telnet pour les switchs L2
— Cablage des différents switchs

2.2 Difficultés rencontrées

— Pas de ssh sur les L2 => utilisation de telnet
— Pas de vtp sur les switchs L2

2.3 Topologie améliorée



2.4 Table d'adressage

Services	**192.168.10.0/24**
Domain Control	192.168.10.1
File Server	192.168.10.2
Web Proxy	192.168.10.3
Exchange	192.168.10.4
DHCP Server	192.168.10.5
Guest	**192.168.30.0/24**
DMZ	**192.168.40.0/24**
DNS SOA	192.168.40.1
Reverse Proxy	192.168.40.2
Web Server	192.168.40.3
User	**192.168.50.0/24**
Management	**192.168.60.0/24**
Core-to-Distrib	**172.16.0.0/29**
pfSense	172.16.0.1
SW01	172.16.0.2
SW02	172.16.0.3
Petit ESXi	172.16.0.4
PC Team Deploy	172.16.0.5
PC Team Secu	172.16.0.6
Web-to-DB	**172.16.0.8/29**
Database	172.16.0.9
Web Server	172.16.0.10

2.5 configuration IOS

Cfr Annexe.

3 Ressources Informatiques

3.1 Tâches réalisées

- Activation de DHCP et la configuration des vlan à l'intérieur de ce dernier
  - Vlan User
  - Vlan Guest
- Configuration du DNS (nom de domaine , Adresse IP...)
- Configuration du serveur windows File et l'attribution des adresses IP

3.2 Difficultés rencontrées

- Suite à un problème de délégation du DNS, nous avons refait un nouveau serveur Windows bien propre.
- Un problème de liaison entre l'Active Directory et le service DNS

4 Mail

4.1 Tâches réalisées

— Téléchargement et installation d'Exchange 2016 sur le serveur Windows (mail) – NON FINI

— — Rôle de boîtes aux lettres
  — Nom d'organisation : OKLN
  — Protection contre les porgrammes malveillants actif

4.2 Difficultés rencontrées

— Bug d'administration du DC et pas d'accès internet pour installer les différents services nécessaires.

5 Sécurité

5.1 Tâches réalisées

— Documentation sur le package quagga OSPF (pfSense)
— Configurer openVPN
— OSPF sur pfSense
— Reverse Proxy
— Mise en place du DNS

5.2 Problèmes rencontrés

openVPN : Il reste encore certains problèmes à régler mais nous sommes en bonne voie. Nous avons eu quelques problèmes car il n'y avait pas de DNS en place.

DNS : Il n'y a pas eu de problèmes majeurs excepté l'absence d'un " ;" dans un fichier de config.

6 Logistique

6.1 Tâches réalisées

Comme les jours précedents, à notre arrivé nous prenons toujours un petit quart d'heure pour vérifier que le matériel est toujours bien en place et est complet. Aujourd'hui nous avons eu besoin de faire des câbles croisés pour connecter les switch entre eux. Étant donné que nous n'en avions pas assez on à du les faire nous-mêmes et nous remémorer les labo de Telecom que nous avions eu les années précédentes. Nous avons bien veillé à ce que l'endroit où nous avons fait les câbles soit propre après notre passage. Nous avons aussi rangé deux switch que nous n'avions plus besoin pour ne pas encombrer le local.

7 Services internet

7.1 Tâches réalisées

— configuration du serveur nginx (Cfr. Annexe)

8 Déploiement

8.1 Tâches réalisées

— Nous avons commencé par installer un serveur de type Windows Server 2016. Nous l'avons ensuite dupliqué pour mettre en place les services suivants :
  — Windows Server Active Directory
  — Windows Server Exchange
  — Windows Server Deploy
— Nous avons ensuite veillé à ce que la configuration des machines virtuelles soit réalisée correctement, nous avons ensuite mis en place la configuration ip.
— Nous avons également mis en place un service DHCP pour simplifier l'administration.
— Nous avons finalement installé une machine Debian, vouée à être dupliquée par la suite pour mettre en place le proxy.

8.2 Difficultés rencontrées

Swapping de fichier ? ? Plus de détails...

9 sources

9.1 Sécurité

— quagga pfSense package `https://forum.pfsense.org/index.php?topic=126842.0`
— quagga pfSense package `https://forum.pfsense.org/index.php?topic=126842.15`
— openVPN `https://en.wikipedia.org/wiki/Certificate_revocation_list`

9.2 Mail

— `https://www.microsoft.com/en-us/download/details.aspx?id=49161`

A config web NGINX

```
server {
    listen   80; ## listen for ipv4; this line is default and implied
    listen   [::]:80 default ipv6only=on; ## listen for ipv6

    root /code/www/;
    index index.php index.html index.htm test.php;

    # Make site accessible from http://localhost/
    server_name www.okln.ephec-ti.be;

    # Redirection HTTP vers HTTPS
        # return 301 https://$server_name$request_uri;

    # Disable sendfile as per https://docs.vagrantup.com/v2/synced-folders/virtualbox.html
    sendfile off;

    # Add stdout logging
    error_log /dev/stdout info;
    access_log /dev/stdout;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to index.html
        try_files $uri $uri/ =404;
    }

    error_page 404 /404.html;
        location = /404.html {
                root /code/404/;
                internal;
        }

        location ^~ /ngd-style.css {
            alias /var/www/errors/style.css;
            access_log off;
        }

        location ^~ /ngd-sad.svg {
            alias /var/www/errors/sad.svg;
            access_log off;
        }

    # pass the PHP scripts to FastCGI server listening on socket
    #
    location ~ \.php$ {
                try_files $uri =404;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_pass unix:/var/run/php-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
            fastcgi_param SCRIPT_NAME $fastcgi_script_name;
        fastcgi_index index.php;
        include fastcgi_params;
    }

        location ~* \.(jpg|jpeg|gif|png|css|js|ico|webp|tiff|ttf|svg)$ {
                expires           5d;
        }

    # deny access to . files, for security
    #
    location ~ /\. {
            log_not_found off;
            deny all;
    }

    location ^~ /.well-known {
```

```
                allow all;
                auth_basic off;
        }

}

server{
    listen 443 ssl;
    root /code/www;

    server_name www.okln.ephec-ti.be;

        ssl_certificate /code/certs/live/www.okln.ephec-ti.be/fullchain.pem;
        ssl_certificate_key /code/certs/live/www.okln.ephec-ti.be/privkey.pem;

        ssl_stapling on;
        ssl_stapling_verify on;
        ssl_trusted_certificate /code/certs/live/www.okln.ephec-ti.be/fullchain.pem;

        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_prefer_server_ciphers on;
        ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';

        #Redirection erreur page 404 perso
        error_page 404 /404.html;
        location = /404.html {
                root /code/404/;
                internal;
        }

}
```

B config infra packet tracer

```
------
CSW01
-----
!

enable
conf t
hostname CSW01
service password-encryption
!configuration de base
!
ip domain-name okln.ephec-ti.be
crypto key generate rsa
2048
!
no ip domain-lookup
banner login "Access for authorized users only !"
service password-encryption
username admin privilege 15
enable secret cisco
ip ssh time-out 15
ip ssh authentication-retries 3
line console 0
  password cisco
  logging synchronous
  login
  exit
line vty 0 4
  login local
  transport input ssh
  exec-timeout 3 30
```

```
!
!
!-------------------------creation des vlan-----------------------------------------------------------------
!vlan database
vlan 10
name service
vlan 30
name guest
vlan 50
name user
vlan 60
name management
!-------------------------------------------------------------------------------
! SVI
interface vlan 10
  description "vers le VLAN service"
  ip address 192.168.10.254 255.255.255.0
  no shutdown
!
interface vlan 30
  description "vers le VLAN guest"
  ip address 192.168.30.254 255.255.255.0
  ip helper-address 192.168.10.8
  no shutdown
!
interface vlan 50
  description "vers du VLAN user"
  ip address 192.168.50.254 255.255.255.0
  ip helper-address 192.168.10.8
  no shutdown
!
interface vlan 60
  description "vers le VLAN management"
  ip address 192.168.60.254 255.255.255.0
  no shutdown
!

!
! - Configuration de VTP
!
vtp mode server
vtp domain okln.ephec-ti.be
vtp pruning
vtp password cisco
!
! - Configuration des interfaces
!
interface f1/0/1
  description "vers core-to-distribu(f0/1)"
  no switchport
  ip address 172.16.0.2 255.255.255.248
  no shut
!
interface f1/0/2
  description "Vers SW01 (f1/0/1)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f1/0/3
  description "Vers SW02(f1/0/1)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f1/0/4
  description "Vers CSW02(f1/0/1)"
  switchport trunk encapsulation dot1q
```

```
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f1/0/5
  description "Vers CSW02(f1/0/2)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!

! - Routage
!
ip routing
router ospf 1
        network 172.16.0.0 0.0.0.7 area 0
        network 192.168.10.0 0.0.0.255 area 0
        network 192.168.30.0 0.0.0.255 area 0
        network 192.168.50.0 0.0.0.255 area 0
        network 192.168.60.0 0.0.0.255 area 0
exit
!
!router rip
!version 2
!network 172.16.0.0 0
!network 192.168.10.0
!network 192.168.30.0
!network 192.168.50.0
!network 192.168.60.0
!no auto-summary
!
! syslog
!
!logging 192.168.10.2
!logging trap debbuging
!logging on
!
! NTP
!
!ntp server 192.168.10.2
!
! DNS
!
ip name-server 192.168.10.5
ip domain-lookup
!
! Spanning-tree
!
spanning-tree vlan 10 root primary
spanning-tree vlan 30 root secondary
spanning-tree vlan 50 root secondary
spanning-tree vlan 60 root primary
!
!
-----
-----
HSRP
----
----
interface f1/0/1
standby 100 ip 172.16.0.1
standby 100 preempt
-------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------
!
----
!CSW02
----
!
```

```
enable
conf t
hostname CSW02
service password-encryption
! - configuration de base-----
!
ip domain-name okln.ephec-ti.be
crypto key generate rsa
2048
!
no ip domain-lookup
banner login "Access for authorized users only !"
service password-encryption
username admin privilege 15
enable secret cisco
ip ssh time-out 15
ip ssh authentication-retries 3
line console 0
  password cisco
  logging synchronous
  login
  exit
line vty 0 4
  login local
  transport input ssh
  exec-timeout 3 30
!
! ------------------------------------------------------------------------------
!------------------------creation des vlan-------------------------------------
vlan 10
name service
vlan 30
name guest
vlan 50
name user
vlan 60
name management
!------------------------------------------------------------------------------
!
interface vlan 10
  description "vers du VLAN service"
  ip address 192.168.10.254 255.255.255.0
  no shutdown
!
interface vlan 30
  description "vers du VLAN gest"
  ip address 192.168.30.254 255.255.255.0
  ip helper-address 192.168.10.8
  no shutdown
!
interface vlan 50
  description "vers du VLAN user"
  ip address 192.168.50.254 255.255.255.0
  ip helper-address 192.168.10.8
  no shutdown
!
interface vlan 60
  description "vers du VLAN management"
  ip address 192.168.60.254 255.255.255.0
  no shutdown
!

!
! - Configuration de VTP
!
vtp mode server
vtp domain okln.ephec-ti.be
vtp pruning
```

```
vtp password cisco
!
! - Configuration des interfaces
!
interface f1/0/1
  description "vers core-to-distribu(f0/1)"
  no switchport
  ip address 172.16.0.3 255.255.255.248
  no shut
!
interface f1/0/2
  description "Vers CSW01(f0/5)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f1/0/3
  description "Vers CSW01(f0/4)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f1/0/4
  description "Vers vlan management"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f1/0/5
  description "Vers vlan management"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!

! - Routage
!
ip routing
router ospf 1
        network 172.16.0.0 0.0.0.7 area 0
        network 192.168.10.0 0.0.0.255 area 0
        network 192.168.30.0 0.0.0.255 area 0
        network 192.168.50.0 0.0.0.255 area 0
        network 192.168.60.0 0.0.0.255 area 0
exit
!
!router rip
!version 2
!network 172.16.0.0 0
!network 192.168.10.0
!network 192.168.30.0
!network 192.168.50.0
!network 192.168.60.0
!no auto-summary
!
! syslog
!
!logging 192.168.30.2
!logging trap debbuging
!logging on
!
! NTP
!
!ntp server 192.168.10.2
!
! DNS
!
ip name-server 192.168.10.5
```

```
ip domain-lookup
!
! Spanning-tree
!
spanning-tree vlan 10 root secondary
spanning-tree vlan 30 root primary
spanning-tree vlan 50 root primary
spanning-tree vlan 60 root secondary
!
-----
-----
HSRP
----
----
interface f1/0/1
standby 100 ip 172.16.0.1
standby 100 priority 110
standby 100 preempt
--------------------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------
hostname SW01
! ----------------------------------------------------------------------------
!
!
!

enable
conf t
hostname SW01
service password-encryption
! - configuration de base
!
ip domain-name okln.ephec-ti.be
crypto key generate rsa
2048
!
no ip domain-lookup
banner login "Access for authorized users only !"
service password-encryption
username admin privilege 15
enable secret cisco
ip ssh time-out 15
ip ssh authentication-retries 3
line console 0
  password cisco
  logging synchronous
  login
  exit
line vty 0 4
  login local
  transport input ssh
  exec-timeout 3 30
!
exit
! - Création des VLANs
!
!vlan database
!vlan 10 name service
!vlan 30 name guest
!vlan 50 name user
!vlan 60 name management
!
interface vlan 10
  description "vlan de service reseau"
  ip address 192.168.10.253 255.255.255.0
  no shutdown
!
ip default-gateway 192.168.10.254
```

```
!
! - Configuration de VTP
!
vtp mode transparent
vtp mode client
vtp password cisco
vtp domain okln.ephec-ti.be
!
!Configuration des interfaces
!
interface range F0/1 - 2
  description "CSW01"
  switchport trun encapsulation dotq1
  switchport mode trunk
  switchport trunk native vlan 60
  no ip routing
!
!
interface range F0/3 - 10
  description "vlan user"
  switchport mode access
  switchport access vlan 50
   no shutdown
!
interface range F0/11 - 24
  description "non utilise"
  switchport mode access
  switchport access vlan 50
  shutdown
!

------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------------------------------
hostname SW02
! ------------------------------------------------------------------------
!
!
!
!
enable
conf t
hostname SW02
service password-encryption
! - configuration de base
!
ip domain-name okln.ephec-ti.be
crypto key generate rsa
2048
!
no ip domain-lookup
banner login "Access for authorized users only !"
service password-encryption
username admin privilege 15 secret cisco
ip ssh time-out 15
ip ssh authentification-retries 3
line console 0
  password cisco
  logging synchronous
  login
  exit
line vty 0 4
  login local
  transport input ssh
  exec time-out 3 30
!
! - Création des VLANs
!
!vlan database
```

```
!vlan 10 name service
!vlan 30 name guest
!vlan 50 name user
!vlan 60 name management
!
interface vlan 10
  description "vlan de service reseau"
  ip address 192.168.10.252 255.255.255.0
  no shutdown
!
ip default-gateway 192.168.10.254
!
! - Configuration de VTP
!
vtp mode transparent
vtp mode client
vtp password cisco
vtp domain okln.ephec-ti.be
!
! - Configuration des interfaces
!
interface range F0/1 - 2
  description "CSW01"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
  no ip routing
!
!
interface range F0/3 - 10
  description "vlan user"
  switchport mode access
  switchport access vlan 50
  no shutdown
  exit
!
interface range F0/11 - 24
  description "non utilise"
  switchport mode access
  switchport access vlan 50
  shutdown
!
```