

PROJET INFRA - CYBER



Projet réalisé par :
Aurélien Chatillon
Mohammad-Reza SHAKIBAEI

PARIS
ynov
CAMPUS

TABLE DES MATIÈRES

I- Contexte: -----	
a. Le projet infra-sécu-----	
b. Gestion du projet-----	
c. Mise en situation-----	
II- Nos solutions:-----	
a. L'architecture de notre infrastructure-----	
b. Composants et logiciels utilisés-----	
c. Commandes effectuées-----	
III- Evolution-----	

Contexte :

a. Le projet Infra-sécu

Lors de notre cursus en Bachelor 3 informatique à l'école Paris Ynov, il nous a été demandé de réaliser un projet commun entre étudiant en informatique spé infrastructure des SI et Cybersécurité. Nous avons le choix entre plusieurs projets qui sont les suivants :

- ☐ Architecture réseau et sécurité
- ☐ Plateforme de sauvegarde
- ☐ Infrastructure as code et conteneurisation
- ☐ Gestion d'un intranet

Nous avons choisi de réaliser le projet **Architecture réseau et sécurité**, ce projet a pour objectif de nous permettre d'appliquer diverses compétences acquises lors de notre formation mais aussi d'en acquérir de nouvelles. Les axes abordés sont la configuration et administration d'un réseau, la mise en place d'une architecture système et réseaux *from scratch* ainsi que la gestion de la sécurité d'un réseau.

Cette réalisation est évaluée sur l'ensemble de la production. L'évaluation prend en considération une présentation orale de 15 minutes, une démonstration du fonctionnement de notre infrastructure, et d'un rapport.

Les fonctionnalités recommandé et demandé pour le projet sont les suivants :

- ❖ Fonctionnalités possibles :
- ❖ Firewall
- ❖ Portail captif
- ❖ DMZ
- ❖ Honeypot
- ❖ VLAN
- ❖ Redondance réseau
- ❖ Sauvegarde de la configuration réseau
- ❖ SOC
- ❖ Détection d'intrusion

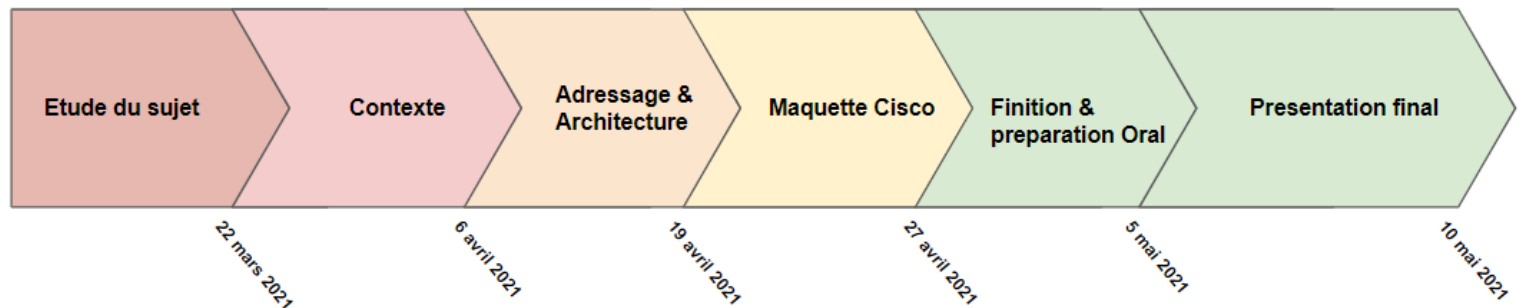
Les propositions concernant la mise en place l'infrastructure :

- ❖ Utiliser un logiciel préférence Open Source
- ❖ Etablir une redondance des équipements et élimination des SPOF
- ❖ Sécuriser le réseau
- ❖ Etablir une connexion internet/isolé
- ❖ Séparer les différents acteurs

Ce projet de fin de cursus a pour objectif de valider nos compétences mais aussi d'en acquérir de nouvelles.

b. Gestion du projet

Planning des tâches :




Répartition des tâches :



Afin de réaliser ce projet nous avons choisis de collaborés à deux sur chacune des tâches afin de pouvoir monter en compétence de manière équivalente. Mais avec des soucis de délai, il peut arriver d'intervertir des tâches.

Collaboration :

Communication :

Logiciel	Avantages
	<ul style="list-style-type: none">- Appels- Partage d'écran- Envoie de fichiers léger

Partage :

Logiciel	Avantages
	<ul style="list-style-type: none">- Partage de documents et fichiers lourds
	<ul style="list-style-type: none">- Utilisation d'un ordinateur à distance afin de pouvoir faire des manipulations

c. Mise en situation

Une entreprise de taille moyenne nommée J&M – Jean et Marc emménagent dans de nouveaux locaux et souhaitent déployer une nouvelle infrastructure. Pour cela il fait appel à notre agence de prestataire spécialisé en Infra-Réseau « Cynetis » afin de réaliser une architecture système et réseaux adapté et sécurisé pour leur société.

J&M est une entreprise avec différents pôles d'activité, il existe un service de gestion des ressources humaines, un service comptabilité mais aussi un service IT. La société dispose de nombreux sites web en ligne et des données sensibles, elle ne peut pas se permettre d'avoir des pannes réseaux ou encore des failles de sécurité car cela impliquerait une perte énorme.

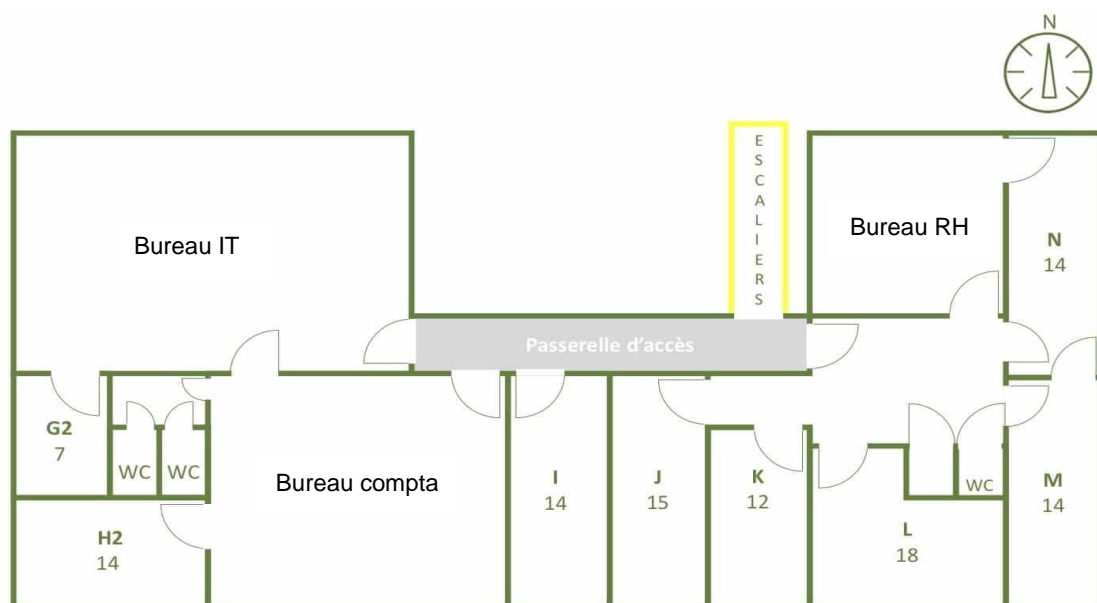
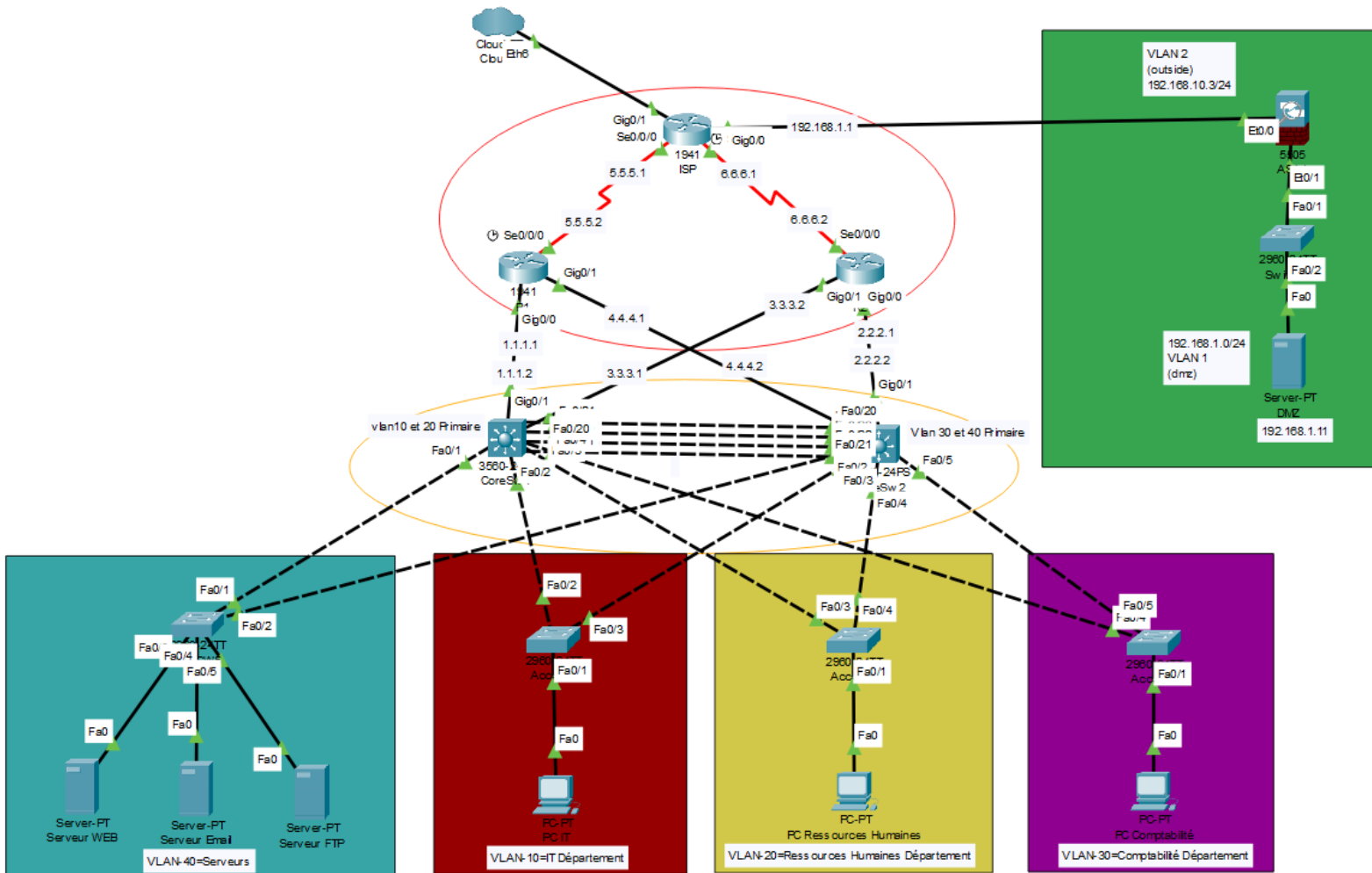


Figure : Plan des locaux de J&M

Plan d'action :

a. L'architecture de notre infrastructure



b. Plan d'adressage

Réseau	IP	Type	Nom d'hôte	Description générale
192.168.40.	40	Serveur	Serveur WEB	VLAN 40
192.168.40.	41	Serveur	Serveur Email	VLAN 40
192.168.40.	42	Serveur	Serveur FTP	VLAN 40
192.168.10.	10	PC	PC-IT	VLAN 10
192.168.20.	20	PC	PC Ressources Humaines	VLAN 20
192.168.30.	30	PC	Pc Comptabilité	VLAN 30

VLAN

Réseau	IP	Type	Nom d'hôte	Description générale
192.168.	10.0	VLAN-10	CoreSW1-CoreSW2	AccSW1
192.168.	20.0	VLAN-20	CoreSW1-CoreSW2	AccSW2
192.168.	30.0	VLAN-30	CoreSW1-CoreSW2	AccSW3
192.168.	40.0	VLAN-40	CoreSW1-CoreSW2	AccSW5

OSPF

Réseau	IP	Type	Nom d'hôte	Description générale
1.1.1.	1	Routage	R1	réseau 1.1.1.0
1.1.1.	2	Routage	CoreSW1	réseau 1.1.1.0
2.2.2.	1	Routage	R2	réseau 2.2.2.0
2.2.2.	2	Routage	CoreSW2	réseau 2.2.2.0
3.3.3.	1	Routage	CoreSW1	réseau 3.3.3.0
3.3.3.	2	Routage	R2	réseau 3.3.3.0
4.4.4.	1	Routage	R1	réseau 4.4.4.0
4.4.4.	2	Routage	CoreSW2	réseau 4.4.4.0
5.5.5.	1	Routage	ISP	réseau 5.5.5.0
5.5.5.	2	Routage	R1	réseau 5.5.5.0
6.6.6.	1	Routage	ISP	réseau 6.6.6.0
6.6.6.	2	Routage	R2	réseau 6.6.6.0

DMZ

Réseau	IP	Type	Nom d'hôte	Description générale
192.168.1.	1	Routage	ISP	réseau 192.168.1.0

Adressage pour DMZ :

DMZ

Réseau	IP	Type	Nom d'hôte	Description générale
192.168.10.	3	VLAN-2	ASA1	FireWall vlan outside
192.168.1	20.0	VLAN-1	ASA1	FireWall vlan DMZ
192.168.1.	11	Serveur	DMZ	Serveur DMZ

c. Logiciel utilisée : Cisco Packet Tracer

Cisco Packet Tracer est un logiciel développé par Cisco pour faire des plans d'infrastructure de réseaux locaux en temps réel et voir toutes les possibilités d'un réseau et sa future mise en œuvre. Le logiciel est gratuit, facile à installer et à exploiter, les possibilités de configuration et mise en place de réseaux assez conséquentes. Mais le logiciel n'est pas open source et est donc limité à l'appareil cisco.

d. Les composants de notre infrastructure

Ordinateur – ThinkCentre M720s :

ThinkCentre M720s

Référence : 10ST007BFR

Processeur ⓘ

Processeur Intel® Core™ i5-9400 9e génération (2,9 GHz, 6 cœurs, 9 Mo de cache, 65W, DDR4-2666)

Système d'exploitation ⓘ

Windows 10 Professionnel 64 bits

Mémoire totale ⓘ

8 Go UDIMM DDR4 2666MHz

Disque dur ⓘ

1 To HDD 7200rpm

Unité optique ⓘ

DVD±RW

Garantie

Garantie 3 ans sur site

Adaptateur secteur

180W

Carte graphique ⓘ

Carte graphique intégrée

Carte réseau ⓘ

Intégré 100/1000M

Format ⓘ

SFF - Small Form Factor 85% Power 180W

M.2 Storage Card

Aucun

WiFi Wireless LAN Adapters

Aucun



Serveur – SYS-E300-9D-4CNBTP

Model

Brand	SUPERMICRO
Model	SYS-E300-9D-4CN8TP

CPU Supported

CPU Type	Intel Xeon processor D-2123IT, CPU TDP support 60W
----------	--

Memory Supported

Max Memory Supported	Up to 512GB DDR4 ECC LRDIMM Up to 256GB DDR4 ECC / non-ECC RDIMM
Memory Type Supported	2666 / 2400 / 2133 MHz ECC DDR4 ECC LRDIMM and ECC / Non-ECC RDIMM Operating speed up to 2400 MHz

Storage Supported

Serial ATA	SoC controller for 4 SATA3 (6 Gbps) ports, (or 2 NVMe U.2 / 8 SATA3 through two Port Eight Intel PCH SATA 3.0 Ports or Two MINI-SAS HD ports)
------------	---

Graphics

GPU/VPU	Aspeed AST2500 BMC
---------	--------------------

Expansion Slots

PCI Express	1 x PCI-E 3.0 x8 slot
-------------	-----------------------

Communications

Number of LAN	Quad 1 GbE with Intel I350-AM4 Dual 10GBase-T with Intel X557 Dual 10G SFP+ via SoC
---------------	---

Panel Ports

Rear USB	2 x USB 3.0 ports
RJ45	2 x 10G SFP+ ports 2 x 10GBase-T LAN ports 4 x 1GbE LAN ports 1 x Dedicated IPMI LAN port



Le serveur est un dispositif qui permet à un ou plusieurs clients divers services. Tel l'accès aux World Wide Web, le courrier électronique, le partage de périphériques, le stockage en base de données

Router1941 – Cisco 1941 AX Bundle

Cisco 1941 AX Bundle w/ APP,SEC lic

Connectivity Technology:	Wired
Data Link Protocol:	Ethernet, Fast Ethernet, Gigabit Ethernet
Device Type:	Router
Remote Management Protocol:	SNMP, RMON
Encryption Algorithm:	SSL
Status Indicators:	Stromversorgung, Link/Aktivität
Construction:	original
Flash Memory:	256 MB (installiert) / 8 GB (Max)
RAM:	2 GB (installiert) / 2 GB (Max)
Network / Transport Protocol:	IPSec, PPPoE, L2TPv3
Enclosure Type:	Desktop, an Rack montierbar - modular - 2U
Compliant Standards:	IEEE 802.3, IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag, ANSI T1.101, ITU-T G.823, ITU-T G.824, CISPR 22 Klasse A, CISPR 24, EN55024, EN55022 Klasse A, EN50082-1, AS/NZS 60950-1, ICES-003 Klasse A, CS-03, R&TTE, FCC CFR47 Part 15,
Features:	Firewall, VPN-Support, MPLS-Unterstützung, Syslog-Unterstützung, Inhaltsfilterung, IPv6-Unterstützung, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Dynamic Multipoint VPN (DMVPN), Web Services Management Agent (WSMA),
Routing Protocol:	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, statisches IPv4-Routing, statisches IPv6-Routing, Policy-Based Routing (PBR), MPLS, Bidirectional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast
Interfaces:	2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 Verwaltung: 1 x Konsole - RJ-45 Verwaltung: 1 x Konsole - Mini-USB, Typ B Seriell: 1 x Zusatz - RJ-45 USB: 2 x 4-polig USB Typ A
Expansion Slots:	2 (gesamt)/ 2 (frei) x EHWIC 2 (gesamt)/ 1 (frei) x CompactFlash 1 (gesamt)/ 1 (frei) x ISM



Le routeur est un équipement réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles.

SwitchCore 3560 – Cisco 3560CX-12PC-S

GÉNÉRAL

Type de périphérique	Commutateur - 12 ports - Géré
Type de boîtier	De bureau, Montable sur rack, Montage sur rail DIN, fixation murale 1U
Sous-type	Gigabit Ethernet
Ports	12 x 10/100/1000 (PoE+) + 2 x SFP Gigabit combiné
Power over Ethernet (PoE)	PoE+
Budget PoE	240 W
Performances	Performances
Capacité	Interfaces virtuelles (VLAN): 1023
Support de cadre Jumbo	9018 octets
Protocole de routage	RIP-1, RIP-2, routage IP statique
Protocole de gestion à distance	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, TFTP, CLI
Méthode d'authentification	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Caractéristiques	Prise en charge de BOOTP, prise en charge d'ARP, prise en charge du réseau local (LAN) virtuel, prise en charge de Syslog, prise en charge DiffServ, prise en charge d'IPv6, prise en charge du protocole STP (Spanning Tree Protocol), DHCP snooping, assistance Port Aggregation Protocol (PAgP), assistance Access Control List (ACL), qualité de service (QoS), sans ventilateur, Shaped Round Robin (SRR), notification de l'adresse MAC, Remote Switch Port Analyzer (RSPAN), Energy Efficient Ethernet, Multicast VLAN Registration (MVR), Class of Service (CoS), Weighted Tail Drop (WTD)
Normes de conformité	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ae, IEEE 802.1ab (LLDP), IEEE 802.3az
RAM	512 Mo
Mémoire Flash	128 Mo
Indicateurs d'état	Statut du port, vitesse de transmission du port, port mode duplex, système, liaison/activité

EXTENSION/CONNECTIVITÉ

Interfaces	Interfaces
------------	------------



Le commutateur réseau (Switch), est un équipement qui va nous permettre de relier plusieurs segments dans le réseau informatique et de créer des circuits virtuels.

Switch 2960 24TT - Cisco - WS-C2960-24TT-L - Catalyst 2960 24 10/100

Dimensions & Weight	
Depth:	23.6 cm
Height:	4.4 cm
Weight:	3.63 kg
Width:	44.5 cm
Environmental Parameters	
Humidity Range Operating:	10 - 95% (non-condensing)
Humidity Range Storage:	10 - 95% (non-condensing)
Max Operating Temperature:	40 °C
Max Storage Temperature:	70 °C
Min Operating Temperature:	-5 °C
Min Storage Temperature:	-25 °C
Expansion / Connectivity	
Interfaces:	24 x 100Base-TX RJ-45 2 x 1000Base-T RJ-45
General	
Authentication Method:	Secure Shell (SSH), RADIUS, TACACS+
Compliant Standards:	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Device Type:	Switch - 24 ports - Managed
Enclosure Type:	Rack-mountable 1U
Encryption Algorithm:	SSL
Features:	Layer 2 switching, auto-sensing per device, dynamic IP address assignment, auto-negotiation, BOOTP support, ARP support, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, Syslog support, DiffServ support, Broadcast Storm Control, IPv6 support, Multicast Storm Control, Unicast Storm Control, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, DHCP snooping, Dynamic Trunking Protocol (DTP) support, Port Aggregation Protocol (PAgP) support, Access Control List (ACL) support, Quality of Service (QoS), Link Aggregation Control Protocol (LACP), Port Security, MAC Address Notification, Remote Switch Port Analyzer (RSPAN)
Flash Memory:	32 MB Flash
MAC Address Table Size:	8K entries
Performance:	Switching capacity: 32 Gbps Forwarding performance (64-byte packet size): 6.5 Mpps
Ports:	24 x 10/100 + 2 x 10/100/1000
RAM:	64 MB
Remote Management Protocol:	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH
Status Indicators:	Port transmission speed, port duplex mode, power, link OK, system, link/activity
Subtype:	Fast Ethernet



Firewall ASA 5505 - CISCO ASA5505-BUN-K9 - Cisco ASA5505

Grille De Montage	Oui
Format	1U
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
Dissipation Thermique	72 BTU/H
Connexions Simultanées	10000
Certification	FCC, CE, VCCI ITE, CISPR 22, EN 60950, EN 61000-3-2, IEC 60950, EN 61000-3-3, UL 60950, CSA 22.2 No. 60950, EN55022, AS/NZ 3548
Wifi	Non
Nombre D'utilisateurs	10 Utilisateur(S)
Nombre De VLANs	3
Algorithme De Sécurité Soutenu	3DES,AES
Voyants	Oui
Technologie De Connectivité	Avec Fil
Fast Ethernet (Cuivre) Nombre De Ports	8
Quantité De Ports USB 2.0	3
Nombre De Port Ethernet LAN (RJ-45)	8
Nombre De Ports Série	1
Mémoire Interne	512 Mo
Mémoire Flash	128 Mo
Tension D'entrée AC	100-240 V
Fréquence D'entrée AC	50 - 60 Hz
Courant D'entrée	1.8 A
Puissance De Crête	96 W
Température D'opération	0 - 40 °C
Température Hors Fonctionnement	-25 - 70 °C
Taux D'humidité De Fonctionnement	5 - 95%
Altitude De Fonctionnement	0 - 2000 M
Altitude De Non Fonctionnement	0 - 4570 M
Dimensions (LxPxH)	200,04 X 174,5 X 44,5 Mm
Poids	1,8 Kg



Le pare-feu est un système nous permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur notre réseau informatique

e. Protocoles utilisés

La VLAN - Virtual Local Area Network :

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Les VLANs présentent les intérêts suivants :

Améliorer la gestion du réseau.

- Optimiser la bande passante.
- Séparer les flux.
- Segmentation : réduire la taille d'un domaine de broadcast.

La sécurité permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines appartenant à des VLAN différents est alors de passer par un routeur.

Le VTP - Trunking Protocol :

VLAN Trunking Protocol est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco. Elle permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local. Le VTP fonctionne sur les commutateurs Cisco dans un de ces 3 modes :

- Client
- Serveur
- Transparent

Le STP - Spanning Tree Protocol :

Le Spanning Tree Protocol est un protocole réseau permettant de déterminer une topologie réseau sans boucle dans les LAN avec ponts.

Le STP a trois caractéristiques principales qui sont avantageuses pour l'exploitation d'un réseau.

- La redondance le STP fournit une redondance à tous les périphériques du réseau.
- Les moyens de redondance terme que chaque connexion dispose de plusieurs sauvegardes qui peuvent être utilisés en cas de problèmes avec la connexion primaire.
- Le STP s'assure que chaque appareil possède un chemin à plusieurs commutateurs.

L'HSRP - Hot Standby Routing Protocol :

HSRP, soit Hot Standby Routing Protocol, est un protocole qui permet à un routeur d'être le secours d'un autre routeur situé sur le même réseau. Il est un protocole propriétaire de Cisco inspiré du protocole normalisé VRRP. Le principe de fonctionnement est que tous les routeurs émulent une adresse IP virtuelle qui sera utilisée comme passerelle par les équipements du réseau. Pour cela, chacun des routeurs configure son protocole HSRP avec un niveau de priorité. Celui qui disposera du plus grand se verra élu et sera actif. Les autres seront passifs en attendant la perte du premier routeur. Les avantages sont donc :

- Elle permet redondance des équipements
- Elle crée une tolérance aux pannes, la continuité de service
- Offre une disponibilité de la passerelle par défaut du réseau

L'EtherChannel:

L'EtherChannel est une technologie d'agrégation de liens utilisée principalement sur les commutateurs de Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet en un lien logique. Elle a pour avantage d'augmenter la vitesse et la tolérance aux pannes entre :

- Les commutateurs
- Les routeurs et les serveurs

L'OSPF - Open Shortest Path First:

Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus rapide vers chacun des réseaux connus dans la LSDB. Il a les avantages suivants :

- Son temps de convergence est court
- Il intègre la notion de taille de masque variable (VLSM), indispensable à la gestion des réseaux
- Il est économe en bande passante : en régime, seuls de courts messages *hello* sont envoyés, et en cas de changement de topologie, seuls les LSA modifiés sont envoyés aux voisins.

Les ACL - Access Control List :

Access Control List (ACL) est configuré sur un pare-feu ou un routeur permettant de filtrer, est une liste d'adresses ou de ports autorisés ou interdits par le dispositif. Les Access Control List sont divisés en trois grandes catégories, l'ACL standard, l'ACL étendue et la nommée-étendue. Elle va nous permettre d'augmenter la sécurité d'une infrastructure système et réseaux.

DHCP – Dynamic Host Configuration Protocol :

Le DHCP est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP des machines d'un réseau, en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. Il permet un réel gain de temps et permet une meilleure évolutivité de l'infrastructure.

ISP- Internet Service Provider :

C'est un Fournisseur d'accès à Internet

f. Commandes effectuées

Configuration des VLAN'S : CoreSW1:

<u>Vlan 10</u> Réseau des IT	Switch(config)#host Switch(config)#hostname CoreSW1 CoreSW1(config)#vlan 10 CoreSW1(config-vlan)# na CoreSW1(config-vlan)# name IT CoreSW1(config-vlan)#exit
<u>Vlan 20</u> Réseau des RH	CoreSW1(config)#vlan 20 CoreSW1(config-vlan)#nam CoreSW1(config-vlan)#name HR CoreSW1(config-vlan)#exit
<u>Vlan 30</u> Réseau de la comptabilité	CoreSW1(config)#vlan 30 CoreSW1(config-vlan)#nam CoreSW1(config-vlan)#name Accounting CoreSW1(config-vlan)#exit
<u>Vlan 40</u> Réseau pour les serveurs	CoreSW1(config)#vlan 40 CoreSW1(config-vlan)#name SERVERFARM CoreSW1(config-vlan)#exit

Résultat :

<u>Show vlan</u>	10 IT active 20 HR active 30 Accounting active 40 SERVERFARM active 1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active
-------------------------	--

Configuration du VTP et Trunking : CoreSW1

Mise en place vtp	<pre> CoreSW1(config)#vtp CoreSW1(config)#vtp m CoreSW1(config)#vtp mode s CoreSW1(config)#vtp mode server Device mode already VTP SERVER. CoreSW1(config)#vtp do CoreSW1(config)#vtp domain cis CoreSW1(config)#vtp domain cisco.com Changing VTP domain name from NULL to cisco.com CoreSW1(config)#vt CoreSW1(config)#vtp se CoreSW1(config)#vtp se CoreSW1(config)#vtp ver CoreSW1(config)#vtp version 2 CoreSW1(config)#exit </pre>
Trunking 21 a 24	<pre> CoreSW1(config)#int rang CoreSW1(config)#int range f0/21-24 CoreSW1(config-if-range)#sw CoreSW1(config-if-range)#switchport tr CoreSW1(config-if-range)#switchport trunk enca CoreSW1(config-if-range)#switchport trunk encapsulation dot CoreSW1(config-if-range)#switchport trunk encapsulation dot1q CoreSW1(config-if-range)#sw CoreSW1(config-if-range)#switchport mo CoreSW1(config-if-range)#switchport mode tru CoreSW1(config-if-range)#switchport mode trunk </pre>
Trunking 1 a 3	<pre> CoreSW1(config)#int ra CoreSW1(config)#int range f0/1-3 CoreSW1(config-if-range)#sw CoreSW1(config-if-range)#switchport tr CoreSW1(config-if-range)#switchport trunk enc CoreSW1(config-if-range)#switchport trunk encapsulation do CoreSW1(config-if-range)#switchport trunk encapsulation dot1q CoreSW1(config-if-range)#sw CoreSW1(config-if-range)#switchport mo CoreSW1(config-if-range)#switchport mode tr CoreSW1(config-if-range)#switchport mode trunk </pre>

Résultat :

Show vtp status	<pre> CoreSW1#show vtp status VTP Version capable : 1 to 2 VTP version running : 2 VTP Domain Name : cisco.com VTP Pruning Mode : Disabled VTP Traps Generation : Disabled Device ID : 00D0.976C.1C00 Configuration last modified by 0.0.0.0 at 3-1-93 02:14:05 Local updater ID is 0.0.0.0 (no valid interface found) Feature VLAN : ----- VTP Operating Mode : Server Maximum VLANs supported locally : 1005 Number of existing VLANs : 5 Configuration Revision : 1 MD5 digest : 0xD9 0xFC 0x2F 0x67 0x17 0xC8 0x14 0xA5 0x1B 0x19 0xFE 0x24 0x59 0x42 0xB8 0x52 CoreSW1# </pre>
-----------------	---

Show interface trunk	CoreSW1#show interfaces trunk				
	Port	Mode	Encapsulation	Status	Native vlan
	Fa0/1	on	802.1q	trunking	1
	Fa0/2	on	802.1q	trunking	1
	Fa0/3	on	802.1q	trunking	1
	Fa0/4	on	802.1q	trunking	1
	Fa0/21	on	802.1q	trunking	1
	Fa0/22	on	802.1q	trunking	1
	Fa0/23	on	802.1q	trunking	1
	Fa0/24	on	802.1q	trunking	1
	Port	Vlans allowed on trunk			
	Fa0/1	1-1005			
	Fa0/2	1-1005			
	Fa0/3	1-1005			
	Fa0/4	1-1005			
	Fa0/21	1-1005			
	Fa0/22	1-1005			
	Fa0/23	1-1005			
	Fa0/24	1-1005			

Configuration du VTP et Trunking : CoreSW2

Mise en place vtp	<pre>Switch(config)#vtp Switch(config)#vtp mode server Device mode already VTP SERVER. Switch(config)#vtp version 2 VTP mode already in V2. Switch(config)#show vtp status</pre>
Trunking 2 a 5	<pre>Switch(config)#int range f0/2-5 Switch(config-if-range)#sw Switch(config-if-range)#switchport trunk enc Switch(config-if-range)#switchport trunk encapsulation do Switch(config-if-range)#switchport trunk encapsulation dot1q Switch(config-if-range)#sw Switch(config-if-range)#switchport mode tr Switch(config-if-range)#switchport mode trunk</pre>
Trunking 21 a 24	<pre>Switch(config)#int ran Switch(config)#int range f0/21-24 Switch(config-if-range)#sw Switch(config-if-range)#switchport tru Switch(config-if-range)#switchport trunk enc Switch(config-if-range)#switchport trunk encapsulation so Switch(config-if-range)#switchport trunk encapsulation do Switch(config-if-range)#switchport trunk encapsulation dot1q Switch(config-if-range)#sw Switch(config-if-range)#switchport mode tr Switch(config-if-range)#switchport mode trunk</pre>

```
Switch#show vtp status
VTP Version capable          : 1 to 2
VTP version running          : 2
VTP Domain Name               : cisco.com
VTP Pruning Mode              : Disabled
VTP Traps Generation         : Disabled
Device ID                     : 00E0.8F08.8D00
Configuration last modified by 0.0.0.0 at 3-1-93 02:57:03
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
-----
VTP Operating Mode            : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs      : 5
Configuration Revision         : 9
MD5 digest                    : 0x0E 0x5F 0x3F 0xB9 0x63 0x1C
                                0x24 0x0E
                                0xF2 0xD0 0x97 0x4C 0xA3 0x77
0x8B 0x24
Switch#
```

VTP Client et Trunk sur tous les Access Switch

<u>AccSW1</u>	<pre>Switch(config)#int range f0/2-3 Switch(config-if-range)#sw Switch(config-if-range)#switchport mo Switch(config-if-range)#switchport mode tr Switch(config-if-range)#switchport mode trunk Switch(config-if-range)# Switch(config-if-range)#</pre>
<u>AccSW2</u>	<pre>Switch(config)#hostname AccSW2 AccSW2(config)#int range f0/3-4 AccSW2(config-if-range)#sw AccSW2(config-if-range)#switchport mo AccSW2(config-if-range)#switchport mode trun AccSW2(config-if-range)#switchport mode trunk AccSW2(config-if-range)#</pre>
<u>AccSW3</u>	<pre>Switch(config)#hostname AccSW3 AccSW3(config)#int range f0/4-5 AccSW3(config-if-range)#sw AccSW3(config-if-range)#switchport mo AccSW3(config-if-range)#switchport mode tru AccSW3(config-if-range)#switchport mode trunk AccSW3(config-if-range)#</pre>
<u>AccSW4</u>	<pre>AccSW5(config)#int range f0/1-2 AccSW5(config-if-range)#sw AccSW5(config-if-range)#switchport mo AccSW5(config-if-range)#switchport mode tr AccSW5(config-if-range)#switchport mode trunk</pre>

Résultat :

<u>Show vlan</u>	<pre> VLAN Name Status Ports ----- 1 default active Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2 10 IT active 20 HR active 30 Accounting active 40 SERVERFARM active 1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active </pre>
------------------	---

Show interface trunk

```
AccSW6>show interface trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking      1
Fa0/2     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,40
Fa0/2     1,10,20,30,40

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,40
```

Assignment des ports aux vlan

AccSW1

```
AccSW1(config)#int range f0/1
AccSW1(config-if-range)#sw
AccSW1(config-if-range)#switchport mode
AccSW1(config-if-range)#switchport mode acc
AccSW1(config-if-range)#switchport mode access
AccSW1(config-if-range)#sw
AccSW1(config-if-range)#switchport acc
AccSW1(config-if-range)#switchport access vlan 10
```

AccSW2

```
AccSW2(config)#int range f0/1
AccSW2(config-if-range)#sw1
AccSW2(config-if-range)#switchport mod
AccSW2(config-if-range)#switchport mode acc
AccSW2(config-if-range)#switchport mode access
AccSW2(config-if-range)#sw
AccSW2(config-if-range)#switchport acc
AccSW2(config-if-range)#switchport access vl
AccSW2(config-if-range)#switchport access vlan 20
AccSW2(config-if-range)#
```

AccSW3

```
AccSW3(config)#int range f0/1
AccSW3(config-if-range)#sw
AccSW3(config-if-range)#switchport mo
AccSW3(config-if-range)#switchport mode acc
AccSW3(config-if-range)#switchport mode access
AccSW3(config-if-range)#sw
AccSW3(config-if-range)#switchport acc
AccSW3(config-if-range)#switchport access vlan 30
AccSW3(config-if-range)#
```

AccSW4

```
AccSW5(config)#int range f0/3-5
AccSW5(config-if-range)#sw
AccSW5(config-if-range)#switchport mod
AccSW5(config-if-range)#switchport mode acc
AccSW5(config-if-range)#switchport mode access
AccSW5(config-if-range)#sw ..
AccSW5(config-if-range)#switchport acc
AccSW5(config-if-range)#switchport access vl
AccSW5(config-if-range)#switchport access vlan 40
```

Résultat :

Show running config	<pre>AccSW5#show running-config Building configuration... Current configuration : 1279 bytes ! version 13.2 no service timestamps log datetime msec no service timestamps debug datetime msec no service password-encryption ! hostname AccSW5 ! ! ! ! ! ! spanning-tree mode pvst spanning-tree extend system-id ! interface FastEthernet0/1 switchport mode trunk ! interface FastEthernet0/2 switchport mode trunk ! interface FastEthernet0/3 switchport access vlan 40 switchport mode access ! interface FastEthernet0/4 switchport access vlan 40 switchport mode access ! interface FastEthernet0/5 switchport access vlan 40 switchport mode access !</pre>
Show vlan	<pre>AccSW5#show vlan VLAN Name Status Ports ----- 1 default active Fa0/4, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2 10 IT active 20 HR active 30 Accounting active 40 SERVERFARM active Fa0/3, Fa0/4, Fa0/5 1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2 ----- 1 enet 100001 1500 - - - - - 0 0 10 enet 100010 1500 - - - - - 0 0 --More--</pre>

Configuration du STP – CoreSW1 :

<u>Vlan 10</u>	<pre>CoreSW1(config)#int vlan 10 CoreSW1(config-if)# %LINK-5-CHANGED: Interface Vlan10, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to CoreSW1(config-if)# CoreSW1(config-if)#ip ad CoreSW1(config-if)#ip address 192.168.10.1 255.255.255.0 CoreSW1(config-if)#no sh CoreSW1(config-if)#no shutdown CoreSW1(config-if)#exit</pre>
<u>Vlan 20</u>	<pre>CoreSW1(config)#int vlan 20 CoreSW1(config-if)# %LINK-5-CHANGED: Interface Vlan20, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up CoreSW1(config-if)#ip ad CoreSW1(config-if)#ip address 192.168.20.1 255.255.255.0 CoreSW1(config-if)# CoreSW1(config-if)#exit</pre>
<u>Vlan 30</u>	<pre>CoreSW1(config)#int vlan 30 CoreSW1(config-if)# %LINK-5-CHANGED: Interface Vlan30, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up CoreSW1(config-if)#ip ad CoreSW1(config-if)#ip address 192.168.30.1 255.255.255.0 CoreSW1(config-if)# CoreSW1(config-if)#no shutdown CoreSW1(config-if)#exit</pre>
<u>Vlan 40</u>	<pre>CoreSW1(config)#int vlan 40 CoreSW1(config-if)# %LINK-5-CHANGED: Interface Vlan40, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up ip ad CoreSW1(config-if)#ip address 192.168.40.1 255.255.255.0 CoreSW1(config-if)#no shutdown</pre>
<u>Primary 10 et 20</u>	<pre>CoreSW1(config)#sp CoreSW1(config)#spanning-tree vla CoreSW1(config)#spanning-tree vlan 10,20 pri CoreSW1(config)#spanning-tree vlan 10,20 root CoreSW1(config)#spanning-tree vlan 10,20 root pri CoreSW1(config)#spanning-tree vlan 10,20 root primary</pre>

Résultat :

Show running conf

```
interface Vlan10
  mac-address 0001.c707.ec01
  ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
  mac-address 0001.c707.ec02
  ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
  mac-address 0001.c707.ec03
  ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
  mac-address 0001.c707.ec04
  ip address 192.168.40.1 255.255.255.0
!
ip classless
!
ip flow-export version 5
!
```

Show spanning tree

```
Interface              Role Sts Cost          Prio.Nbr Type
-----
Fa0/1                  Desg FWD 19          128.1   P2p
Fa0/2                  Desg FWD 19          128.2   P2p
Fa0/4                  Desg FWD 19          128.4   P2p
Fa0/3                  Desg FWD 19          128.3   P2p
Fa0/22                 Desg FWD 19          128.22  P2p
Fa0/24                 Desg FWD 19          128.24  P2p
Fa0/21                 Desg FWD 19          128.21  P2p
Fa0/23                 Desg FWD 19          128.23  P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address      0001.C707.EC63
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596 (priority 24576 sys-id-ext 10)
             Address      0001.C707.EC53
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface              Role Sts Cost          Prio.Nbr Type
-----
Fa0/1                  Desg FWD 19          128.1   P2p
Fa0/2                  Desg FWD 19          128.2   P2p
Fa0/4                  Desg FWD 19          128.4   P2p
Fa0/3                  Desg FWD 19          128.3   P2p
Fa0/22                 Desg FWD 19          128.22  P2p
Fa0/24                 Desg FWD 19          128.24  P2p
Fa0/21                 Desg FWD 19          128.21  P2p
Fa0/23                 Desg FWD 19          128.23  P2p

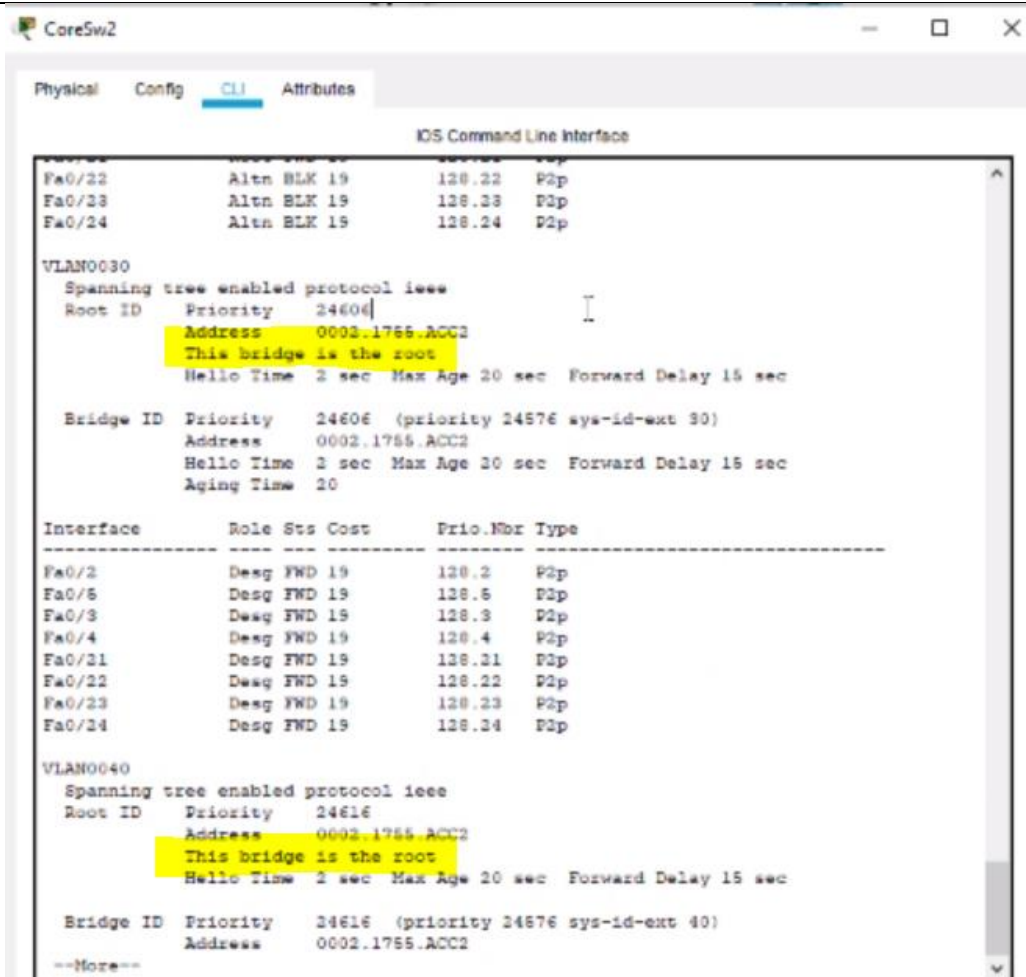
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address      0001.C707.EC63
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596 (priority 24576 sys-id-ext 20)
             Address      0001.C707.EC53
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Configuration du STP – CoreSW2 :

Même configuration des vlan que CoreSW1	-
Primary 30 et 40	<pre>Switch(config)#spanning-tree vl Switch(config)#spanning-tree vlan 30,40 root Switch(config)#spanning-tree vlan 30,40 root pr Switch(config)#spanning-tree vlan 30,40 root primary Switch(config)#</pre>

Résultat :

<u>Show spanning-tree</u>	 <p>The screenshot shows the CLI of CoreSW2 with the following output:</p> <pre>CoreSw2 Physical Config CLI Attributes IOS Command Line Interface VLAN0030 Spanning tree enabled protocol ieee Root ID Priority 24606 Address 0002.1755.AC03 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 24606 (priority 24576 sys-id-ext 30) Address 0002.1755.AC03 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 20 Interface Role Sts Cost Prio.Nbr Type ----- Fa0/2 Desg FWD 19 128.2 P2p Fa0/5 Desg FWD 19 128.5 P2p Fa0/3 Desg FWD 19 128.3 P2p Fa0/4 Desg FWD 19 128.4 P2p Fa0/21 Desg FWD 19 128.31 P2p Fa0/22 Desg FWD 19 128.22 P2p Fa0/23 Desg FWD 19 128.23 P2p Fa0/24 Desg FWD 19 128.24 P2p VLAN0040 Spanning tree enabled protocol ieee Root ID Priority 24616 Address 0002.1755.AC02 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 24616 (priority 24576 sys-id-ext 40) Address 0002.1755.AC02 --More--</pre>
---------------------------	--

Configuration EtherChannel :

CoreSW1	<pre>CoreSW1(config)#int range f0/21-24 CoreSW1(config-if-range)#chann CoreSW1(config-if-range)#chan CoreSW1(config-if-range)#channel-group 1 mode % Incomplete command. CoreSW1(config-if-range)#channel-group 1 mode on CoreSW1(config-if-range)# Creating a port-channel interface Port-channel 1 %LINK-5-CHANGED: Interface Port-channel1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up CoreSW1(config-if-range)#show etherchannel summary ^ % Invalid input detected at '^' marker. CoreSW1(config-if-range)#end CoreSW1# %SYS-5-CONFIG_I: Configured from console by console CoreSW1#show etherchannel summary Flags: D - down P - in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator u - unsuitable for bundling w - waiting to be aggregated d - default port Number of channel-groups in use: 1 Number of aggregators: 1 Group Port-channel Protocol Ports -----+-----+-----+----- 1 Po1(SU) - Fa0/21(P) Fa0/22(P) Fa0/23(P) Fa0/24(P) CoreSW1#</pre>
CoreSW2	<pre>Switch(config)#int range f0/21-24 Switch(config-if-range)#chan Switch(config-if-range)#channel- Switch(config-if-range)#channel-grou Switch(config-if-range)#channel-group 1 mode on Switch(config-if-range)# Creating a port-channel interface Port-channel 1 %LINK-5-CHANGED: Interface Port-channel1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up Switch(config-if-range)#end Switch# %SYS-5-CONFIG_I: Configured from console by console Switch#show etherchannel summary Flags: D - down P - in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator u - unsuitable for bundling w - waiting to be aggregated d - default port Number of channel-groups in use: 1 Number of aggregators: 1 Group Port-channel Protocol Ports -----+-----+-----+----- 1 Po1(SU) - Fa0/21(P) Fa0/22(P) Fa0/23(P) Fa0/24(P) Switch#</pre>

HSRP sur CoreSW1:

<u>Port channel conf</u>	<pre>CoreSW1(config)#int port-channel 1 CoreSW1(config-if)#s CoreSW1(config-if)#sw CoreSW1(config-if)#switchport tr CoreSW1(config-if)#switchport trunk en CoreSW1(config-if)#switchport trunk encapsulation d CoreSW1(config-if)#switchport trunk encapsulation dot1q</pre>
<u>Vlan 10</u>	<pre>CoreSW1(config)#int vlan 10 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 ip 192.168.10.254 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pri CoreSW1(config-if)#standby 1 priority 200 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pre CoreSW1(config-if)#standby 1 preempt CoreSW1(config-if)# CoreSW1(config-if)# CoreSW1(config-if)#exit CoreSW1(config)#</pre>
<u>Vlan 20</u>	<pre>CoreSW1(config)#int vlan 20 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1i %HSRP-6-STATECHANGE: Vlan10 Grp 1 state Speak -> Standby P %HSRP-6-STATECHANGE: Vlan10 Grp 1 state Standby -> Active ^ % Invalid input detected at '^' marker. CoreSW1(config-if)# CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 ip 192.168.20.254 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pri CoreSW1(config-if)#standby 1 priority 200 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pre CoreSW1(config-if)#standby 1 preempt CoreSW1(config-if)# CoreSW1(config-if)# CoreSW1(config-if)#exit CoreSW1(config)#</pre>
<u>Vlan 30</u>	<pre>CoreSW1(config)#int vlan 30 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 ip 192.168. %HSRP-6-STATECHANGE: Vlan20 Grp 1 state Speak -> Standby 20 %HSRP-6-STATECHANGE: Vlan20 Grp 1 state Standby -> Activ ^ % Invalid input detected at '^' marker. CoreSW1(config-if)# CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 ip 192.168.30.254 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pri CoreSW1(config-if)#standby 1 priority 150 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pre CoreSW1(config-if)#standby 1 preempt CoreSW1(config-if)#exit CoreSW1(config)#</pre>
<u>Vlan 40</u>	<pre>CoreSW1(config)#int vlan 40 CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 ip 192.168.40.25 %HSRP-6-STATECHANGE: Vlan30 Grp 1 state Speak -> Standby 4 %HSRP-6-STATECHANGE: Vlan30 Grp 1 state Standby -> Active CoreSW1(config-if)#st CoreSW1(config-if)#standby 1 pri CoreSW1(config-if)#standby 1 priority 150 CoreSW1(config-if)#st CoreSW1(config-if)#standby pr CoreSW1(config-if)#standby pre CoreSW1(config-if)#standby preempt CoreSW1(config-if)#</pre>

Résultat :

Show brief

```
CoreSW1#show standby brief
                P indicates configured to preempt.
                |
Interface    Grp  Pri  P State    Active        Standby        Virtual IP
Vl10         1    200  P Active   local         192.168.10.2   192.168.10.254
Vl20         1    200  P Active   local         192.168.20.2   192.168.20.254
Vl30         1    150  Standby  192.168.30.2 local         192.168.30.254
Vl40         1    150  Standby  192.168.40.2 local         192.168.40.254
CoreSW1#
```

Show running config

```
!
interface Vlan10
 mac-address 0001.c707.ec01
 ip address 192.168.10.1 255.255.255.0
 standby 1 ip 192.168.10.254
 standby 1 priority 200
 standby 0 preempt
!
interface Vlan20
 mac-address 0001.c707.ec02
 ip address 192.168.20.1 255.255.255.0
 standby 1 ip 192.168.20.254
 standby 1 priority 200
 standby 0 preempt
!
interface Vlan30
 mac-address 0001.c707.ec03
 ip address 192.168.30.1 255.255.255.0
 standby 1 ip 192.168.30.254
 standby 1 priority 150
 standby 0 preempt
!
interface Vlan40
 mac-address 0001.c707.ec04
 ip address 192.168.40.1 255.255.255.0
 standby 1 ip 192.168.40.254
 standby 1 priority 150
 standby 0 preempt
```


HSRP sur CoreW2 :

<u>Port channel conf</u>	<pre>Switch(config)#int port-channel 1 Switch(config-if)#s Switch(config-if)#sw Switch(config-if)#switchport t Switch(config-if)#switchport trunk en Switch(config-if)#switchport trunk encapsulation d Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)# Switch(config-if)# Switch(config-if)#exit</pre>
<u>Vlan 10</u>	<pre>Switch(config)#int vlan 10 Switch(config-if)#s Switch(config-if)#st Switch(config-if)#standby 1 ip 192.168.10.254 Switch(config-if)#st Switch(config-if)#standby 1 pri Switch(config-if)#standby 1 priority %HSRP-6-STATECHANGE: Vlan10 Grp 1 state Speak -> Standby 150 Switch(config-if)# Switch(config-if)#st Switch(config-if)#standby 1 pr Switch(config-if)#standby 1 pre Switch(config-if)#standby 1 preempt Switch(config-if)#exit</pre>
<u>Vlan 20</u>	<pre>Switch(config)#int vlan 20 Switch(config-if)#st Switch(config-if)#standby 1 ip 192.168.20.254 Switch(config-if)#st Switch(config-if)#standby 1 pri Switch(config-if)#standby 1 priority 150 Switch(config-if)#st Switch(config-if)#standby 1 pre Switch(config-if)#standby 1 preempt Switch(config-if)#exit</pre>
<u>Vlan 30</u>	<pre>Switch(config)#int vlan 30 Switch(config-if)#st Switch(config-if)#standby 1 ip 192.168.30.2 %HSRP-6-STATECHANGE: Vlan20 Grp 1 state Speak -> Standby 54 Switch(config-if)#st Switch(config-if)#standby 1 pri Switch(config-if)#standby 1 priority 200 Switch(config-if)#st Switch(config-if)#standby 1 pre Switch(config-if)#standby 1 preempt Switch(config-if)#exit</pre>
<u>Vlan 40</u>	<pre>Switch(config)#int vlan 40 Switch(config-if)#st Switch(config-if)#standby 1 ip Switch(config-if)#standby 1 ip 192.168.40.254 Switch(config-if)#s Switch(config-if)#st Switch(config-if)#standby 1 pri Switch(config-if)#standby 1 priority 200 Switch(config-if)#st Switch(config-if)#standby 1 pre Switch(config-if)#standby 1 preempt Switch(config-if)# Switch(config-if)#end Switch#</pre>

Résultat :

Show brief	<pre>Switch#show standby brief P indicates configured to preempt. Interface Grp Pri P State Active Standby Virtual IP Vl10 1 150 P Standby 192.168.10.1 local 192.168.10.254 Vl20 1 150 P Standby 192.168.20.1 local 192.168.20.254 Vl30 1 200 P Active local 192.168.30.1 192.168.30.254 Vl40 1 200 P Active local 192.168.40.1 192.168.40.254 Switch#</pre>
Show running config	<pre>Switch(config)#int port-channel 1 Switch(config-if)#s Switch(config-if)#sw Switch(config-if)#switchport t Switch(config-if)#switchport trunk en Switch(config-if)#switchport trunk encapsulation d Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)# Switch(config-if)# Switch(config-if)#exit Switch#</pre>

Configuration OSPF sur CoreSW1 :

Conf f0/20	<pre>CoreSW1(config)#int f0/20 CoreSW1(config-if)#no sh CoreSW1(config-if)#no swi CoreSW1(config-if)#no switchport CoreSW1(config-if)#ip ad CoreSW1(config-if)#ip address 1.1.1.2 255.255.255.0 CoreSW1(config-if)#no sh CoreSW1(config-if)#no shutdown CoreSW1(config-if)#</pre>
Conf g0/1	<pre>CoreSW1(config)#int g0/1 CoreSW1(config-if)#ip ad CoreSW1(config-if)#no sw CoreSW1(config-if)#no switchport CoreSW1(config-if)#ip ad CoreSW1(config-if)#ip address 1.1.1.2 255.255.255.0 CoreSW1(config-if)#no sh CoreSW1(config-if)#no sh CoreSW1(config-if)#no shutdown CoreSW1(config-if)#</pre>
Conf OSPF	<pre>CoreSW1(config)#int range f0/21-24 CoreSW1(config-if-range)#exit CoreSW1(config)# CoreSW1(config)#router os CoreSW1(config)#router ospf 1 CoreSW1(config-router)#net CoreSW1(config-router)#network 1.1.1.0 0.0.0.255 area 0 CoreSW1(config-router)#network 1.1.1.0 0.0.0.255 area 0 CoreSW1(config-router)#net CoreSW1(config-router)#network 3.3.3.0 0.0.0.255 are CoreSW1(config-router)#network 3.3.3.0 0.0.0.255 area 0 CoreSW1(config-router)#net CoreSW1(config-router)#network 192.168.10.0 0.0.0.255 area 0 CoreSW1(config-router)# ! Invalid input detected at '^' marker. CoreSW1(config-router)#network 192.168.10.0 0.0.0.0.255 area 0 CoreSW1(config-router)# ! Invalid input detected at '^' marker. CoreSW1(config-router)#network 192.168.10.0 0.0.0.255 area 0 CoreSW1(config-router)#network 192.168.20.0 0.0.0.255 area 0 CoreSW1(config-router)#network 192.168.30.0 0.0.0.255 area 0 CoreSW1(config-router)#network 192.168.40.0 0.0.0.255 area 0 CoreSW1(config-router)#</pre>

Configuration OSPF sur CoreSW12 :

<u>Conf f0/20</u>	<pre>Switch(config)#int g0/1 Switch(config-if)#ip ad Switch(config-if)#no swi Switch(config-if)#no switchport Switch(config-if)#ip ad Switch(config-if)#ip address 2.2.2.2 255.255.255.0 Switch(config-if)#no sh Switch(config-if)#no shutdown Switch(config-if)#</pre>	
<u>Conf g0/1</u>	<pre>Switch(config-if)#int f0/20 Switch(config-if)#no swi Switch(config-if)#no switchport Switch(config-if)#ip ad Switch(config-if)#ip address 4.4.4.2 255.255.255.0 Switch(config-if)#no sh Switch(config-if)#no shutdown Switch(config-if)#</pre>	
<u>Conf OSPF</u>	<pre>Switch(config)#router ospf 1 Switch(config)#router ospf 1 Switch(config-router)#net Switch(config-router)#network 4.4.4.0 0.0.0.255 area 0 Switch(config-router)#network 2.2.2.0 0.0.0.255 area 0 Switch(config-router)#network 192.168.10.0 0.0.0.255 area 0 Switch(config-router)#network 192.168.30.0 0.0.0.255 area 0 01:42:48: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Vlan10 from LOADING to FULL, Loading Done Switch(config-router)# 01:42:52: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Vlan20 from LOADING to FULL, Loading Done Switch(config-router)#network 192.168.30.0 0.0.0.255 area 0 Switch(config-router)#network 192.168.40.0 0.0.0.255 area 0 Switch(config-router)# 01:43:19: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Vlan40 from LOADING to FULL, Loading Done 01:43:21: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Vlan30 from LOADING to FULL, Loading Done Switch(config-router)#</pre>	

Configuration OSPF et ISP sur R3:

Conf ispf

```
Router>enable
Router#conf
Router#configure ter
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip add
Router(config-if)#ip address 5.5.5.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Router(config-if)#int
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
Router(config-if)#int s0/0/1
Router(config-if)#ip add
Router(config-if)#ip address 6.6.6.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Router(config-if)#int g0/0
Router(config-if)#ip
Router(config-if)#ip add
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shu
Router(config-if)#no shutdown

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

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

Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 10.10.10.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 5.5.5.1 YES manual up up
Serial0/0/1 6.6.6.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
Router#ping 5.5.5.2
```

Conf ospf

```
Router(config)#router os
Router(config)#router ospf 1
Router(config-router)#net
Router(config-router)#network 5.5.5.0 0.0.0.255 area 0
Router(config-router)#network 5.5.5.0 0.0.0.255 area 0
01:58:32: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.2 on Serial0/0/0 from
LOADING to FULL, Loading Done

Router(config-router)#network 6.6.6.0 0.0.0.255 area 0
Router(config-router)#network 6.6.6.0 0.0.0.255 area 0
01:58:55: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.2 on Serial0/0/1 from
LOADING to FULL, Loading Done

Router(config-router)#network 10.0 0.0.0.255 area 0
^
% Invalid input detected at '^' marker.

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0
Router(config-router)#
```

Configuration OPF sur R1 :

<u>Conf des interface</u>	<pre>R1(config)#int g0/0 R1(config-if)#ip add R1(config-if)#ip address 1.1.1.1 255.255.255.0 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R1(config-if)# R1(config-if)# R1(config-if)#int s0/0/0 R1(config-if)#ip add R1(config-if)#ip address 5.5.5.2 255.255.255.0 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface-Serial0/0/0, changed state to down R1(config-if)#int g0/1 R1(config-if)#ip add R1(config-if)#ip address 4.4.4.1 255.255.255.0 R1(config-if)#no shutdown</pre>
<u>Conf ospf</u>	<pre>R1(config)#router ospf 1 R1(config-router)#net R1(config-router)#network 1.1.1.0 0.0.0.255 area 0 R1(config-router)#network 5.5.5.0 0.0.0.255 area 0 01:46:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on GigabitEthernet0/0 from LOADING to FULL, Loading Done R1(config-router)#network 4.4.4.0 0.0.0.255 area 0 R1(config-router)# 01:46:12: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.2 on GigabitEthernet0/1 from LOADING to FULL, Loading Done</pre>

Configuration OSPF sur R2 :

<p><u>Conf des interface</u></p>	<pre> Router>enable Router#con Router#conf ter Router#conf terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#conf te Router(config)#int g0/0 Router(config-if)#ip add Router(config-if)#ip address 2.2.2.1 255.255.255.0 Router(config-if)#no shutd Router(config-if)#no shutdown Router(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router(config-if)#int g0/1 Router(config-if)#ip Router(config-if)#ip dd Router(config-if)#ip add Router(config-if)#ip address 3.3.3.3 255.255.255.0 Router(config-if)#no shutd Router(config-if)#no shutdown Router(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up Router(config-if)#int s0/0/0 Router(config-if)#ip add Router(config-if)#ip address 6.6.6.2 255.255.255. % Invalid input detected at '^' marker. Router(config-if)#ip address 6.6.6.2 255.255.255.0 Router(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down Router(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up </pre>
<p><u>Conf ospf</u></p>	<pre> Router>enable Router#conf ter Router#conf terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router os Router(config)#router ospf 1 Router(config-router)#netw Router(config-router)#network 3.3.3.0 0.0.0.255 area 0 Router(config-router)#network 0 0.0.0.255 area 0 01:50:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on GigabitEthernet0/1 from LOAD Router(config-router)#network 2.2.2.0 0.0.0.255 area 0 Router(config-router)#network 6.6.6.0 0.0.0.255 area 0 01:51:07: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.2 on GigabitEthernet0/0 from Router(config-router)#network 6.6.6.0 0.0.0.255 area 0 Router(config-router)# </pre>

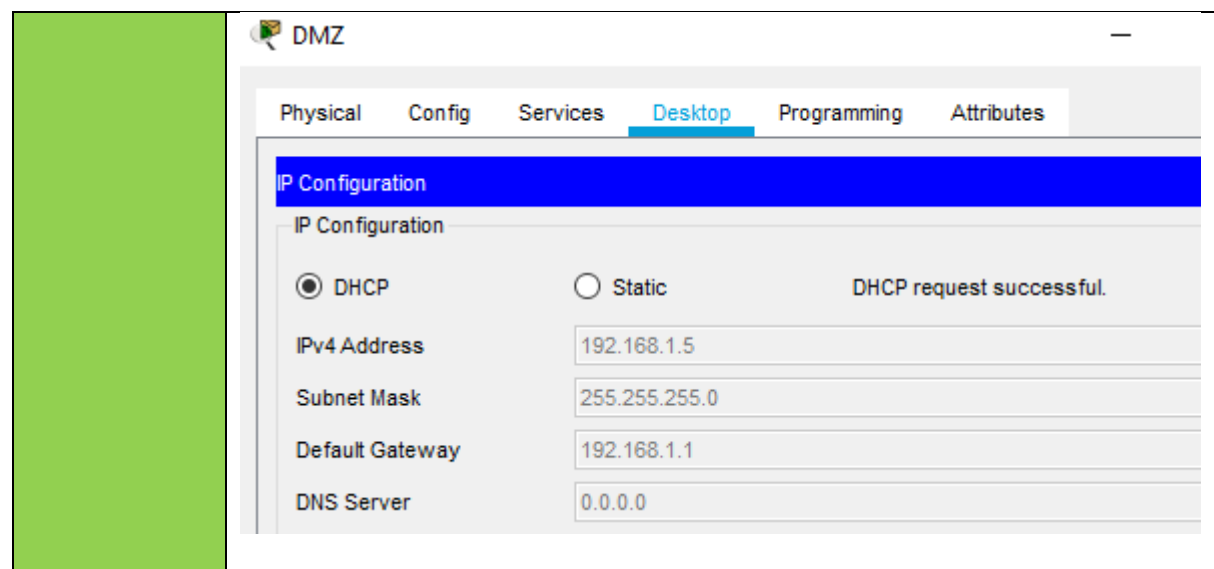
ACL :

Firewall ASA ACL's pour permettre le ping du serveur sur le routeur	<pre>access-list 100 extended permit icmp host 192.168.1.11 any access-list entrant extended permit icmp any any access-list global_access extended permit icmp any any .</pre>
--	---

DHCP :

Firewall ASA	<pre>dhcpd auto_config outside ! dhcpd address 192.168.1.5-192.168.1.36 inside dhcpd enable inside .</pre>
---------------------	--

Résultat :



The screenshot shows the DMZ configuration interface. The 'Desktop' tab is selected under the 'Config' section. The 'IP Configuration' section is expanded, showing the 'DHCP' radio button selected. The 'Static' radio button is also visible. A message 'DHCP request successful.' is displayed. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are filled with the values 192.168.1.5, 255.255.255.0, 192.168.1.1, and 0.0.0.0 respectively.

Field	Value
IPv4 Address	192.168.1.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Evolutions :

Honeypot :

Qu'est-ce que c'est ?

Un honeypot est un système en réseau utilisé comme leurre afin d'attirer les cybercriminels et ainsi détecter, dévier ou étudier leurs tentatives de piratage. Pour plus tard envisagé diverses améliorations de notre système.

Comment le mettre en place ?

Pour cela nous mettons en place un serveur avec une certaine adresse ip. Les pings vont d'abord passer serveur puis atteindre les autres si la requête respecte notre sécurité.

Portail captif :

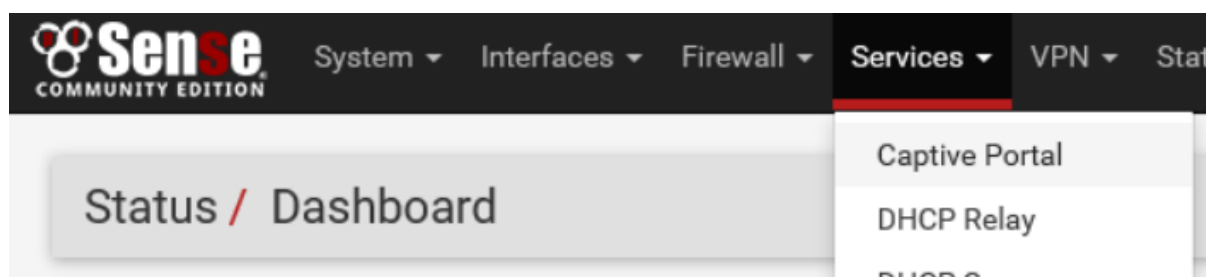
Qu'est-ce que c'est ?

Le portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web précis.

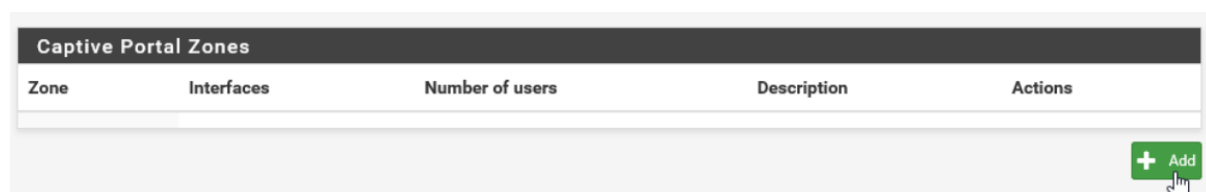
Comment le mettre en place ?

Pour mettre en place le portail captif nous pouvons utiliser pfsense sur lequel on effectue les manipulations suivantes :

Pfsense propose une interface dans lequel nous pouvons via les services mettre ne place le portail captif.



Nous pouvons ensuite ajoute notre nouveau portail :



Nous pourrions ensuite effectuées toutes les configurations nécessaires afin de l'adapté à notre infrastructure.

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Interfaces	<div><div>WAN</div><div>LAN</div></div> <p>Select the interface(s) to enable for captive portal.</p>
Maximum concurrent connections	<div>3</div> <p>Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.</p>
Idle timeout (Minutes)	<div>15</div> <p>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</p>
Hard timeout (Minutes)	<div>900</div> <p>Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).</p>
Pass-through credits per MAC address.	<div></div> <p>Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.</p>

IPS et l'IDS :

Qu'est-ce que c'est ?

Les IPS sont des IDS actifs : En cas de détection d'une attaque, L'IPS réagi en temps réel en stoppant les trafics suspects, notamment en bloquant les ports. Un IDS est un mécanisme qui a pour objectif de repérer tout type de trafic pouvant être malveillant. Cela permet ainsi d'avoir une action de prévention sur les différents risques d'intrusion, IDS va détecter les activités respectant pas la norme et lancé une alerte par suite de ça.

Comment le mettre en place ?

Nous effectuons une configuration sur routeur de niveau 3 cisco afin de le mettre en place.