3TI - 2017-2018

Réseau d'entreprise

OKLN - Jour 2

Groupe B

---

6 Février 2018

1 Introduction

Pour cette seconde journée du cours de de réseau d'entreprise, l'équipe a été confronté à pas mal de problèmes dont la résolution est difficile. Cela a entrainé dès lors du retard sur le planning. Vous trouverez ci-dessous les points de vue de chaque groupe de travail et leurs difficultés rencontrées.

2 Infrastructure réseau

2.1 Tâches réalisées

Le 5 Février 2018, nous avons réalisé une infrastructure adaptée à nos besoins. Nous avions réalisé les schémas logiques et physiques correspondant. Cependant, suite à notre entretien avec M. Schalkwijk, nous avons apporté quelques modifications à celles-ci.

Nous avons commencé par mettre en place les VLANs tels que définis dans le schéma logique.

La seconde étape a été la configuration IP de notre réseau. Sans cela, de nombreux services ne peuvent être installés et configurés.

Par la suite, nous avons mis en place le protocoles de routage OSPF et le protocole VTP afin de simplifier l'administration de notre infrastructure.

2.2 Difficultés rencontrées

Nous avons été confronté à quelques problèmes qui ont eu pour conséquence de ralentir notre progression. Les problèmes rencontrés ont été les suivants :

Comment mettre en place une solution de secours en cas de panne du réseau ?

La solution a été de rajouter un switch L3 dans l'infrastructure. Ainsi en cas de panne, un composant de secours pourra assurer le fonctionnement du réseau.

Comment répondre au manque d'interfaces disponibles ?

Nous avons ajouté un switch L2 supplémentaire afin d'avoir plus d'interface à disposition et ainsi augmenté la capacité du réseau.

Comment répartir les VLANs sur les switch L3 ?

Deux options se présentaient à nous. Nous pouvions soit répartir les VLANs sur les 2 switch L3 afin de partager les ressources, soit les installer sur le même switch. C'est finalement cette dernière option qui a été adoptée, le second switch L3 servira en cas de panne dans le réseau.

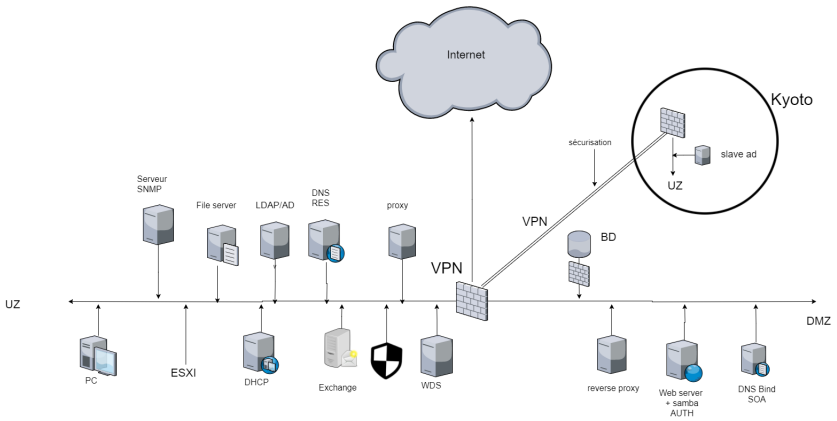
Comment définir le chemin prioritaire ?

Pour répondre à cette question, nous nous sommes tournés vers un protocole propriétaire nommé HSRP. Ce protocole va assurer une disponibilité optimale du réseau et une résistance aux pannes intéressante.

Comment assurer la sécurité des zones principales ?

Nous avons décidé de mettre la TZ et la DMZ au niveau de firewall dans le but d'améliorer la sécurité du réseau.

2.3 Topologie améliorée



2.4 Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
RT-01	Fa 0/3/0	192.168.100.85	255.255.255.0	N/A
	Fa 0/3/1	192.168.110.84	255.255.255.0	N/A
	Fa 0/3/3	172.16.0.1	255.255.255.248	N/A
Switch-1	Fa 0/1		255.255.255.0	192.168.100.85
Switch-0	Fa 0/1		255.255.255.224	192.168.110.84
SW-01	Fa 1/1		255.255.255.0	N/A
	Fa 2/1		255.255.255.0	172.16.0.1
	Fa 0/1		255.255.255.0	
SW-02 (L3)	Fa 0/6			

Table d'attribution des VLAN et des ports

Numéro de VLAN - Nom	Attribution des ports	Réseau
10 - User Zone serveurs		192.168.10.0 /24
30 - Guest		192.168.30.0 /24
N/A - DMZ		192.168.40.0 /24
50 - User		192.168.50.0 /24
60 - Management		192.168.60.0 /24
N/A -Core-to-distribu		172.16.0.0 /29

Informations supplémentaires:

Zone	MAC	Int	Adresse IP	Passerelle par défaut
DMZ	B3	EM2	192.168.40.254/24	
WAN	9F	EM0	193.190.65.84	193.190.65.81
UZ(LAN)	A9	EM1	172.16.0.1 /29	

2.5 configuration version 1

Cfr Annexe A.

3 Mail

La configuration du serveur mail reste en standby tant que la mise en place des serveurs n'est pas terminée. Pour gagner du temps durant la phase d'implémentation, nous avons développé les procédures à suivre afin d'installer un serveur Microsoft Exchange.

Les clients mail pris en charge par Microsoft Exchange sont les suivants :

— Outlook 2016

— Outlook 2013

— Outlook 2010 SP2

— Outlook pour Mac pour Office 365

— Outlook pour Mac 2011

La marche à suivre peut être consultée sur Github : `https://github.com/EPHEC-OKLN/Mail`

4 Sécurité

4.1 Tâches réalisées

- Installation de pfSense
  - Création de la machine virtuelle
  - Configuration des interfaces
  -

Zone	Interface	Suffix Mac	Adress IP
WAN	EM0	9f	193.190.65.84
UZ	EM1	a9	172.16.0.1
DMZ	EM2	b3	192.168.40.254

- configuration de pfSense
  - Mise en place des zones
  - mise en place de la NAT
- Règles du pare-feu
- **WAN**
  1. Refuser tout le trafic entrant sauf exceptions.
  2. Autoriser le trafic http(s) (tcp :80, tcp :443) vers le reverse proxy.
  3. Autoriser le trafic ftp (tcp :20, tcp :21) vers les serveurs web.
  4. Autoriser le trafic dns (tcp :53, udp/- :53) vers le SOA.
- **DMZ**
  1. Autoriser le trafic vers internet.
  2. Interdire le trafic vers la UZ (sauf exceptions).
  3. Autoriser le trafic LDAP (tcp :389) vers l'AD.
- **UZ**
  1. Autoriser le trafic vers internet
  2. Autoriser le trafic vers la DMZ

4.2 Problèmes rencontrés

- **Infra**
  Certaines NICs (Network Interfaces) n'appartenaient pas au bon réseau, nous avons du prendre le temps de recâbler et de reconfigurer calmement les switchs physiques et virtuels.
- **Interface Web**
  L'interface web était inaccessible malgré le fait que SSH fonctionnait. Une option avait été mal configurée `revert http to webConfigurator{}`, en lisant la documentation sur internet, nous avons pu corriger notre erreur et accéder à l'interface.

4.3 Remarques

Il a été important de travailler avec les gens de l'équipe "infra" pour s'assurer que chaque NIC était connectée au bon réseau.

5 Logistique

5.1 Tâches réalisées

Nous avons réalisé l'inventaire du matériel à notre arrivée dans la classe ce matin afin de vérifier qu'il ne manquait rien. Par la suite, nous avons dû nous munir d'un switch layer 3 en plus du matériel que l'on avait déjà. nous avons organisé un repas de midi en commun des deux groupes et en présence de nos professeurs. Les responsables logistique de chaque groupe ont travaillé main dans la main pour gérer la commande, le paiement et la livraison des pizzas !

5.2 Difficultés rencontrées

Les pizzas étaient en retard à cause du Pizza Hut de Wavre qui n'a pas été très compétent et donc, par conséquent, nous avons pris du retard sur notre journée.

5.3 Remarques importantes

Nous nous sommes rendus compte que gérer la commande de nourriture d'une grosse équipe peut sembler facile, anodin et inutile mais au final, cela demande quand même une organisation assez conséquente. De plus, le fait de manger tous ensemble sur le temps de midi rapproche l'équipe et permet une meilleure ambiance de travail.

6 Services internet

6.1 Tâches réalisées

Nous avons avancés sur le site internet, nous avons mis en place un agenda adaptable par les employés via le service google. La page d'inscription ainsi que la page des formations est presque terminée.

Nous avons également pu obtenir un nom de domaine pour le site web ainsi que les informations utiles pour la configuration du serveur DNS.

6.2 Difficultés rencontrées

Nous rencontrons des problèmes de CSS pour la page des formations. Nous sommes toujours dans l'attente du serveur pour le déploiement du serveur web.

6.3 Technologies utilisées

Nous avons choisi d'utiliser le calendrier google car il est facile d'utilisation et d'également de l'implémenter sur le site web. D'autre part, nous pouvons le gérer en le partageant via des adresses mails.

6.4 Remarques facultatives

Il faut bien centrer les formations sur le site web et également ajouter du PHP pour pouvoir finaliser l'inscription.

7 Déploiement

7.1 Tâches réalisées

Nous avons commencé par configurer le petit serveur. Sur celui-ci, nous avons installé les vSwitch suivant :

— WAN

— DMZ

— web-db

Nous avons ensuite configuré les ports group suivant :

— uz-group

— management Network

— wan-group

— dmz-group

— web-db

L'étape suivante a été l'installation d'une machine virtuelle pfsense pour la configuration et la gestion du pare-feu. Nous avons finalement déployé une machine Debian afin de la cloner pour les différents services nécessaires.

Au final 4 clonages auront été effectués pour répondre à nos besoins.

7.2 Difficultés rencontrées

Nous avons eu des problèmes avec le mapping du clavier sur Debian à cause de l'hyperviseur ESXI.

La solution a été de déployer une machine Debian configurée depuis WorkStation.

8 Collaboration

Le rôle de collaborateur consiste à être l'intermédiaire, la liaison, entre les deux groupes, si on a une question ou un doute sur un sujet, le responsable de la collaboration va voir l'équipe correspondant dans l'autre groupe et lui pose

la question. Ce rôle consiste donc à maintenir le lien entre les deux groupes. Le responsable passe régulièrement dans les différentes sections pour savoir s'ils ont besoin d'un renseignement sur un sujet précis.

Le chargé de collaboration a commencé son travail en s'assurant que les groupes allaient dans la même direction au niveau des chartes.

Par la suite, l'équipe d'infrastructure réseau ayant eu des soucis avec l'image cisco et compromettant ainsi la sécurité du réseau, les parties infrastructures réseau et les parties sécurité réseau des deux équipes ont donc beaucoup collaboré pour essayer de trouvez des solutions.

9 Rapports & organisation

9.1 Tâches réalisées

Nous avons pu finir de rassembler tous les "sous-rapports" afin de finaliser le rapport du jour 1. Nous avons pu entamer le rapport du jour 2 au fur et à mesure que la journée se déroulait et que de nouvelles choses étaient apportées par les sous-groupes.

9.2 Difficultés rencontrées

Il était nécessaire de rappeler régulièrement aux gens dans les équipes de noter ce qu'ils faisaient au fur et à mesure de la journée afin d'avoir le plus de traces possibles de ce qui c'étaient passés, cependant malgré nos rappels insistants ce n'étaient pas toujours fait et les équipes devaient faire l'exercice de se rappeler du plus de chose possibles en fin de journée.

Une autre difficulté qui s'est présentée est le fond pas toujours claire/complètes des notes remises par les différents sous-groupes. Nécessitant alors de notre part un aller-retour régulier vers chacun des groupes pour clarifier les choses.

9.3 Remarques importantes

10 sources

10.1 sécurité

— `https://doc.pfsense.org`

10.2 Déploiement

— `https://kb.vmware.com/s/article/1027876`

10.3 rapports

— `https://fr.sharelatex.com/learn/Tables#Colouring_a_table_.28cells.2C_rows.2C_columns_and_lines.29`

10.4 Services internet

—

A config version1

```
hostname S1-CSW-01
!
enable
conf t
enable secret class
service password-encryption
! ------------------------------------------------------------------------------
!------------------------creation des vlan-------------------------------------------------------------------
vlan 10 name service
vlan 30 name guest
vlan 50 name user
vlan 60 name management
!-------------------------------------------------------------------------------
! - 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 !"
line console 0
  login local
  logging synchronous
line vty 0 4
  login local
!
!

!
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
!
```

```
! - Configuration des interfaces
!
interface f0/1
  description "vers core-to-distrubu(f0/1)"
  no switchport
  ip address 172.16.0.2 255.255.255.248
  no shut
!
interface f0/2
  description "Vers swuith1 (f0/1)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f0/3
  description "Vers swuith2(f0/1)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f0/4
  description "Vers layers3(2)(f0/1)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f0/5
  description "Vers layers3(2)(f0/2)"
  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 primary
spanning-tree vlan 50 root primary
spanning-tree vlan 60 root primary
!
!
-----
-----
HSRP
----
----
interface f0/1
standby 100 ip 172.16.0.1
standby 100 preempt
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
hostname S2-CSW-02
!
!
!
enable
conf t
enable secret class
service password-encryption

! ------------------------------------------------------------------------
!------------------------creation des vlan-----------------------------------------------------------------
vlan 10 name service
vlan 30 name guest
vlan 50 name user
vlan 60 name management
!-------------------------------------------------------------------------------
! - configuration de base
!
ip domain-name formation.lab
crypto key generate rsa
2048
!
no ip domain-lookup
banner login "Access for authorized users only !"
line console 0
  login local
  logging synchronous
line vty 0 4
  login local
!
!

!
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
!
! - Configuration des interfaces
!
interface f0/1
  description "vers core-to-distrubu(f0/1)"
  no switchport
  ip address 172.16.0.3 255.255.255.248
  no shut
!
interface f0/2
  description "Vers layers3(1)(f0/5)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f0/3
  description "Vers layers3(1)(f0/4)"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f0/4
  description "Vers vlan managment"
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk native vlan 60
!
interface f0/5
  description "Vers vlan managment"
  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 primary
spanning-tree vlan 30 root primary
spanning-tree vlan 50 root primary
spanning-tree vlan 60 root primary
!
-----
-----
HSRP
----
----
interface f0/1
standby 110 ip 172.16.0.1
standby 110 preempt
--------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------
hostname SW02
! ------------------------------------------------------------------------
!
!
enable
conf t
enable secret class
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
line console 0
  login local
  logging synchronous
line vty 0 15
  login local
  transport input ssh
!
! - Création des VLANs
!
vlan 10
  name service
!
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 client
vtp domain okln.ephec-ti.be
!
! - Configuration des interfaces
!
interface range F0/1 - 2
  description "Vers layers3(1)"
  switchport mode trunk
  switchport trunk native vlan 60
!
!
interface range F0/3 - 5
  description "vlan user"
  switchport mode access
  switchport access vlan 50
   no shutdown
!
interface range F0/6 - 24
  description "non utilise"
  switchport mode access
  switchport access vlan 50
  shutdown
!

-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------------
hostname SW03
! ------------------------------------------------------------------------
!
!
!
enable
conf t
enable secret class
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
line console 0
  login local
  logging synchronous
line vty 0 15
  login local
  transport input ssh
!
! - Création des VLANs
!
vlan 10
  name service
!
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 client
vtp domain okln.ephec-ti.be
!
! - Configuration des interfaces
!
interface range F0/1 - 2
  description "Vers layers3(1)"
  switchport mode trunk
  switchport trunk native vlan 60
!
!
interface range F0/3 - 5
  description "vlan user"
  switchport mode access
  switchport access vlan 50
   no shutdown
!
interface range F0/6 - 24
  description "non utilise"
  switchport mode access
  switchport access vlan 50
  shutdown
!
© 2018 GitHub, Inc.
Terms
Privacy
Security
Status
Help
Contact GitHub
API
Training
Shop
Blog
About
```