

Ynov Informatique B3  
2020/2021



# Documentation d'architecture

2ème PROJET : Architecture réseau et sécurité

## **Présenté par:**

Arthur KOZIOR  
Hedi BEN MOHAND  
Omar KALLEL

- **Contexte du projet:**

Nous avons été contacté par une entreprise d'E-commerce dans le but de revoir leur infrastructure réseau. Dans le cadre de cette exercice, nous proposons une infrastructure composée d'un firewall sécurisant le trafic au sein du réseau, une DMZ qui permettra de conserver les données sensibles hors d'atteinte dans l'éventualité d'une faille de sécurité du réseau composé de VLAN pour les post mis a disposition des clients.



Dans une société d'E-commerce il est essentiel de fournir un réseau sécurisé, ainsi qu'une sécurité importante dûe au flux important de passage dans ces lieux. Il est primordial pour le bon déroulement du travail d'une société d'E-commerce de mettre en place une infrastructure qui puisse pallier à différents soucis et permettre une continuité d'activité.

## **Gestion de projet :**



### **Répartition des tâche :**

HEDI : VM, DOCS

ARTHUR : CISCO PACKET TRACER, DOCS

OMAR : DOCS

### **Moyen de communication :**

	<ul style="list-style-type: none"><li>- Appels</li><li>- Partage d'écran</li><li>- Partage d'informations</li><li>- Répartition des tâches</li></ul>
	<ul style="list-style-type: none"><li>- Partage de travaux</li><li>- Edition de documents</li><li>- Plan d'adressage</li></ul>

- **Travail demandé:**

Mise en place d'une architecture réseau avec des fonctionnalités avancées et de haute disponibilité de préférence Open Source avec une redondance des équipements et élimination des SPOF, en intégrant des fonctionnalités comme:

- Un firewall,
- Un portail captif,
- Une DMZ,
- Un Honeypot,
- Un VLAN,
- Une redondance réseau
- Une sauvegarde de la configuration réseau,
- Un SOC
- Une Détection d'intrusion.

En répondant à des exigences comme:

Le réseau est-il sécurisé ou non sécurisé?

Est ce qu'il est connecté à internet ou isolé?

Où sont les PC clients?

Où sont les serveurs?

Qu'en est t'il de la robustesse du réseau?

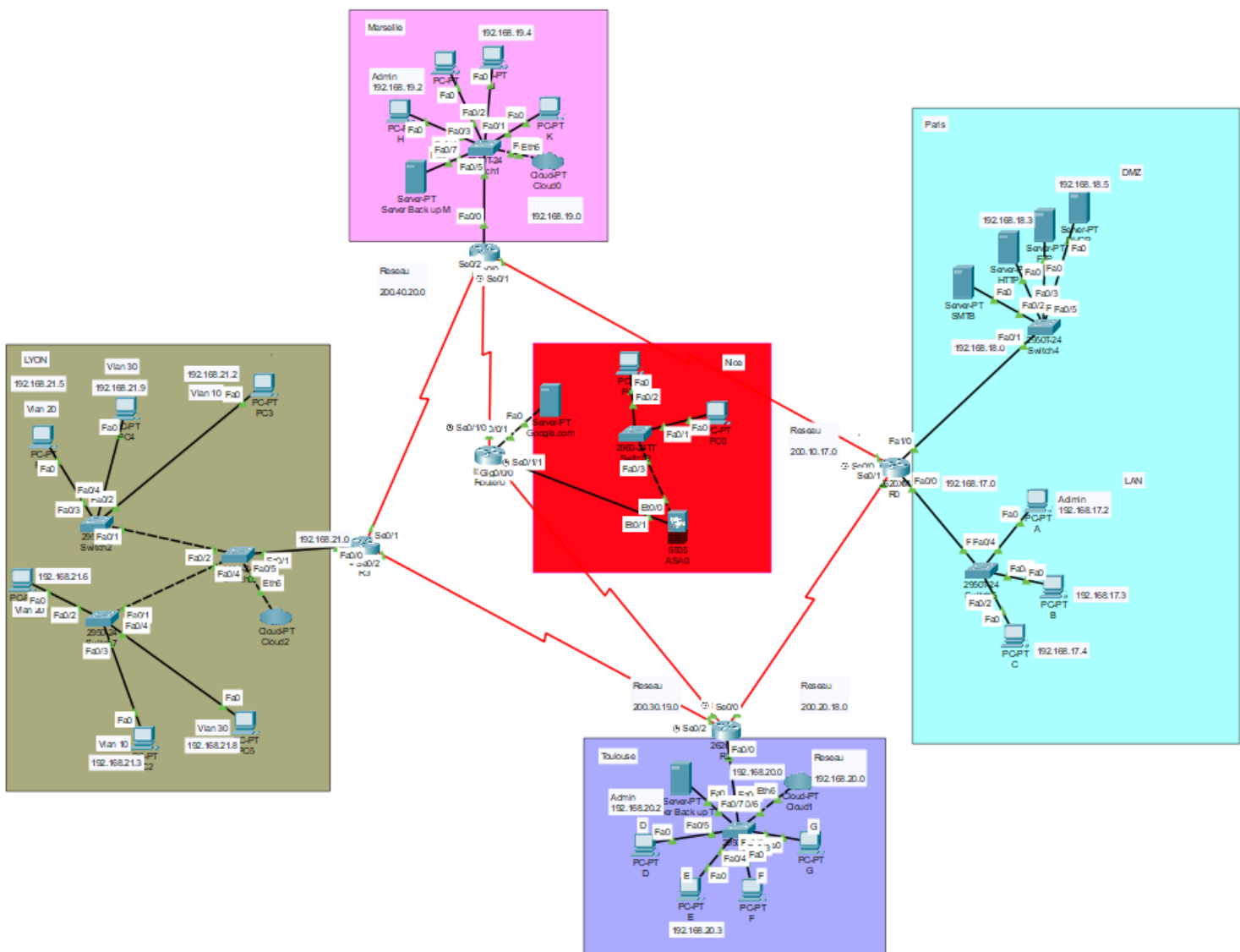
Avoir une structure qui permettra de se connecter avec les différents réseaux des différentes régions.

- **Solutions:**

Afin de répondre à la problématique demandée, nous avons donc imaginé l'architecture réseau en utilisant l'outil de Cisco Packet Tracer.

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc . . .

Nous avons donc opté pour cette architecture implémente des fonctionnalités variée comme: le firewall, un portail captif, une DMZ, un VLAN, des zones de réseau protéger des intrusions venant de l'extérieur, une zone de réseau qui communique avec l'extérieur à travers internet.



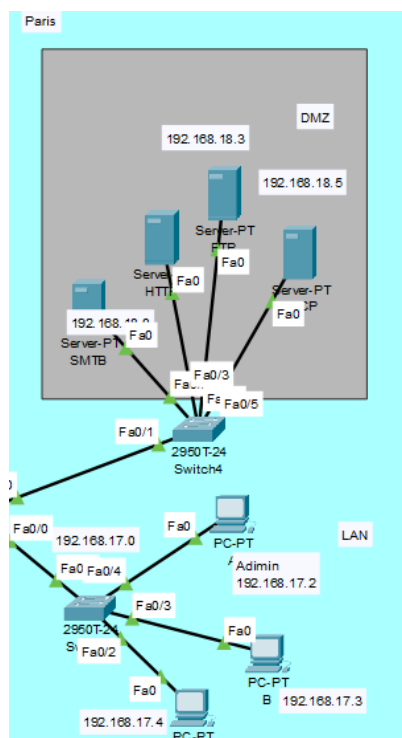
## Plan d'adressage:

Réseau	IP	Type	Nom d'hôte
192.168.18.0	2	Serveur	SMTB
192.168.18.0	3	Serveur	HTTP
192.168.18.0	4	Serveur	FTP
192.168.18.0	5	Serveur	DHCP
192.168.19.0	21	Serveur	Back Up M
192.168.20.0	21	Serveur	Back Up T
8,8,8,0	0	Serveur	Google.com
192.168.17	2	PC	Admin
192.168.17	3	PC	PC-02
192.168.17	4	PC	PC-03
192.168.19	2	PC	Admin
192.168.19	3	PC	PC-02
192.168.19	4	PC	PC-03
192.168.19	5	PC	PC-04
192.168.20	2	PC	Admin
192.168.20	3	PC	PC-02
192.168.20	4	PC	PC-03
192.168.20	5	PC	PC-04
172.16.1,	5 -> 10	DHCP	
192.168.18	2 -> 10	DHCP	
172.16.1,	1	Pare-feu	ASA0
192.168.	21.1	VLAN-10	
192.168.	21.65	VLAN-20	
192.168.	21.129	VLAN-30	
192.168.	21.1	VLAN-10	
192.168.	21.65	VLAN-20	
192.168.	21.129	VLAN-30	

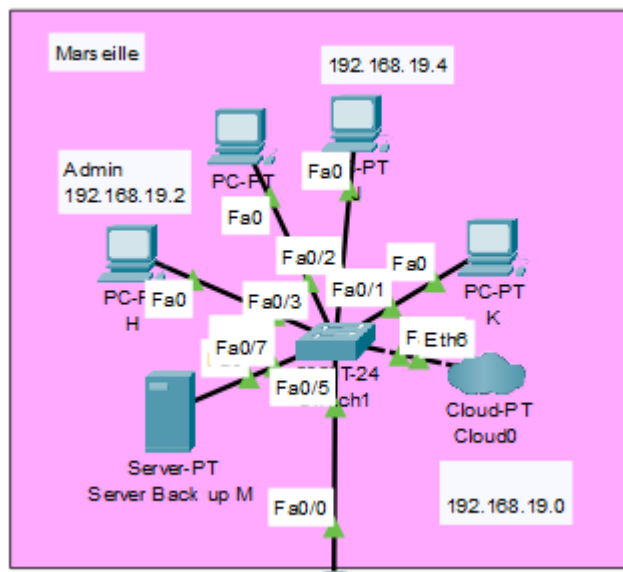
## Description du schéma de réseau:

- La zone bleue ciel - Paris:

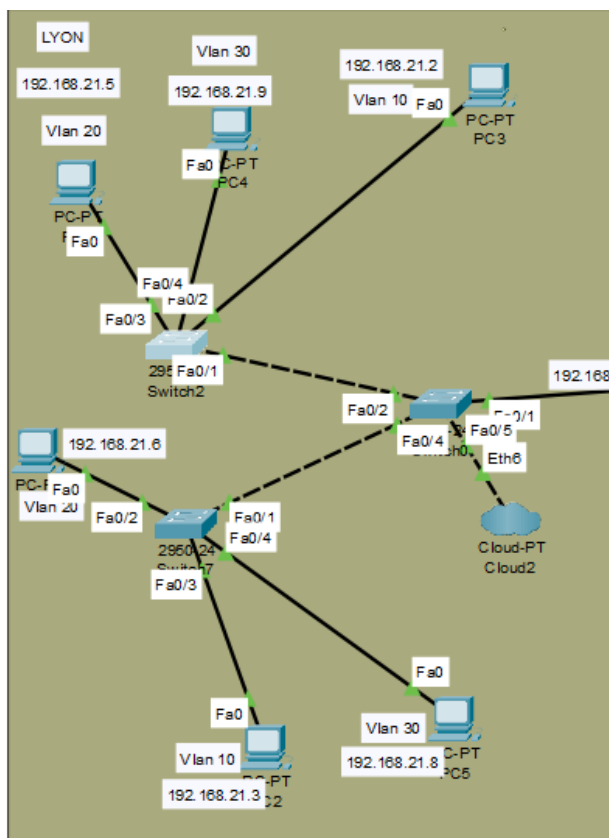
Cette zone abrite la DMZ et aussi un réseau Lan



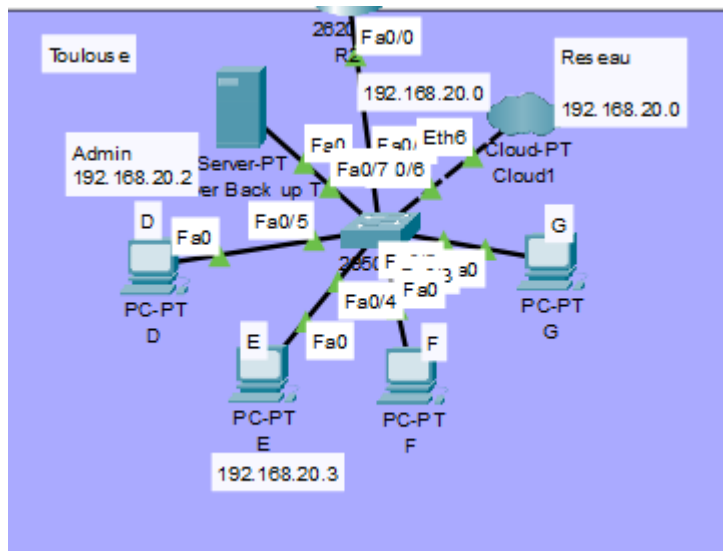
- La zone rose - Marseille:  
Cette zone abrite des utilisateurs(clients), un serveur backup.



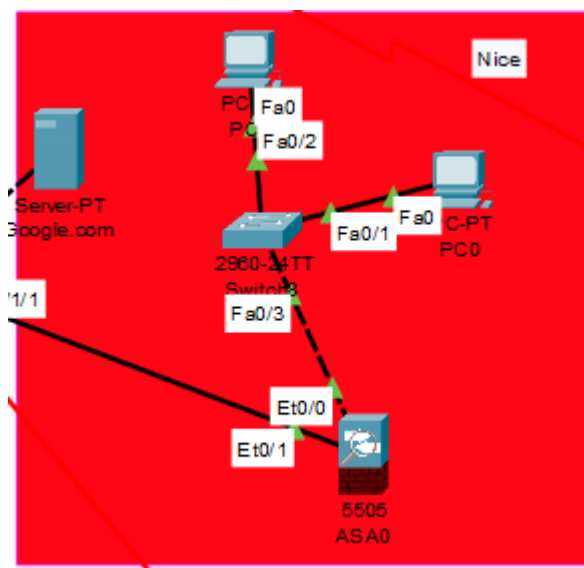
- La zone kaki - Lyon:  
Cette zone abrite différents Vlan, les utilisateurs(clients).



- la zone violette - Toulouse:  
Cette zone abrite les utilisateurs(clients), un serveur backup



- la zone rouge - Nice:  
Cette zone abrite des utilisateur, un pare feu, ainsi qu'un serveur pour se connecter à internet

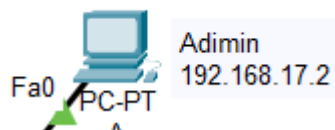




## DMZ:

Nous avons configuré une dmz accessible seulement par les administrateurs. Celui-ci sera le seul dans le réseau à pouvoir communiquer avec elle et les autres membres du réseau ne pourront pas la voir.

### Admin Accès DMZ



Les pc admin de l'entreprise on tout le fin sur leur ip : 192.168.???.2 de leurs adresses IP et seront les seul a pouvoir interagir avec la DMZ

### ACL Access list DMZ

```
R0>
R0>enable
R0#show acces
R0#show access-lists
Standard IP access list 1
 10 permit host 192.168.17.2
 20 permit host 192.168.19.2
 30 permit host 192.168.20.2
 40 deny any
.
```

Pour configurer notre dmz nous avons interdit toutes communications entrantes sauf celles venant des pc administrateurs. Grâce à cette configuration nous réduisons grandement le risque d'intrusion sur nos serveurs ainsi que la localisation de ceci dans le réseau.

## IP Route

Pour les IP Routes on a dû définir les adresses ip et les masques à emprunter pour pouvoir organiser les communications des différents réseaux par les routeurs.

```
O 192.168.17.0/24 [110/65] via 200.20.18.1, 01:07:58,
Serial0/1
O 192.168.18.0/24 [110/65] via 200.20.18.1, 01:07:58,
Serial0/1
O IA 192.168.19.0/24 [110/129] via 200.20.18.1, 01:07:58,
Serial0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/0
R 192.168.21.0/24 [120/1] via 200.30.19.1, 00:00:10, Serial0/2
O 200.10.17.0/24 [110/128] via 200.20.18.1, 01:07:58,
Serial0/1
C 200.20.18.0/24 is directly connected, Serial0/1
C 200.30.19.0/24 is directly connected, Serial0/2
O 200.40.20.0/24 [110/128] via 200.30.19.1, 01:08:03,
Serial0/2
```

Cela permet notamment au pc de différents réseaux de pouvoir communiquer entre eux.

## VLAN

Les pc des utilisateurs communiquent entre eux dans le même VLAN nous avons notamment segmenté les différents pôles de l'entreprise(It,Compta...) pour éviter les conflits.

Fa0/23, Fa0/24			Fa0/21, Fa0/22,
10	RH	active	Fa0/2
20	PR	active	Fa0/3
30	ES	active	Fa0/4

Un membre du VLAN 10 ne pourra pas communiquer avec un membre du VLAN 20

## Telnet admin

Cette configuration nous permet de donner aux administrateurs les droits de se connecter et configurer les routeurs, là où les users ne pourront que les utiliser pour transmettre leurs données.

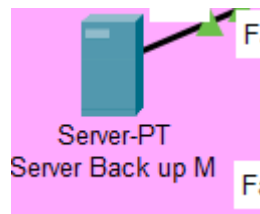
```
C:\>telnet 192.168.17.1
Trying 192.168.17.1 ...Open

User Access Verification

Password:
R0>|
```

## Server backup

Pour maximiser la sécurité de nos données et dans une idée de continuité de service nous avons incorporé deux serveurs de back up.



Ces serveurs ont pour but de pouvoir revenir à une version antérieure en cas de problème et minimiser les pertes en cas d'incident sur les serveurs de productions, grâce au TFTP.

## DHCP

Tous nos serveurs ont un DHCP.

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0060.5C14.4EE9
IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	192.168.18.2
Subnet Mask	255.255.255.0

Cela nous permet d'assurer la configuration des paramètres ip des machines, notamment en leurs attribuant automatiquement des paramètres IP et un masque de sous-réseau.

## Configuration internet

Nous avons fait en sorte d'éviter les téléchargements depuis internet, les utilisateurs ne peuvent pas télécharger de fichier, mais peuvent consulter des sites web.

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int gi
Router(config)#int gigabitEthernet 0/0/0
Router(config-if)#ip add
Router(config-if)#ip address 203.1.1.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

Router(config-if)#int gi
Router(config-if)#int gig
Router(config-if)#int gigga
Router(config-if)#int giga
Router(config-if)#int gi
Router(config-if)#exit
Router(config)#int gi
Router(config)#int gigabitEthernet 0/0/1
Router(config-if)#ip add
Router(config-if)#ip address 8.8.8.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

Router(config-if)#exit
Router(config)#router os
Router(config)#router ospf 1
Router(config-router)#netw
Router(config-router)#network 231.1.1.0 0.0.0.255 ar
Router(config-router)#network 231.1.1.0 0.0.0.255 area 0
Router(config-router)#netw
Router(config-router)#network 8.8.8.0 0.0.0.255 are
Router(config-router)#network 8.8.8.0 0.0.0.255 area 0
Router(config-router)#

```

## Router vers le Serveur google et le Firewall

La mise en place d'un firewall permet de gérer les trafics et restreindre les accès.

```

ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic LAN interface
   translate_hits = 6, untranslate_hits = 4

ciscoasa#show dhcpd binding all
IP address      Client Identifier      Lease expiration
Type
172.16.1.6      000B.BE12.B998         --
Automatic
172.16.1.5      0090.0C32.3AC0         --
Automatic
.              .

ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-
max 4096) alert-interval 300
access-list aled; 2 elements; name hash: 0x3c1cdb9e
access-list aled line 1 extended permit tcp any any(hitcnt=0)
0xcaa697ba
access-list aled line 2 extended permit icmp any any(hitcnt=4)
0x5d5e0cb9

```

Cette pratique permet de donner une première sécurité à notre réseau

**Matériel utiliser :**

PC ThinkCentre M900:

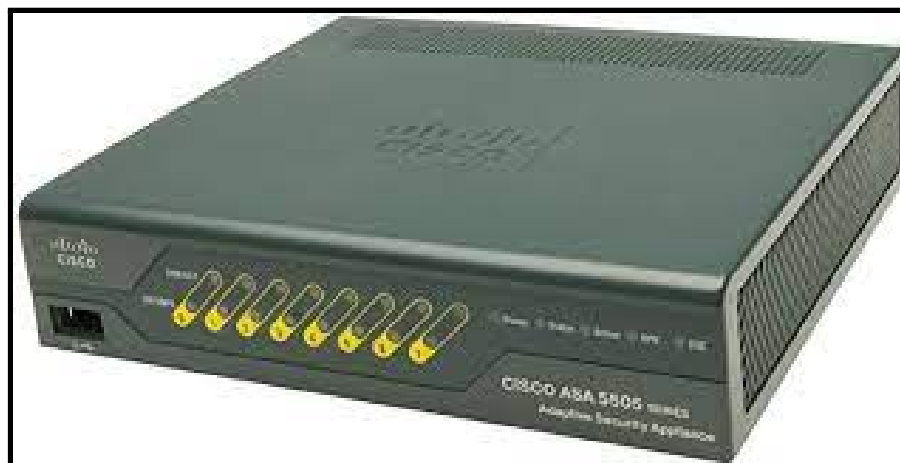
#### Fiche technique sur Lenovo ThinkCentre M900 Tiny Core i5 2,5 GHz - SSD 256 Go RAM 8 Go

- Couleur : Noir
- Capacité de stockage : 256 Go
- Type de stockage : SSD
- Mémoire : 8 Go
- Modèle : ThinkCentre M900 Tiny
- Vitesse du processeur : 2,5 GHz
- Marque du processeur : Intel
- Type du processeur : Core i5
- Nom de la Carte Graphique : Intel HD Graphics 530
- Système d'exploitation : Windows 10
- Réseau : Wifi
- Bluetooth : Non
- Date de sortie : Juin 2014
- Année de sortie : 2015
- Capacité de stockage SSD (Go) : 256
- Processeur : Core i5-6500T
- WiFi : Oui
- Marque : Lenovo
- Poids : 1300 g



Firewall 5505:

Informations générales	
Nom	Cisco ASA 5505 150Mbit/s
Type produit	Pare-feux (matériel)
Marque	Cisco
Transmission des données	
Débit du pare-feu	150 Mbit/s
Débit du VPN	100 Mbit/s
Mobile VPN IPSec	10
Connexions de pare-feu maximum par seconde	4000
Réseau	
Nombre d'utilisateurs	10 utilisateur(s)
Nombre de VLANs	3
Wifi	Non
Connectivité	
Connectivité	Avec fil
Nombre de port ethernet LAN (RJ-45)	8
Nombre de ports série	1
Quantité de Ports USB 2.0	3
Fast Ethernet (cuivre) Nombre de ports	8
Sécurité	
Algorithme de sécurité soutenu	3DES, AES



Switch 2960:



Informations générales	
Nom	Cisco Catalyst 2960-Plus
Type produit	Commutateurs réseaux
Marque	Cisco
Caractéristiques de gestion	
Support MIB	Oui
Banc de commutateurs	L2
Qualité de service (QoS)	Oui
Support à la multidiffusion	Oui
Gestion basée sur le web	Oui
Type de commutateur	Géré
Connectivité	
Port de console	RJ-45
Quantité de ports Ethernet RJ-45 de commutation de base	24
Type de port Ethernet RJ-45 de commutation de base	Fast Ethernet (10/100)
Quantité de ports Combo SFP	2
Réseau	
Full duplex	Oui
Assistance contrôle des flux	Oui
Agrégation de lien	Oui
Limitation du débit	Oui
Standards réseau	IEEE 802.1p, IEEE 802.1x
Support VLAN	Oui
Transmission des données	
Support de trames étendues (Jumbo Frames)	Oui
Nombre de VLANs	255
Débit	6,5 Mpps
Sécurité	
Algorithme de sécurité soutenu	802.1x RADIUS
Filtrage d'adresse MAC	Oui



Server HPE ProLiant DL20 :

## GÉNÉRAL

Type	Serveur
Facteur de forme	Montable sur rack - 1U
Evolutivité des Serveurs	1 voie
Nombre de baies pour unités échangeables à chaud	4

## PROCESSEUR / CHIPSET

CPU	Intel Xeon E-2236 / 3.4 GHz
Vitesse maximale en mode Turbo	4.8 GHz
Nombre de coeurs	6 cœurs
Nombre d'unités centrales	1
Nombre maximum d'unités centrales	1
Évolutivité de l'unité centrale	Évolutif
Caractéristiques principales du processeur	Technologie Hyper-Threading, technologie Intel Turbo Boost 2, Intel Smart Cache
Connecteur d'unité centrale	Socket LGA1151

## MÉMOIRE CACHE

Taille installée	L3 - 12 Mo
Cache par processeur	12 Mo

## RAM

Taille installée	16 Go / 64 Go (maximum)
Technologie	DDR4 SDRAM - ECC
Vitesse de mémoire effective	2666 MHz
Vitesse nominale de la mémoire	2666 MHz



Router 4331:

Informations générales	
Nom	Cisco ISR 4331 Routeur connecté Ethernet/LAN Noir
Type produit	Routeurs connectés
Marque	Cisco
Caractéristiques Ethernet LAN	
Technologie de câblage	10/100/1000Base-T(X)
Full duplex	Non
LAN Ethernet : taux de transfert des données	10,100,1000 Mbit/s
Ethernet/LAN	Oui
Connectivité	
Nombre de port ethernet LAN (RJ-45)	5
Port WAN	Ethernet (RJ-45)
Port RS-232	2
Nombre de ports USB	2
Version USB	2.0
Réseaux mobiles	
Données du réseau	Non pris en charge
Réseau	
Standards réseau	IEEE 802.1Q,IEEE 802.1ag,IEEE 802.3,IEEE 802.3ah
Protocoles	
Protocole de routage	BGP,EIGRP,IS-IS,OSPF
Caractéristiques de gestion	
Gestion basée sur le web	Oui
Bouton de réinitialisation	Oui
Qualité de service (QoS)	Oui
Sécurité	
Algorithme de sécurité soutenu	3DES,AES
Pare-feu de sécurité	Zone Based
Pare-feu	Oui

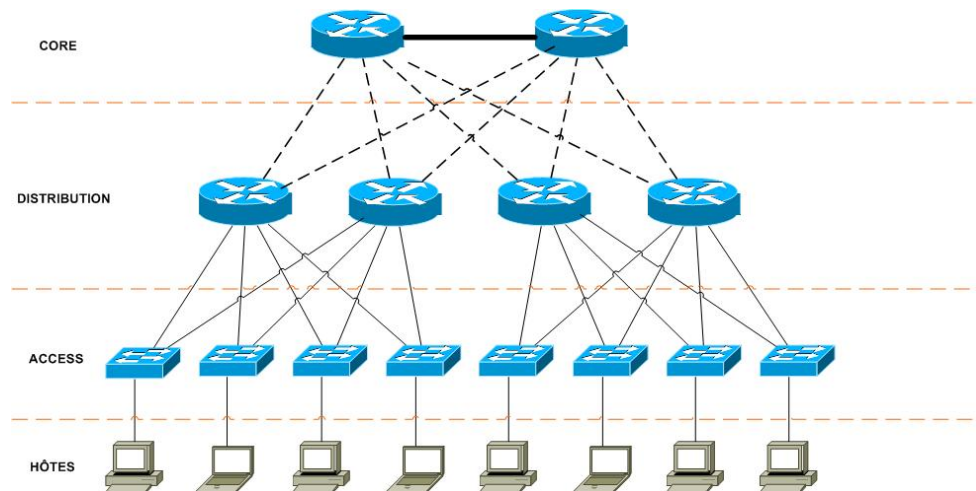


## Future evolution

En vue de notre prochain entretien, nous prévoyons de mettre en place des vm qui serviront de démonstration, pour des features demandées dans le cahier des charge. Il s'agirait d'un portail captif, d'un honeypot et une détection d'intrusion et la redondance réseaux.

### La redondance réseaux:

Aussi nommée redondance de liens, elle consiste à fournir plusieurs connexions Internet pour assurer une continuité de service. Si le premier lien tombe, les flux sont redirigés vers le second lien. La redondance d'accès permet d'assurer une plus grande disponibilité.



### Honeypot:

Le honeypot est une méthode de défense active qui consiste à attirer, sur des ressources, des attaquants afin de les identifier, voir les neutraliser.

### Détection d'intrusion:

Le système de détection d'intrusion aussi appelé IDS est un mécanisme qui permet de repérer des activités anormales ou suspectes sur la cible que l'on analyse. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

### Portail captif:

Le portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.

